2026

Cognitive Warfare: A Democratic Defence

VOLUME 1: PROTECTING OUR HEARTS & MINDS IN DEFENCE OF DEMOCRACY

ELIZABETH ANDERSON WITH AMBASSADOR EITVYDAS BAJARŪNAS

Table of Contents

Acknowledgements ***6***

Executive Summary ***7***

Part I: The Stakes ***10***

Chapter 1: The Target Is the Mind **10**

Defining the Domain 12

Four Vectors, One Architecture 15

Cognitive Sovereignty and the Case for Democratic Defence 16

Chapter 2: Why Democracies Are Vulnerable **18**

Structural Openness and Its Costs 18

The Platform Problem 19

Trust, Pluralism, and Speed 21

The Mandate Vacuum 23

Why Reactive Response Is Insufficient 23

Chapter 3: The Threat Landscape **25**

The Actor Landscape 26

AI as Force Multiplier 35

What Adversaries Are Actually Attacking 40

Chapter 4: What Success Looks Like for the Adversary **43**

Five Conditions for Adversary Success 44

The Mechanisms of Arrival 46

The Integrated Architecture 52

The Measurement Gap and What Comes Next 55

Part II: The Defence ***56***

Chapter 5: Three Objectives, Six Layers **56**

Six Layers Between Two Foundations 58

Mapping the Cognitive Advantage Triad to the Architecture 64

A Note on Analytical Perspective 66

The Systems-Theoretic Rationale 66

Chapter 6: The Lower Foundation: Social Infrastructure and Societal Resilience **68**

Connection as the Root of Cognitive Resilience 68
Emotional Self-Regulation as Foundational Resilience Infrastructure 70
Building the Foundation: Education, Culture, Service, and Civilian Capacity 73
The Vocabulary of Defence and the Whole-of-Society Requirement 76

Chapter 7: From Resilience to Response 79

The Resilience-Only Trap 79
Active Defence: Detection, Attribution, Exposure, Cost Imposition 81
The Three-Tier Offensive Framework and Democratic Constraints 84

Part III: Primary Case Studies 90

Chapter 8: Germany 90

Threat Actors and Methods 91
The AfD as Parliamentary Vector 94
What Makes Germany Distinctive: Three Pillars 97
Coordination Architecture 99
The Bundeswehr's Cognitive Doctrine 101
Honest Limitations 103
Layer Mapping 106
Partner Landscape 107

Chapter 9: Canada 110

Threat Actors and Methods 112
The United States 113
The Alberta Convergence 113
What Makes Canada Distinctive: Three Pillars 118
Coordination Architecture 121
Honest Limitations 121
Layer Mapping 124
Partner Landscape 125
Canada's Unique Opportunity 127

Chapter 10: The EU and NATO 131

The EU as Regulatory Power 132
NATO's Cognitive Warfare Doctrine: From Concept to Capability Gap 133
The Convergence and the Gap 135
Honest Limitations 137

Layer Mapping 139
Partner Landscape 140

Part IV: Collective Security for the Cognitive Domain 142

Chapter 11: The Fracturing Alliance 142

Collective Defence, Collective Security, and the Rupture 144
Disaggregating the US Paradox 145
The Endogenous Threat: Cognitive Stress from Within 147
What the Fracturing Alliance Is Destroying 151
Building for Resilience: What the Coalition Architecture Requires 152

Chapter 12: The Idea Worth Defending 156

The Signs the West Missed 157
The West is More Than Democracy 158
Canada's Role in the West 159
The Deliberate European Project 161

Chapter 13: The Canada-Germany-EU Corridor 163

The Scaffolding Is Already There 163
The Institutional Scaffolding 163
The Operational Gap 164
The Bilateral Anchor 165
The Defence-Industrial Dimension 167
What the Corridor Enables 168

Part V: Recommendations 171

Chapter 14: Recommendations for Germany 171

Recommendation 1: Close the Integrated Situational Awareness Gap 171
Recommendation 2: Establish a Russia-Vulnerability Mapping Programme 172
Recommendation 3: Resource the VIGINUM-Style Agency 172
Recommendation 4: Reform the Bundeswehr's Cognitive Doctrine 173
Recommendation 5: Expand the Canada-Germany Digital Alliance into the Cognitive Domain 174
Recommendation 6: Build the Coalition of the Willing on Democratic Cognitive Defence 175
Recommendation 7: Defend and Modernise the Politische Bildung Infrastructure 175
A Coherent Institutional Package 176

Chapter 15: Recommendations for Canada 178

The Canadian context: diagnostic and methodological foundations 178
Recommendation 1: Complete Rapid Response Mechanism Canada 181
Recommendation 2: Establish a dedicated foreign intelligence service 181
Recommendation 3: Modernise the Communications Security Establishment 182
Recommendation 4: Build the regulatory architecture for data sovereignty and platform accountability 183
Recommendation 5: Build digital sovereignty infrastructure alongside regulatory architecture 185
Recommendation 6: Increase cognitive defence coordination architecture across levels of government 186
Recommendation 7: Treat emotional self-regulation as Layer 1 cognitive defence infrastructure 188
Recommendation 8: Establish a Canadian Cognitive Defence Agency 190
Recommendation 9: Build Canada's European cognitive defence partnerships 192
Recommendation 10: Create a doctrine of Free Press and Information Peacekeeping 200
A coherent architectural package 203
Closing 204
Endnotes 205

Chapter 16: Recommendations for the European Union 207

Recommendation 1: Resource the Regulatory Architecture 207
Recommendation 2: Operationalise the FIMI Deterrence Playbook 208
Recommendation 3: Sharpen the FIMI Toolbox 208
Recommendation 4: Close the Domestic Gap 209
Recommendation 5: Build the External Coalition 210
Recommendation 6: Build the Layer 1 Foundation 211
A Coherent Architectural Package 212
Endnotes 212

Chapter 17: Recommendations for Democratic Cooperation 213

Recommendation 1: Operationalise the FIMI ISAC and the European Centre for Democratic Resilience as the architecture of collective democratic cognitive defence 214
Recommendation 2: Extend the EU regulatory perimeter to like-minded partner democracies 215
Recommendation 3: Adopt whole-of-society security frameworks that name the cognitive domain 216
Recommendation 4: Treat defence-industrial cooperation as cognitive sovereignty 217
Recommendation 5: Sustain the American democratic ecosystem as a collective commitment 218
Recommendation 6: Treat Ukraine as the operational anchor 219
A coherent architectural package 220
Endnotes 221

Conclusion 222

ANNEXES *228*

Annex A: Note on Further Research **228**

Annex B: Key Concepts and Terms **229**

Definitional Approach: Maximalist versus Minimalist 229

Governing Concepts 229

Core Concepts 231

Key Manipulation Techniques 239

The following terms describe specific operational techniques documented in this report's field research and open-source analysis. Environment-Shaping Techniques 239

Institutional and Practitioner Vocabulary 246

Annex C: Methodology and Interview Base **253**

Acknowledgements

This report was authored by Elizabeth Anderson. Ambassador Eitvydas Bajarūnas served as Distinguished Advisor to the report.

The author conducted research interviews across Europe and Canada between November 2025 and April 2026. Over one hundred interviews were conducted in the course of the research. All interviews were conducted off the record, unless the interviewee specified that they would prefer to be cited. Where on-record attribution was granted, it appears in the endnotes. Where it was not, contributions are referenced by role and vantage, to protect the candour of the research and the working relationships that made it possible.

The author is extremely appreciative of every interlocutor who lent their time and provided their insight. The quality of this report could not have been achieved without the tremendous depth of insight they offered.

The report was produced with the support of Konrad-Adenauer-Stiftung Canada.

Executive Summary

Democracy has one non-negotiable precondition: citizens must be capable of forming genuine political preferences and acting on them freely. Every other feature of democratic governance, every election, every law, every institution, depends on that precondition holding. Remove it, and the institutions remain standing while the substance they were built to protect is gone.

Cognitive warfare is the form of conflict designed to remove it. It does not aim to stuff ballot boxes or topple governments. It manipulates the information environment and the democratic processes through which citizens form every political judgment they make, and quietly degrades the conditions under which genuine belief is possible: flooding the environment with uncertainty until exhaustion displaces engagement, and severing the connections between citizens and the institutions and shared realities that make democratic participation meaningful. This is a different category of conflict.

The democracies that understand this are the ones surviving sustained attack. Ukraine has demonstrated it at the highest possible stakes: it is surviving a full-scale assault by a larger aggressor, not primarily through military hardware but through what this report calls Layer 1, the social infrastructure of cultural mobilisation, shared identity, and bonds of connection and trust that no adversary operation has yet been able to break. The democracies that do not understand it are discovering, too late and too slowly, that the institutions of governance can still remain, while the substance of democracy is already gone.

Liberal democracies have invested significantly in their social systems, their public institutions and processes, and their conventional and cyber defence capabilities. What they have not yet fully understood is the scope of what cognitive defence actually requires: the epistemic foundations on which all of those investments depend, and the social infrastructure that sustains the conditions for genuine democratic participation.

The political class has not been inattentive. Canadian Prime Minister Carney described the current moment in January 2026, at the World Economic Forum in Davos, as a fundamental rupture in the international order, the most significant since the end of the

Second World War. Germany under Chancellor Friedrich Merz has responded to that rupture with its most consequential security pivot in a generation: €500 billion in infrastructure and defence investment, new legislative authorities for cyber operations, and the activations of Germany's National Security Council for the first time. Both Canada and Germany have understood the kinetic and economic dimensions of the rupture described by Prime Minister Carney. Neither has yet built the institutional architecture to address its cognitive dimension. That is the gap this report exists to close. This is not just a Canadian gap or a German gap. It is a democratic gap.

This report is a call to recognise that cognitive warfare is not a peripheral or emerging threat. It is the primary competitive domain in which authoritarian states or non-state actors are challenging democratic societies right now, at scale, at low cost, and with growing sophistication. Russia, China, and aligned actors are conducting continuous operations targeting not just elections but the trust, social cohesion, and political will that democracy depends on. They are doing so in an information environment and democratic processes that democratic societies built for openness and that adversaries have now learned to exploit with precision and little attribution.

This report presents a six-layer framework for democratic cognitive defence developed by the author, following more than 100 interviews with experts across fifteen countries and within EU and NATO institutions. The framework draws on engagement with the EUISS cognitive resilience literature and the NATO Chief Scientist cognitive warfare research programme without being derived from either; the architecture, the dual-foundation structure, and the layer-by-layer mapping are original to the author. It draws on the institutional experience of the democracies that have built the most credible responses: Finland, Sweden, Estonia, Lithuania, Ukraine, and others. The framework is not theoretical. It considers what leading democracies have actually constructed, and it positions Canada, Germany, and their allies not as pioneers designing in the dark, but as late adopters of proven models.

The framework rests on two foundations. The lower foundation is social infrastructure: the bonds of connection, trust, and shared identity that make whole-of-society defence not just a concept but a lived reality. The upper foundation is political will: the sustained

institutional commitment to treat cognitive defence as a continuous obligation rather than an episodic response to the next crisis.

On those foundations sit six operational layers covering: individual resilience, information environment integrity, platform accountability, detection and attribution, active defence, and sovereign response capacity. No single layer is sufficient. The threat operates simultaneously across all of them.

The report concludes with specific recommendations for Canada, Germany, the European Union, and allied cooperation. It advocates for a corridor of cooperation between Canada, Germany, and the EU whose institutional scaffolding is already in place but whose operational utility has not yet been structurally cemented. It also addresses the fracturing of the broader alliance architecture and the need for democracies to build cognitive defence capacity that does not depend on the assumption of goodwill of any American administration.

NATO was built around more than military hardware. It was built around a political covenant: the shared conviction that the freedom to choose, the rule of law, the market economy and the dignity of the individual are worth defending collectively. Cognitive warfare attacks that covenant directly and invisibly. Defending it requires that democracies understand the threat for what it is, build the architecture to address it, and find their way back to the connection with each other and with the values that make their societies worth defending.

The world of the past is not coming back. What comes next will be shaped, in part, by the choices democratic allies make now, in the window of opportunity that remains open but is inexorably closing. The democracies that wait to act will discover, too late, that the ground on which democratic life depends does not give way all at once. It gives way gradually, and then completely. This report is the argument for making those choices, and the architecture for making them count.

Part I: The Stakes

Chapter 1: The Target Is the Mind

Democracy has one non-negotiable precondition: citizens must be capable of forming genuine political preferences and acting on them freely. Every other feature of democratic governance, media freedom, elections, accountability, the rule of law, the mandate that allows governments to act, depends on that precondition holding. Remove it, and the institutions remain but the substance they were built to protect is gone.

For years, with increasing sophistication and at exceedingly low cost, foreign actors have been working to remove or compromise it.

They have gone beyond simply seizing ballots or padding voter rolls, and have instead undertaken something more efficient than that. They have found success by entering the information environment and democratic processes, including elections, and quietly shaping what feels true, what feels threatening, who feels trustworthy, and what feels worth defending. They do not need to change what citizens believe. They need only to degrade the conditions under which genuine belief is possible: to flood the environment with uncertainty until exhaustion displaces engagement, and cynicism displaces the social trust on which democratic life depends. When that threshold is crossed, leaders cannot govern because they can no longer draw a genuine mandate and legitimacy from the people they are meant to represent.

Any citizen who scrolled through their feed this morning made dozens of small judgments shaped by that architecture. They are the voters who will decide the next election.

In 2025 alone, the European External Action Service, the EU's diplomatic service, documented 540 foreign information manipulation incidents targeting more than 100 countries. One in four involved AI tools and affected close to 200 organisations, including NATO, traditional media, and heads of state. The author's own field research found that across democratic governments individual officials frequently recognised the threat in principle, while their institutions had not yet built architecture proportionate to it, and in

some cases, believed existing frameworks were sufficient. We find them to be structurally inadequate.

The UK House of Commons Foreign Affairs Committee, reporting in March 2026, described liberal democracies as “sitting ducks.”[1] They are largely correct, with the exception of some frontline states that have developed practical counter-manipulation structures.

Cognitive warfare is the deliberate targeting of how people perceive, reason, and act. The strategic objective is to degrade the social trust and political will on which democratic governance depends. The tactics are not new: states have sought to manipulate the beliefs and behaviours of adversary populations for centuries. What has changed is the scale of risk that non-democratic states are willing to accept, and the magnitude of their operations. Digital platforms and artificial intelligence have expanded the scale and engineered the individual specificity of these operations to a degree that was not previously possible, at a cost that is next to nothing for the adversary. Because cognitive warfare targets society as a whole, it must be met with a whole-of-society response. This report sets out how democracies can build such defence.

Readers approaching this report from a NATO institutional background will note that the Alliance has developed its own working definitions through the concept development process at Allied Command Transformation. The MC-endorsed NATO working definition frames cognitive warfare as the fight for cognitive superiority, comprising deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain and protect cognitive advantage. Cognitive advantage is broken into three components: narrative advantage (dominance over perception and interpretation), psychological advantage (dominance over an adversary’s cohesion, morale, performance and will to fight), and decision advantage (dominance over an adversary’s situational understanding and decision making). These definitions are NATO unclassified working definitions not yet through the NATO Standardisation Office, provided to the author through field research at Allied Command Transformation, May 2026. The report’s analytical definition is broader: it encompasses the full threat architecture including the civilian cognitive environment and social infrastructure layers that military doctrine addresses only partially. The two frameworks are complementary.

The NATO definitions establish the institutional frame within which the Alliance is operationalising its response. This report's analytical definition captures what is happening to democratic societies, including what falls outside any military frame. The civilisational stakes were named with precision more than four decades ago, before the cognitive warfare frame existed and before the digital tools that now operationalise it had been imagined. Writing in 1984 from Parisian exile about what Russian power had done to Central Europe, Milan Kundera formulated what was at stake in terms only a Czech writer who had lived through Soviet occupation could bring: "Russian totalitarian civilization is the radical negation of the West as it emerged at the dawn of the Modern Age, a West founded on the thinking, doubting self, and defined by cultural creation as the expression of that unique and inimitable individual ego."[2] Forty years later, the methods have changed; the negation Kundera named has not. What cognitive warfare ultimately targets is the doubting self on which democratic citizenship rests, and the social conditions under which that self can form. The architecture this report proposes is, at its foundation, an architecture for protecting the conditions of selfhood that make democratic life possible.

Defining the Domain

Cognitive warfare is used during both war and peace, which most democratic governments have failed to understand. Our adversaries do not observe the same distinction. We are already in a state of sustained geopolitical and geoeconomic competition with our adversaries, and the goal is to degrade us before ever needing to go to war, to achieve those same strategic objectives. In *The Art of War,* Sun Tzu wrote that "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting."[3] Two thousand years later, it remains the animating logic of cognitive warfare. As Lawrence Freedman, Emeritus Professor of War Studies at King's College London, has argued, strategy at its core has always been about shaping the behaviour of others through the management of their perceptions and expectations, a framework that positions cognitive warfare not as a novel threat category but as the contemporary expression of the oldest strategic logic.[4]

One further precision matters for how we name this threat throughout the report. Calling cognitive warfare a war, rather than a form of warfare, risks playing into adversary

framing. We believe the correct analytical frame must communicate severity without conceding strategic ground. We are not at war. We are in a state of sustained hostile competition in which adversaries are waging warfare continuously, below the threshold of kinetic force (albeit very close as in the case of sabotage operations), exploiting precisely the gap between those two things. Democracy requires individual citizens to believe in their information environment enough that they are reasonably confident in their ability to decide about what they want their future to be. A democracy that has lost control of its information and narrative environment to such an extent that citizens can no longer know what they truly believe will cease to have a functioning democracy. This will not happen with a loud bang, but through a long-drawn-out process that risks passing a threshold of no return. This is what liberal societies must prevent.

Military doctrines have long organised themselves around domains perceived to have a distinct sphere of military operations: land, sea, air, and, more recently, cyber and space. Each domain designation carries operational weight. It means dedicated doctrine, assigned command responsibility, resourcing that reflects strategic priority, and training architecture built around domain-specific threats and conditions. The cognitive domain, by which this report means the arena in which perception, reasoning, and will are deliberately targeted as strategic objectives, meets every criterion for domain recognition. Its operating environment is distinct from the information ecosystem that serves as its medium. Its threat actors are identifiable. Its effects are measurable, if imperfectly. And the defence requirements it generates, cannot be disaggregated across existing domains without losing what is essential: that the target is not a system, a territory, or a network, but the human mind and the social conditions under which it functions. Conceptualizing the cognitive domain as such is not a rhetorical move. It is the precondition for building the architecture proportionate to the threat.

The cognitive domain has no geography, and it operates through open societies in ways it cannot in closed ones. Closed societies control what their citizens can see, while directing the same operations outward. When an AI-generated fake image of military equipment hidden inside an Iranian school circulated on Instagram the day before a real US strike on a different Iranian school , democratic citizens, journalists, and governments

around the world were already operating inside a pre-shaped information environment. Cognitive operations conducted in one country land in every open society on earth.

In this report, we adopt the maximalist definition: cognitive warfare encompasses any operation whose primary strategic objective is to affect how people perceive, reason, and act, regardless of means employed. As Claverie and du Cluzel establish, the cognitive effect is not a by-product of action but its very objective.[5] The distinguishing criterion is strategic intent. Operations with cognitive effects but other primary objectives are not cognitive warfare under this definition. A definition too narrow to encompass what adversaries are actually doing is not a definition at all.[6]

A more operationally specific working definition has been developed by NATO Allied Command Transformation, though it has not yet been approved at the political level by the Alliance. ACT defines cognitive warfare as "the fight for cognitive superiority," with contesting in this environment comprising "deliberate, synchronized military and non-military activities throughout the continuum of competition designed to gain, maintain and protect cognitive advantage." The associated full-spectrum approach is defined as "an approach integrating military, government, and societal systems into a coordinated effort across the continuum of competition," synchronising actions and leveraging "diplomatic, informational, military, economic, financial, intelligence, and law enforcement tools to deter, disrupt, or destroy adversary capabilities and influence while building population resilience."[7] The two definitions are compatible. The ACT working definition is the operational frame; the maximalist definition adopted by this report is the analytical frame. The ACT working definition captures what adversaries are doing in synchronised, deliberate, full-spectrum form. The maximalist definition adopted here is broader in scope: it encompasses the ACT working definition while extending to operations whose primary strategic objective is to affect how people perceive, reason, and act regardless of whether the means employed are deliberate, synchronised, or military. The broader frame is necessary because a substantial share of operations producing cognitive effects against democratic societies are conducted by actors outside the ACT working definition's synchronised state-actor frame: proxy networks, economic opportunists, ideological aligned non-state actors, and platform architectures whose effects on cognition are systemic regardless of intent.

ACT further disaggregates the objective of cognitive warfare into cognitive advantage, defined as “ongoing operations, activities, and efforts to continuously shape the cognitive dimension,” comprising three components. Narrative advantage is “the degree of dominance gained over perception and interpretation, including legitimacy and strength, compared to an adversary.” Psychological advantage is “the degree of dominance gained over an adversary’s cohesion, morale, performance and will to fight.” Decision advantage is “the degree of dominance gained over an adversary’s situational understanding and decision making.”[8] These three forms of advantage are the operational objectives adversaries pursue and the operational objectives democratic cognitive defence must deny.

Four Vectors, One Architecture

Cognitive warfare operates through four interlocking vectors. The **message vector** exploits real grievances: historical wounds, identity fractures, institutional failures, social disparities. It works to weaponise that which already exists rather than inventing it. Fiona Hill, former Senior Director for Europe and Russia on the US National Security Council, has documented how Russia’s cognitive strategy targets pre-existing democratic vulnerabilities rather than manufacturing new ones, a logic that explains why the most effective operations feel authentic to their targets.[9] The **messenger vector** extends reach without leaving fingerprints: state media such as Russian RT and Chinese CGTN, bot networks, influencers whose audiences do not ask who funds them, and platform algorithms distributing content without any adversary needing to direct it. The **medium vector** is the architecture that underpins the message: platforms engineered for engagement, where engagement is maximised by fear, outrage, and division. A citizen might want a bowl of ice cream but they also know that ice cream all the time is bad for their health. Similarly, they want a healthy information diet, and what they are receiving has been engineered without their consent. The **audience vector** is the targeting layer. Adversaries do not target randomly. They target those whose emotional regulation is already under strain: diaspora communities facing transnational repression, individuals experiencing economic precarity or social exclusion, men experiencing social marginalisation who are offered belonging in online spaces while radicalising narratives are embedded within that community architecture, and young people navigating identity

formation precisely because the need for belonging during adolescence creates exploitable openings.

What adversaries are targeting, across all of these groups, is not a political preference. It is something far more fundamental: the basic human needs that every person carries, for safety, belonging, and connection. When those needs are under sustained threat, the capacity for deliberative democratic reasoning degrades. In Chapter 4 we examine that mechanism in full. Here it is enough to say that adversaries are not attacking what citizens think. They are attacking the conditions under which citizens can think at all.

These four vectors form an architecture whose combined purpose is not persuasion but a specific neurological state. A population flooded with uncertainty and chaos becomes desperate for certainty, willing to accept forms of governance it would otherwise reject. That is adversary success: not conversion, but exhaustion. Adversaries also manufacture the perception that distrust is universal, so that citizens who privately hold democratic values believe, falsely, that everyone around them has already abandoned them. They do not need to change what people believe. They need to change what people believe about other peoples' perception of their lived reality. Against this architecture of exploitation, media literacy is insufficient. The defence must operate at the level of the human being, not the content. This is what this report means by cognitive defence.

Cognitive Sovereignty and the Case for Democratic Defence

The argument of this report can be most precisely framed as a call for cognitive sovereignty, i.e. the sovereign capacity of democratic citizens to form genuine political preferences free from coercion. Economic warfare targets what democracies can do. Cognitive warfare targets whether their citizens will sustain the political will to do it. When leaders maintain clarity and consistency in their reasoning under sustained pressure, they signal that democratic participation requires exactly that steadiness. The cognitive defence architecture this report recommends begins at that political level and runs all the way down to the emotional regulation capacity of individual citizens.

Protecting the information environment in which citizens form genuine political preferences is the first obligation of any government that takes democratic legitimacy seriously. A democracy whose citizens cannot do this does not fail dramatically. It hollows

out quietly, crossing thresholds that cannot be undone, until one day the institutions remain but the liberal values they were built to protect has disappeared.

Endnotes

1 UK House of Commons Foreign Affairs Committee, Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy, HC 703 (London: House of Commons, 27 March 2026)

2 Milan Kundera, 'The Tragedy of Central Europe,' *The New York Review of Books*, 26 April 1984, translated from the French by Edmund White.

3 Sun Tzu, The Art of War, trans. Samuel B. Griffith (Oxford University Press, 1963).

4 Lawrence Freedman, *Strategy: A History* (Oxford University Press, 2013), esp. Part I; and *The Future of War: A History* (PublicAffairs, 2017).

5 Bernard Claverie and François du Cluzel, 'Cognitive Warfare: The Future of Cognitive Dominance,' NATO Allied Command Transformation, 2022.

6 Elisabeth Dick, 'Defining Cognitive Warfare: Maximalist versus Minimalist Approaches,' Netherlands Defence Academy, December 4, 2025.

7 NATO ACT Cognitive Warfare Definition, https://www.act.nato.int/activities/cognitive-warfare/

8 ibid

9 Fiona Hill, There Is Nothing for You Here: Finding Opportunity in the Twenty-First Century (Mariner Books, 2021); and Hill, 'Putin's Strange Victory,' Foreign Affairs, 2021.

Chapter 2: Why Democracies Are Vulnerable

Cognitive warfare succeeds against democracies not only because adversaries are skilled, but because democracies have built conditions that make them structurally exploitable. Understanding those conditions is the analytical precondition for building defences against them.

Structural Openness and Its Costs

Democracy is built upon a foundation of openness. Free expression protects malicious speech alongside legitimate discourse. Such openness cannot be secured without becoming authoritarian. The legal standards democracies have built to protect citizens from state overreach are precisely the standards that constrain their ability to respond to operations that exploit those same protections. This is a structural condition to be understood and designed around.

The vulnerability runs deeper. Democratic governance depends on citizens who can tolerate uncertainty, revise their views, and hold competing perspectives simultaneously. The world operates in shades of grey, and democracy specifically requires citizens capable of sitting with that complexity, of maintaining good faith engagement with those who hold different views, and of reaching provisional judgments without shutting down further inquiry. Cognitive Load Theory posits that the mind can only process a limited amount of information at once. Bounded rationality is the principle that human decision-making is constrained by available information and cognitive limits. Both establish that the human mind operates under strict limits of attention and processing capacity.

When political realities exceed those limits, individuals do not respond by thinking harder. They simplify, often at the cost of accuracy. Under stress or sustained threat, the tolerance for ambiguity collapses further: people become more prone to holding firm in their own sense of right and wrong, less able to see nuance, and more receptive to the kind of definitive answers that offer immediate psychological relief even when they foreclose the complexity democracy requires. Adversaries understand this. They do not need to convince populations of specific falsehoods. They need only exhaust their capacity for complexity. The goal is not to win the argument but to make argument itself feel unbearable or too complex, and to make truth itself feel unreachable.

The Platform Problem

The information environment in which this exploitation occurs was built by private companies. The structural inflection point is identifiable: the 2018 shift to engagement-based algorithms fundamentally altered the information environment by incentivising sensationalised content at scale. One major social media platform generated approximately $16 billion in a single year on advertising it assessed with reasonable confidence was fraudulent.[1] The structural incentive to allow harm because the platform benefits from it is the enabling environment adversaries then exploit. This is the business model.

Democracy has always required a town square: a shared space where citizens encounter and contest different ideas in an effort to form collective judgments. In the digital age that town square has become privately owned. The platforms that have inherited this function were built for profit, not the public good. US President Franklin Roosevelt warned in 1938 that "the liberty of a democracy is not safe if the people tolerate the growth of private power to a point where it becomes stronger than their democratic state itself. That, in its essence, is Fascism."[2] The platforms that now govern the information environments of democratic societies are not subject to democratic accountability. They are primarily motivated by shareholder returns. Democracies cannot fully flourish under this model, and pretending otherwise is the first mistake of any cognitive defence architecture that assumes platforms will voluntarily act against their own financial interests. The problem extends beyond indifference to active harm: research published in *Science* in March 2026 found that AI sycophancy, the tendency of these systems to affirm, flatter, and agree with users rather than challenge them, is widespread across eleven state-of-the-art models and is demonstrably harmful. AI tools optimised for engagement actively decrease prosocial intentions and promote user dependence.[3] A platform architecture designed to maximise engagement produces responses that tells citizens what they want to hear. That is the structural opposite of the epistemic friction that democratic deliberation requires. The scale of the deliberate choice involved is documented. A BBC investigative report published in March 2026, drawing on more than a dozen whistleblowers and internal company documents, found that Meta made a senior management decision to allow more borderline harmful content, including misogyny and conspiracy theories, into

user feeds in order to compete with TikTok on engagement. This was following internal research that already confirmed that the algorithm “presumes users like content that outrages them and want more of it.”[4] The same investigation found that TikTok systematically prioritised cases involving politicians over reports of child sexual blackmail and terrorism recruitment, in order to maintain relationships with governments and avoid regulation. These are the decisions of profit-seeking corporations that have studied the harm, confirmed it, and chosen to profit off of it regardless.

The adversarial information infrastructure therefore does not require a state actor to construct it. In 2016, two individuals discovered that highly sensationalised content generated advertising revenue, which incentivised an entire ecosystem of similar operations. That ecosystem evolved from sensationalised political content into scam architectures and eventually into supply-chain infrastructure for serious organised crime. States then exploit existing infrastructure rather than constructing their own. This is the mechanism by which the platform problem and the state actor problem interact: adversaries are effective not because they are creative but because they are opportunistic. They operate in an environment that private actors have already made hostile to epistemic health.

The consequence for democratic discourse is direct. The information environment has become so saturated with synthetic, sensationalised content that citizens no longer know what to believe. The questions that now accompany any piece of information – Is this real? Is this AI? Who is behind this? – are warning signs of collapse. A democracy requires citizens who can reach shared judgments about reality. An information environment engineered to maximise outrage and division, and to make truth itself feel perpetually contested, does not produce those citizens. It produces division and paralysis.

The structural basis for this vulnerability is more precisely located than the platform framing suggests. Field research synthesis and the peer-reviewed literature converge on a finding that complicates the dominant narrative: time on social media does not reliably predict affective polarisation. Job loss does. Economic dislocation, experienced as a rupture in the social contract that structures dignity and daily meaning, predicts affective polarisation with a lag of several years. Adversary operations do not manufacture this

condition. They find it pre-existing and amplify it. No amount of media literacy investment can close a vulnerability that originates in economic experience rather than information exposure.

Trust, Pluralism, and Speed

High-trust societies are more efficient democracies, and evidence suggests they are also happier. The World Happiness Report documents a sustained decline in wellbeing in the United States, Canada, Australia, and New Zealand, the only major democracies where younger generations report lower life satisfaction today than in 2006-2010. In most of the world, younger people are happier than they were twenty years ago. In the anglosphere, they are not. The report points directly to social media architecture as a contributing driver of this divergence.[5] The institutional implication is significant: the social trust on which democratic governance depends is being actively degraded, and the mechanism is partially the same platform architecture that adversaries exploit. The contrast is sharpest with Finland, which has ranked first in the World Happiness Report for eight consecutive years and whose high-trust social model is examined as a benchmark throughout this report.

Institutional trust is essential for democratic governance. It enables citizens to accept collective decisions from institutions they did not individually control. Adversaries do not need to make citizens distrust specific institutions. They need to make distrust feel like the rational default.

Pluralism, similarly, is simultaneously a democratic value and an opportunity for adversaries. Diverse societies have more fault lines to exploit. Legitimate grievances, historical wounds, and economic anxieties are not manufactured by adversaries. They are real, and that reality is what gives adversaries their traction. Hannah Arendt, writing in the *Origins of Totalitarianism*, observed that totalitarian movements find their most fertile ground in populations that have become isolated, people who have lost their connections to community, whose shared social fabric has frayed, and who have retreated from public life into private disengagement.[6] The cognitive warfare threat is, at its most basic, a problem of connection and social fabric before it is a problem of information. A message that lands because the underlying condition is a genuine one is

harder to counter than a fabricated one, because countering it requires acknowledging the grievance while refusing its weaponisation. That is a difficult political task for which most democratic governments are poorly equipped.

The speed asymmetry compounds both vulnerabilities. It is not a new challenge. In 1710, English writer and cleric Jonathan Swift wrote: “Falsehood flies, and the Truth comes limping after it.”[7]

Disinformation spreads faster than correction. Adversary operations are designed to generate immediate emotional arousal; correction requires the slower cognitive process of fact-checking, contextualising, and revising. Democratic deliberation, by design, is slow. First-mover advantage in narrative space is structurally built into the threat environment that democracies face.

Gaming platforms represent a distinct and underweighted vulnerability. Unlike social media platforms, which insert adversary content into existing civic discourse, gaming platforms and adjacent communities on Discord and streaming services build immersive environments in which young men, in particular, spend thousands of hours in communities curated around shared identity. Adversaries have systematically exploited these environments to introduce political radicalisation before participants have developed the media literacy that text-based propaganda would require. The pathway from gaming community to extremist recruitment is documented across multiple national security services and represents a Layer 1 vulnerability that democratic governments have not yet addressed at the institutional level.

Beneath the speed asymmetry lies a deeper structural vulnerability: the capacity of individual citizens for emotional self-regulation. Adversary operations are not designed primarily to persuade. They are designed to provoke. A citizen in acute emotional arousal is neurologically less capable of the deliberative engagement that democratic governance requires. The seizing-and-freezing mechanism described in social psychology holds that under conditions of acute threat, the mind reaches for the first available certainty and closes off further inquiry. Adversaries understand this. They engineer it. Building population-level emotional regulation capacity is not a therapeutic aspiration. It is cognitive defence infrastructure at the deepest available layer.

The Mandate Vacuum

A third structural vulnerability is institutional: democracies have systematically failed to classify what requires active defence. Norway did not designate petroleum as critical infrastructure until after the full-scale invasion of Ukraine, despite petroleum representing approximately half of its annual budget. The Ministry of Petroleum resisted the designation for years to avoid it being seen as a security asset. The same pattern is documented across energy, telecommunications, and digital infrastructure in multiple democracies: the gap between what is strategically and economically important and what is classified as requiring active defence is itself an adversary opportunity.

A parallel mandate vacuum exists at the level of population rather than infrastructure. Democracies with significant multilingual or diaspora populations face an additional structural vulnerability: awareness of cognitive threats travels poorly across linguistic communities, creating exploitable seams that adversaries can activate without triggering counter-response in other parts of the same society.

Why Reactive Response Is Insufficient

Field research synthesis from the platform governance and public health contexts offers a clarifying analogy for why reactive counter-disinformation fails as a primary response. The spread of disinformation follows patterns structurally similar to viral spread: upstream interventions address conditions that make populations susceptible; midstream interventions build resilience in those exposed; downstream interventions treat active spread. Purely reactive responses operate only downstream, treating the symptom without addressing transmission conditions. No public health system treats infectious disease purely through clinical response while ignoring sanitation, vaccination, and the social determinants of health. Cognitive defence frameworks that focus exclusively on counter-messaging are making the equivalent error. The adversarial information environment has endogenous drivers, platform incentive structures, cognitive vulnerabilities, trust deficits, and legitimacy gaps, that persist independently of what any external actor does. The architecture must address them simultaneously. The six layers that follow are that architecture.

Endnotes

1 Jeff Horwitz, ‘Meta Making Billions from Fraudulent Ads, Documents Say,’ Reuters, November 7, 2025.

2 Franklin D. Roosevelt, Message to Congress on the Concentration of Economic Power, April 29, 1938.

3 Myra Cheng et al., ‘Sycophantic AI Decreases Prosocial Intentions and Promotes Dependence,’ *Science* 391, eaec8352 (2026). DOI: 10.1126/science.aec8352. Published 26 March 2026.

4 Marianna Spring and Mike Radford, ‘Meta and TikTok Let Harmful Content Rise after Evidence Outrage Drove Engagement, Say Whistleblowers,’ BBC News, 16 March 2026.

5 World Happiness Report 2025, Wellbeing Research Centre, University of Oxford, in partnership with Gallup and the UN Sustainable Development Solutions Network.

6 Hannah Arendt, The Origins of Totalitarianism (New York: Schocken Books, 1951; revised edition 1958), Part III, 'Ideology and Terror.'

7 Swift J: The Examiner No. 14. (Thursday, November 9, 1710). In A Modest Proposal and Other Prose. Barnes & Noble Publishing, Inc; 2004:195.

Chapter 3: The Threat Landscape

Cognitive warfare as a destabilisation strategy is not unprecedented in kind, but is novel in its scale and speed. States have waged influence operations for centuries. Napoleon deployed systematic propaganda. The British Empire manufactured narratives of civilisational superiority. The Soviet Union perfected forgeries, agents of influence, and active measures through organisations including the KGB's Active Measures directorate. Operation INFEKTION, the KGB campaign falsely attributing HIV to US biological warfare, is the direct template for modern health disinformation.

The West is not innocent of this history. The CIA funded front organisations and manipulated elections across Latin America, Asia, and Africa (operations conducted primarily during the Cold War, in the context of active superpower confrontation with the Soviet Union). The UK's Information Research Department, operating from 1948 to 1977, planted stories in foreign media across Western Europe, sub-Saharan Africa, Southeast Asia, and Latin America, with the strategic objective of countering Soviet influence and protecting British interests during decolonisation. France ran influence networks across Francophone Africa through the Françafrique system. Voice of America and Radio Free Europe were built to shape opinion, not merely to inform it.[1]

This history matters for three reasons. Adversaries operate with a sense of entitlement, responding in kind to decades of interference. Audiences in the Global South are often unsympathetic to Western complaints about foreign interference. This has a direct effect on coalition building. Moral clarity requires honesty. Democracies can only credibly defend rule-based order if they do not violate it, or at least acknowledge when they have violated it. That acknowledgment also has operational value. Exploitable fractures become less potent when the grievance behind them has been openly acknowledged.

What has changed these days is the technology. Cold War operations targeted elite networks, took months to execute, and were expensive and episodic. The same operations today target entire populations, execute in hours, cost almost nothing, and are continuous. The strategic objective remains destabilisation: a democracy consumed by internal conflict cannot project power, sustain alliances, or maintain the external commitments that adversaries most want to eliminate.

The Actor Landscape

What distinguishes the current period from earlier eras of great-power competition is the ideological dimension. Hal Brands has argued that today's conflicts are struggles between larger systems rooted in genuinely incompatible views of politics and geopolitics, not merely contests of interest that could be resolved through bargaining. That framing matters. The actors we describe in this section are not just opportunistic disrupters. They are pursuing a coherent project with the strategic objective of delegitimizing democratic governance as a viable system.

Russia is the primary threat in Europe and across the Atlantic. Its doctrine, rooted in the concept of information confrontation and developed by the Russian military and intelligence community, treats cognitive operations as permanent rather than exclusively wartime activity.[2] Core methods include hack-and-leak operations, troll farms, state media amplification through outlets like RT and Sputnik, proxy amplification through domestic sympathisers and elite cultivation, and historical warfare, i.e. the selective deployment of historical narratives meant to undermine the founding legitimacy of target societies. Proxy amplification overlaps with what the research literature codifies as *information laundering*: the process by which foreign-originated narratives are placed in domestic media ecosystems through intermediary channels, typically local outlets, sympathetic political actors, or social media accounts, to obscure their origin and increase their credibility before they reach the audiences they are intended to move. The technique succeeds because of the *external source effect*: a documented psychological pattern in which content is perceived as more credible when it appears to originate from a foreign or external source than when the same content originates domestically. Foreign placement and domestic recirculation form a feedback loop in which the source-laundering and the credibility-laundering reinforce each other. The mechanism by which historical warfare operates in pre-existing cultural memory has been documented at length by Jade McGlynn in *Memory Makers* and *Russia's War*[3], both of which trace the deliberate construction of historical narrative as an instrument of state power inside Russia and as a vehicle for influence abroad. They have fabricated allegations of sexual violence by NATO soldiers against local civilians, which were reused across Lithuania, Estonia, and Germany to undermine NATO legitimacy. A further and distinct method is what Russian

strategic culture calls *vranye* – a ritualistic performance of untruth whose objective is not persuasion but saturation, flooding the information environment with contradictory claims until reliable belief feels impossible. The technique is named in the analytical literature *information overload*: the deliberate flooding of the information environment with contradictory explanations, competing narratives, and high volumes of content to prevent attribution consensus and exhaust verification capacity. The goal is not to persuade but to overwhelm, and the practitioner literature documents it as a distinct operational category alongside persuasion-based disinformation rather than as a variant of it. The detection architecture must identify the saturation pattern itself, not only individual false claims. RAND researchers Christopher Paul and Miriam Matthews identified the structural logic of this approach in their foundational analysis of Russian propaganda, characterising it as high-volume, multichannel, rapid, continuous, and deliberately inconsistent. It is a model that depends on exhaustion. NATO and UK information operations doctrine names the operational logic as the 4Ds: dismiss, distort, distract, dismay. The goal is not to win the argument but to exhaust the capacity for coherent response. A European Commission Joint Research Centre report published in April 2026 gives this evolution a further name: the “fantasy-industrial complex,” a self-organising and loosely coordinated system whose goal is no longer to make individuals believe specific false claims but to distract, generate distrust, and activate anti-democratic norms and authoritarian behaviours. As that report notes, blaming individuals for being misinformed is a misdiagnosis of the underlying cause: the attention economy structurally privileges negative, emotional, and conflictual content not because of adversary design but because engagement maximisation is the platform business model. The adversary does not need to build the architecture. It already exists. A synthesis of the most recent public threat assessments from Nordic and Baltic intelligence services, published by the International Centre for Defence and Security in March 2026, confirms that hybrid pressure has become a baseline condition rather than an episodic phenomenon: cyber operations, disinformation campaigns, sabotage preparation, and influence operations targeting social cohesion are described across seven national assessments as a continuous rather than wartime feature of the European security environment.[4]

The doctrinal foundation Russian military theorists themselves cite is older than the contemporary information environment by decades. The term is *reflexive control*: the practice of conveying specially prepared information to an opponent in order to incline that opponent to make, voluntarily, the decision the initiator wants made. The concept was developed in the 1960s by the Soviet mathematician Vladimir Lefebvre, codified inside Soviet military doctrine through the 1970s and 1980s, and has been the subject of continuous theoretical and operational development inside Russian military thought for over half a century.[5] The objective of reflexive control is not persuasion. It is paralysis. The architecture is designed to overload adversary decision-making with contradictory information, to construct false strategic images that the adversary then acts on, and to make the adversary take self-defeating decisions while believing those decisions reflect the adversary's own strategic interest. The information confrontation doctrine, the 4Ds, *vranye*, the information-overload technique, the firehose of falsehood, the all-platforms architecture, and the historical-warfare method are each operational instantiations of reflexive control. The doctrine names the unifying objective the techniques are calibrated against, and it explains why Western counter-disinformation frameworks built on the assumption that Russia is attempting to persuade audiences of specific propositions miss the point at the foundational level. Russia is not optimising for belief change. It is optimising for adversary decision-making paralysis. The defensive task changes accordingly: the metrics, the detection architecture, and the response posture must be calibrated against the paralysis objective rather than against persuasion metrics. [6]

Two further structural features distinguish Russian cognitive warfare from the disinformation framing that has dominated democratic policy responses. The first is its multigenerational character: the Institute for the Study of War's 2025 primer documents that Russian information operations span decades and geographies, with narratives selectively activated and deactivated over multiple decades to adapt to evolving Kremlin requirements. Effects may surface years after an operation launches. The second is its all-platforms architecture: Russia uses every transmission channel available, including not only media but also conferences, international frameworks, diplomatic channels, foreign media partnerships, journalist training programmes, religious institutions, and individuals operating across all of these as instruments of cognitive warfare. The most

operationally significant religious-institution vector is the Russian Orthodox Church Moscow Patriarchate, which operates as a foreign-policy and intelligence instrument of the Russian state rather than as a religious institution in any meaningful sense, and which is developed in full in Chapter 18. The implication for democratic response is structural. A defence architecture focused only on social-media disinformation will miss most of the operation. The all-platforms architecture is the doctrinal foundation for the information peacekeeping recommendation developed in Part V. Information Peacekeeping was introduced as a concept by Robert Garigue at the Canadian Department of National Defence in 1993 and developed in the contemporary cyber-age context by Dave McMahon; the recommendation in Part V develops a Canadian application in which democratic media presence, cultural diplomacy, and sustained international broadcasting operate as cognitive defence infrastructure on the same architecture adversaries already use.[7]

Ukrainian practitioners working at the receiving end of Russian operations since 2014 have developed the analytical and institutional response that the all-platforms architecture requires. The operational doctrine they describe applies the military-doctrinal framework of kill chains, the standard framework for the sequenced application of kinetic force against a target, to adversary information operations infrastructure rather than to discrete adversary narratives. The argument is that adversary operations have infrastructure with identifiable nodes (production capacity, amplification networks, embedded media properties, financial flows, institutional partnerships, religious-institution channels, journalist training programmes, cultural-diplomacy vehicles), and that the appropriate defensive response is to apply kill-chain methodology to the infrastructure rather than to engage in narrative-by-narrative counter-messaging. Targeting the infrastructure produces durable defensive gains; targeting the narratives produces individual rebuttals that the infrastructure replaces faster than the rebuttals can accumulate. The doctrine is developed at length in this report from the Ukrainian operational vantage, and it is the operational expression of the analytical recognition that Russian operations cannot be defeated through Western-style counter-messaging because the messaging itself is not the operation. The implication for defensive architecture is structural: democracies must build the institutional capacity to identify, target, and disrupt adversary operations

infrastructure inside their own legal and institutional frameworks, recognising that the defensive task is at the infrastructure level rather than at the narrative level.

Russia's objectives are to destroy the existing global order by breaking the transatlantic alliance and the EU as an institution; compromise democracy as institutional order; prevent democratic spread eastward; and, rehabilitate its imperial ambitions. It is clear Russia fears kinetic conflict with a US-backed NATO. Western sanctions have diminished its capacity for economic warfare; energy coercion has accelerated European energy diversification and the delinking of infrastructure. Cognitive warfare has therefore become the cheapest and most effective form of warfare available. Russia's state-controlled media budget is projected to reach ₽146.3 billion (€1.6 billion) in 2026, seven percent higher than in 2025, during a war where Russia is consuming conventional military resources at an unprecedented rate. It has made a deliberate calculation to invest more heavily in the tools it can still use.[8]

Russia has also identified Canada as a named target. Open-source monitoring documents senior Russian officials predicting that Canada will be severed from British influence and absorbed into the United States without military force, and published analysis framing Anglo-Saxon geopolitical dominance as a primary strategic threat to Russia.[9] Belarus functions as a dependent amplifier of Russian cognitive operations, with capabilities largely supplied by Moscow.

China operates on a different and, in some respects, more consequential architecture. Where Russia weaponises infrastructure it did not build, China has built integrated systems where cyber, technology, law, surveillance, and party structure are inseparable. Field research from the NATO StratCom Centre of Excellence captures the distinction with precision. If Russia is the brown bear clawing at the front door, drawing everyone's attention to its attacks right now, then China is the panda that has already come in through the back window and is quietly raiding the kitchen while everyone fortifies the front door. China is investing now to capitalise later, operating more subtly, and building access that it may not yet fully understand how to exploit. The threat to open societies is not primarily cyber intrusion or disinformation in the Russian style. It is the export of a governance model. China implants it in Belt-and-Road agreements. It sells surveillance packages to authoritarian partners. It embeds control mechanisms in smart city infrastructure. And

promotes technical standards designed to normalise authoritarian data governance globally.

Since 2018, China has shifted from centralised state media to what researchers' term Centralisation+: a coordinated system deploying provincial, city, and county-level actors through more than 200 International Communication Centres including overseas branch locations, designed specifically to operate beneath detection thresholds built to track centralised state media.[10] The AI dimension of this architecture represents its most consequential evolution. Systematic testing of Chinese AI models from ten companies across multiple languages, conducted for the Swedish Psychological Defence Agency, found that Chinese foundation models consistently reproduced official CCP narratives, not as identifiable content insertions but as the default baseline of what the system presents as neutral information. It extended well beyond censorship of sensitive topics to subtle guidance on religion, culture, China's global reputation, and international relations.[11] Models from Alibaba's Qwen family of Large Language Models (LLMs) were the most-used base models globally in the first half of 2025, accounting for 39 percent of all fine-tuned models created on Hugging Face, a widely used global platform for sharing and downloading AI models.

A documented operational evolution warrants specific attention. Field research conducted for this report in the Baltic states found, independently and consistently across multiple sources, that China has shifted away from direct influence operations and toward distributing its narratives through Russian information channels. The strategic logic is sound: Russian-language and Russian-adjacent information infrastructure has established reach, credibility within target communities, and deniability that Chinese-language operations cannot easily replicate. The shift was confirmed independently by three separate Lithuanian sources. Attribution frameworks built to identify the originating actor by linguistic or platform signature will misattribute Chinese operations as Russian and Chinese-Russian coordination as undifferentiated Russian activity.

Under current EU rules, European citizens could be encountering Chinese government narratives through AI tools built on Chinese models without any awareness of their provenance. For Canada, the exposure is specific: it has a large Chinese-speaking diaspora population whose primary AI and information tools may be designed with

propaganda embedded at the infrastructure level. Beijing has also integrated deepfakes into a three-track influence operation architecture: smear campaigns against critics using fabricated visual evidence, fake persona networks to amplify Chinese Communist Party (CCP) narratives at scale, and deepfake-enabled electoral interference in democratic elections.[12]

The distinction between is that China represents a digital autocracy, in which digital tools are constitutive elements of governance itself. Russia is better understood as a digitally-enabled autocracy, which deploys digital tools instrumentally and with considerable effectiveness without having built the comprehensive architectural integration that characterises China's model. The distinction matters for democratic defence. China builds systems and exports the model; Russia exploits systems that already exist.

Iran represents a distinct threat profile that has been systematically underestimated in Western cognitive defence frameworks. Iran treats information control as a core instrument of regime survival domestically, and turns the same apparatus outward. Research by Clemson University's Media Forensics Hub identified a network of accounts on X posing as socially conscious British users, likely operated by or on behalf of the Islamic Revolutionary Guard Corps, targeting the Scottish independence debate with content generating over 224 million potential views. The operation's Iranian origin was exposed by physics: when Israel's June 2025 airstrikes caused an internet blackout affecting 95 percent of Iran's connectivity, every account fell silent simultaneously. A Commons intelligence and security committee report confirmed Iran used social media to encourage a Yes vote in the 2014 referendum, establishing that this operation had persisted for over a decade. What the Iranian case illustrates is an important asymmetry: Iran exports cognitive warfare to exploit the open information environments of its adversaries while suppressing those same conditions domestically.[13]

The trajectory of Iran's cognitive operations, however, remains genuinely uncertain. The US-Israel military campaign against Iran's nuclear infrastructure in 2025 has degraded not only Iran's physical capabilities but its broader strategic calculus. Whether the Islamic Revolutionary Guard Corps will intensify its information operations as a tool of asymmetric retaliation, or whether the campaign has disrupted the operational infrastructure on which those operations depend, is not yet clear. What is certain is that Iran's cognitive warfare

apparatus has demonstrated a decade-long persistence and a willingness to target open democratic societies far removed from its immediate neighbourhood. Allied democracies should not assume that military pressure on Iran translates automatically into reduced cognitive threat.

The Iran case has also produced a contemporaneous example of what the research literature describes as the *information alibi*: a pre-emptive narrative planted before an anticipated event to provide ready-made justification or alternative explanation, seeding the information environment before the primary account can establish itself. Following the 28 February 2026 strike on the Shajareh Tayyebeh elementary school in Minab, southern Iran, in which approximately 168 people were killed, most of them schoolchildren, the Trump administration initially blamed Iran for the strike. The Washington Post subsequently reported that the school had been on a US target list.[14] The information alibi functions by preventing attribution consensus: once multiple competing explanatory frameworks are in circulation, audiences default to whichever framing best aligns with their priors, and the question of what actually happened is displaced by the question of which side is more trustworthy. Democratic information environments are particularly vulnerable to the technique because they treat the existence of competing claims as evidence of legitimate debate rather than as evidence of operational manipulation. The information alibi and the liar's dividend, developed later in this chapter, operate together in the cognitive domain. The alibi pre-positions a competing frame for events that have not yet occurred; the dividend ensures that none of the competing frames can be reliably adjudicated once the events do. Each technique compounds the other, and the Minab strike sits at the intersection of both.

A distinct threat category has emerged within the alliance architecture itself: member states whose domestic political alignments, information environment governance, and relationships with adversary states create exploitable seams that external actors can activate without crossing a border. Alliance membership does not equal alignment. The defence framework must account for threats that arrive through the front door as well as those that approach from outside.

The United States is the most politically difficult case to analyse and the most consequential. US-based platforms own the information environment of the democratic

world. Just six companies – Meta, Google, X, Apple, Amazon, and Microsoft – control what allied populations see, share, and, ultimately, believe. No Cold War-era operation ever achieved this position. The Soviet Union at its height could not meaningfully reach into the daily information diet of allied citizens. These six companies are central to people's lives.

The structural problem is compounded by a political one. The current administration has systematically dismantled the United States' own counter-disinformation architecture. The State Department's Global Engagement Center terminated agreements in 22 countries designed to jointly expose foreign information manipulation campaigns, agreements whose former director, James Rubin, described as "a unilateral act of disarmament."[15] The administration's National Security Strategy, published in December 2025, names no state-level adversaries as threats, does not mention the protection of human rights or democracy, and identifies European liberal democracy as the primary enemy ideology. The administration has aligned itself with the same authoritarian narratives that adversaries deploy against democratic cohesion. There is an inherent tension in that combination that cannot be resolved cleanly. We believe it must be said plainly: the leading member of the democratic Alliance has, during this Administration, ceased to function as a reliable partner in the cognitive domain. The evidence of that shift became irrefutable in April 2026, when Secretary of State Marco Rubio signed a cable directing US embassies and consulates worldwide to coordinate counter-propaganda campaigns explicitly through X, the platform owned by Elon Musk, aligned with the Pentagon's Military Information Support Operations. The cable instructs embassies to recruit local influencers to carry US-funded narratives in ways designed to feel organically local rather than centrally directed. As legal scholar Kate Klonick observed in *Lawfare*, a State Department cable endorsing a specific privately-owned platform as a tool of military psychological operations would have been unthinkable before the structural transformation that dismantled, piece by piece, the legal accountability and institutional resilience that once made such a relationship between government and platforms inconceivable.[16] The implications of that reality run through the rest of this report.

Two mechanisms in this typology are systematically underweighted in existing frameworks and deserve explicit naming. The first is the dormant-narrative reactivation

mechanism. Field research from the Swedish Psychological Defence Agency confirms that the same narrative targeting Swedish social services as hostile to Muslim families had circulated in the Swedish information environment more than a decade before the 2021 to 2022 campaign that exploded into international attention and a terrorist attack in Brussels. The narrative did not gain traction in its earlier iterations. What changed was not a new adversary operation but a combination of domestic activist organisation and platform amplification that created the conditions for a pre-existing narrative to detonate. The policy implication is significant: adversaries do not always need to create new operations. They need to identify dormant narratives, often developed or tested in earlier cycles, and wait for the domestic and technological conditions that will make them resonate. A threat detection architecture that focuses only on new narratives will systematically miss this.

The second is the non-state and proxy actor vector, operating through ideologically motivated non-state actors rather than state intelligence services. The Swedish social services campaign involved Islamist non-state actors in the Middle East exploiting Muslim diaspora communities in Sweden through narratives framing Swedish and Western society as inherently hostile to Islam. This threat category is analytically distinct from Russian state operations and from Chinese technology-embedded influence. It operates through genuine community grievances, makes attribution more difficult, and requires a different detection and response architecture focused on community trust-building and integration rather than on technical forensics of adversary infrastructure.

The common thread across this typology is not regime type but behaviour. The defence framework must therefore be actor-agnostic, defined by the nature of the operation, not the identity of the actor.

AI as Force Multiplier

The actors and objectives described above are not new. What has fundamentally shifted since 2022 is the technology. The release of generative AI has altered the economics of cognitive warfare. What previously required troll farms with hundreds of human operators can now be accomplished by small teams with AI tools. Cost per operation has collapsed; scale has exploded; personalisation is possible at population level.[17] AI-generated

deepfakes have been deployed in elections in Slovenia, Romania, Taiwan, India, and Türkiye. They were also documented in Canada's 2025 federal election, where a deepfake of Prime Minister Carney reached millions of views in the days before polling; in Germany's 2025 federal election, where AI-generated campaign content was deployed by domestic political actors; and in Poland, where a deepfake of the Prime Minister circulated during the 2023 parliamentary elections.[18]

Quality now exceeds most humans' capacity for its detection. The European External Action Service 4th FIMI Report confirms that one in four detected FIMI incidents in 2025 involved AI tools, a year-on-year exponential increase. LLMs are now being deliberately groomed by operators flooding the internet with false information to corrupt AI outputs when citizens use them to verify claims. The adversary is no longer only injecting false content into the information environment, it is corrupting the verification infrastructure citizens rely on to navigate it.[19] Field research by the NORDIS Hub network confirms this mechanism is already operating in practice: mainstream AI tools, including ChatGPT, Google Gemini, and Microsoft Copilot, have been found to reproduce Pravda network* narratives when answering questions in Nordic languages, without flagging the provenance of their sources.

A further vector is data poisoning and model poisoning. This is the act of embedding coded narratives into AI training data before deployment, operating entirely outside individual disinformation campaigns and invisible to content moderation frameworks built to detect them. The deepfake saturation objective compounds the liar's dividend which is a term coined to describe how the existence of synthetic media degrades trust in all authentic media.[20] The aim is not to convince everyone that synthetic content is true, but to make the question "Is this real?" close to unanswerable for everyone.[21] The Vanity Fair piece cited above is itself a documented case of the mechanism: unable to secure an interview with Anthropic's CEO, a senior journalist at a major publication fabricated the interview using Anthropic's own AI fed on the subject's published work, essays, and Davos remarks, and presented the result to readers in the style of Raymond Chandler without disclosure until the final paragraphs. Readers could not tell the difference. The

* Pravda Network is a coordinated system of more than 150 pro-Kremlin websites designed to contaminate AI training data with disinformation

condition the liar's dividend describes is no longer hypothetical. It is the working environment of contemporary journalism.

The US-Iran war that began on 28 February 2026 represents the operational threshold at which this trajectory passed from prediction into condition. Within the first week of the conflict, the Reuters Institute, Brookings, Chatham House, and the broader fact-checking community independently reached the same diagnosis: this was the conflict in which generative AI moved from supplementary to central in the information environment of a major war. Fabricated satellite imagery purporting to show damage to US bases, AI-generated video of Iranian missiles striking Tel Aviv, manipulated before-and-after comparisons of US facilities published through Iranian state-aligned outlets, and the documented failure of platform-native AI systems including Grok and Gemini to correctly authenticate AI-generated content circulated alongside real footage in feeds where provenance could not be established in real time. Within three days, X had restricted its Creator Revenue Sharing programme, suspending creators who posted undisclosed AI imagery of armed conflict, a platform response that itself acknowledged the volume had exceeded what existing systems could absorb. The cumulative consequence is the realisation of what cognitive warfare theorists have warned about for half a decade. Democratic populations did not lose access to truth about the Iran war. They lost access to the conditions under which truth-claims can be adjudicated in real time. The architectural prediction of the liar's dividend has become the operational reality of the information environment, and the threshold, once crossed, does not return to normal.[22]

A new threat category has emerged that sits outside the deepfakes-of-individuals taxonomy. It is AI-generated vox-pop content. From the Latin *vox populi*, these man-on-the-street interview videos carry ambient credibility because of the association with journalistic practices. Field research from Ukraine's Centre for Countering Disinformation identified a campaign that deployed entirely AI-generated footage, including faces, the settings, the audio, and the apparent spontaneity. The giveaway, identified on close forensic examination, was that the eyes were clearly AI-generated. But the production quality was otherwise high, and the format was specifically chosen because viewers assume it represents genuine public opinion. As generation quality continues to improve, easy identifiers will disappear.

This threat category requires detection architecture distinct from deepfakes-of-named-individuals: it targets the perception of popular sentiment rather than the reputation of specific people, and the legal and regulatory frameworks designed for the latter do not address the former. Detection requires identifying synthetic ambient detail rather than facial or vocal substitution.

State-designed AI systems represent a distinct and underweighted category of cognitive threat. The Reporters Without Borders Propaganda Monitor Season 2 (launched March 2026) documents China Global Television Network's reach across television, radio and online platforms in over 160 countries, with its radio service operating in 65 languages, the most expansive language service of any radio broadcaster worldwide.[23] The operational model is media capture rather than content manipulation: CGTN does not primarily fabricate, it occupies the information space with volume and credibility, crowding out independent reporting in markets where local journalism is weak. A parallel finding identifies Chinese AI chatbots trained on state-approved datasets and deployed at scale as propaganda infrastructure: the systems do not insert discrete false claims but shape the frame within which users encounter information about contested topics. Canada's specific exposure runs through its Chinese-language diaspora media ecosystem, where CGTN-affiliated outlets operate without the regulatory constraints that apply to domestic broadcasters.

The asymmetric defender problem underlies all of this. Adversaries can focus all their resources on one attack vector at a time while defenders must defend against all conceivable threats simultaneously. Reactive content moderation cannot be the primary instrument against a threat that is outpacing detection. Detection is currently losing the arms race with generation capability. Cyber operations and cognitive operations are increasingly inseparable, combined in documented Russian patterns for maximum psychological effect. Democracies that treat cyber defence and cognitive defence as separate domains risk missing a significant portion of the threat, one that is designed to exploit precisely that institutional gap.

The gap between adversary capability and democratic response is measurable. The US military's Strategic Capabilities Office is developing the Basic Information Awareness

Operations project to build a common technology stack for cognitive domain operations using commercial AI. The programme's chief technology officer stated publicly that the United States "cannot counter adversarial cognitive warfare at machine speed" and is "behind from the technology perspective." That a senior US military official is on record saying this establishes where the arms race stands and why passive resilience is insufficient. This also reveals an uncomfortable structural reality for Allied democracies. The assumption embedded in most existing cognitive defence frameworks is that ally status confers a degree of protection, i.e. the threat to be defended against is adversarial, not friendly. That assumption does not hold today. Allied governments and civil society institutions have been the targets of coordinated US-funded narrative operations.

We believe that the actor-agnostic defence framework recommended in this report is the only coherent response to a threat environment in which the origin of an operation is no longer a reliable indicator of whether it poses a risk to democratic integrity.

The dual-use military-commercial reality of these technologies complicates the regulatory picture in ways that most democratic governance frameworks have not yet absorbed. For decades, the standard assumption was that military technology trickled down into civilian life: the internet, GPS, satellite imagery. What is now occurring is the reversal. Commercial AI systems built for consumer markets are being absorbed into military infrastructure at pace. OpenAI, Google, and Meta each rolled back their own restrictions on military applications of their technologies between 2024 and 2025. According to research by Mind the Bridge and Fincantieri, one in four technology scaleups globally is now classified as dual-use, with investment in that segment jumping 25 percent in a matter of months to reach nearly US$1.2 trillion, and defence-specific AI start-ups alone receiving US$70.8 billion.[24] Canada and Germany cannot treat AI regulation as primarily an innovation and competition policy question while their adversaries, and some of their Allies, are treating the same technology as a weapons development programme. Today's governance gap is now between states that understand that AI regulation is a security matter and states that have not yet arrived at that conclusion. A cognitive defence architecture that addresses AI-generated disinformation while ignoring the military integration of the platforms generating it is addressing the symptom while leaving the system intact.

What Adversaries Are Actually Attacking

The final and most important element of the threat landscape is a meta-threat. Democracy's adversaries are not only attacking democratic information environments, they are attacking the institutional architecture that democracies have built to defend those environments. Reporting by Anne Applebaum documented a coordinated transatlantic campaign targeting the EU's *Digital Services Act*, framed as a free speech issue, using US government funding channelled through think tanks to capture the civil society layer that is supposed to be the DSA's enforcement constituency. The Heritage Foundation was tasked by the Trump administration to identify European think tanks that would receive US government funding specifically to target the DSA. US embassies across Europe coordinated simultaneous postings attacking EU digital regulation. The tool being attacked is the platform-accountability layer of the six-layer defence architecture that this report conceptualises and subsequently recommends. The attack on the tool is itself a cognitive warfare operation.[25]

Germany has faced the same institutional pattern at scale. The 2025 federal election was targeted by Storm-1516, a GRU-connected operation running more than one hundred German-language fake news websites and more than six thousand bot accounts. Following the Germany's Domestic Intelligence Service's designation of the right-wing Alternative für Deutschland (AfD), a populist party known for anti-immigration and Eurosceptic positions, as an extremist organisation created a further fracture line that Russian operations were able to exploit. Germany's own institutional response was found inadequate at the time. The Peace Research Institute Frankfurt documented the absence of a centralised attribution capacity and a VIGINUM equivalent. This is a gap the Merz government is now addressing with legislation.

Canada's own institutions have identified the stakes. Justice Marie-Josée Hogue, the Commissioner of Canada's 2025 *Public Inquiry into Foreign Interference*, stated that information manipulation poses the single biggest risk to Canadian democracy and is an existential threat. The Commission found significant systemic shortcomings in Canada's existing response capacity, and that campaigns are designed to create persistent uncertainty and distrust in democratic processes rather than to affect specific electoral outcomes.[26] Two further Canadian assessments in 2026 corroborated the Commission's

finding from distinct vantages. The Standing Senate Committee on National Security, Defence and Veterans Affairs, in its April 2026 report *Russia's Disinformation: Understanding the Challenge, Strengthening Canada's Response*, found that Russia's disinformation poses an urgent threat to Canada's national security, democratic institutions, and social cohesion; that the Government's current approach lacks coordination among federal entities; and that no strategic plan exists to address the threat.[27] The May 2026 report *Decision Making and National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum*, by Marcus Kolga, Jennie Phillips, Brian McQuinn, and Bartel Van de Walle, named Canada's cognitive sovereignty as "the ability of Canadians to make political decisions freely, without foreign coercion or manipulation" and as "actively contested by foreign actors seeking to shape Canada's democratic future," converging Russian narrative infrastructure, US official engagement, and AI-driven economic opportunism on the Alberta separatist debate as the most operationally legible Canadian case. The Senate report represents the parliamentary recognition of the threat; the civil-society report represents the empirical case for action.[28] Canada officially recognised this threat in 1990, produced further analysis in 1993, 2000, 2004, and 2016, but has not built the institutional response. The cost of that delay is now measurable.

Endnotes

1 On CIA front organisations and election interference, see Hugh Wilford, The Mighty Wurlitzer: How the CIA Played America (Harvard University Press, 2008). On the UK Information Research Department, see Paul Lashmar and James Oliver, Britain's Secret Propaganda War: The Foreign Office and the Cold War, 1948 to 1977 (Sutton, 1998). On Françafrique, see François-Xavier Verschave, La Françafrique: le plus long scandale de la République (Stock, 1998). On Voice of America and Radio Free Europe, see Arch Puddington, Broadcasting Freedom: The Cold War Triumph of Radio Free Europe and Radio Liberty (University Press of Kentucky, 2000).

2 Mark Galeotti, 'The Gerasimov Doctrine,' *Foreign Policy*, September 5, 2019, and his subsequent critique: 'I'm Sorry for Creating the "Gerasimov Doctrine,"' *Foreign Policy*, March 5, 2018.

3 Jade McGlynn, Memory Makers: The Politics of the Past in Putin's Russia (London: Bloomsbury, 2023); and McGlynn, Russia's War (Cambridge: Polity, 2023).

4 David Cattler, 'Signals from the North: What Nordic and Baltic Intelligence Assessments Reveal About Russia,' International Centre for Defence and Security (ICDS), March 20, 2026. Available at: https://icds.ee/static/icds_brief_signals_from_the_north_cattler.pdf

5 Timothy L. Thomas, 'Russia's Reflexive Control Theory and the Military,' Journal of Slavic Military Studies 17, no. 2 (2004): 237 to 256. On the original Soviet formulation, see Vladimir A. Lefebvre, The Algebra of Conscience (D. Reidel, 1982).

6 Christopher Paul and Miriam Matthews, The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It (RAND Corporation, 2016); and Keir Giles, Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power (Chatham House, 2016).

7 Dave McMahon, 'Cognitive War and Information Peacekeeping,' Sapper Labs Group, 10 December 2021.

8 SIPRI, 'Preparing for a Fourth Year of War: Military Spending in Russia's Budget for 2025,' April 2025.

9 Igor Panarin, presentation at the Islamabad Policy Research Institute forum, November 2024, documented through open-source monitoring of Russian strategic communications.

10 Jordyn Haime, Lu Yushan, Yang Mengli, David Bandurski, *Centralisation+: Understanding China's Transforming Strategy for Global Information Influence*, Swedish Psychological Defence Agency, 2026.

11 Alex Colville, Yang Mengli, Jordyn Haime, David Bandurski, *Guided Intelligence: China's AI Strategy and the Global Information Space*, Swedish Psychological Defence Agency, 2026.

12 Sze-Fung Lee, 'Deepfakes with Chinese Characteristics: PRC Influence Operations in 2024,' *China Brief*, Jamestown Foundation, March 29, 2024.

13 Linvill, Darren and Warren, Patrick, "What's Hiding Under the Kilt? Iranian Trolls for Scottish Independence" (2024). *Media Forensics Hub Reports*. 6. https://open.clemson.edu/mfh_reports/6

14 Washington Post, March 21, 2026. Péter Szijjártó confirmed regular contact with Lavrov in a public statement, March 24, 2026.

15 Anne Applebaum, 'The Longest Suicide Note in American History,' *The Atlantic*, December 16, 2025.

16 Kate Klonick, 'The State Department's X Directive and the End of Platform Independence,' *Lawfare*, April 1, 2026.

17 Lyubov Tsybulska, 'Russia, AI, and the Future of Disinformation Warfare,' RUSI, June 2025; and RUSI, 'Emerging Insights: Russia, AI and Disinformation Warfare,' January 2025.

18 DFRLab, 'Deepfake Video of Canadian Prime Minister Reaches Millions on TikTok, X,' Digital Forensic Research Lab, June 19, 2025. & Centre for Emerging Technology and Security (CETAS), 'From Deepfake Scams to Poisoned Chatbots: AI and Election Security in 2025'.

19 Amaury Lesplingart and Valentin Châtelet, 'Russia-linked Pravda network cited on Wikipedia, LLMs, and X,' Digital Forensic Research Lab (DFRLab) in collaboration with CheckFirst, 12 March 2025

20 The term 'liar's dividend' was coined by Bobby Chesney and Jacob Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,' *California Law Review* 107, no. 6 (2019): 1753–1820.

21 Joe Hagan, 'The Founder of Anthropic Says He Wants to Protect Humanity From AI. Just Don't Ask How,' *Vanity Fair*, March 2026.

22 On the institutional diagnosis, see Sarah Kreps and Doug Kriner, 'Generative AI as a Weapon of War in Iran,' Brookings, April 2026; and Patricia Lewis, 'The Iran War Highlights the Creeping Use of AI in Warfare,' Chatham House, 27 March 2026. On fabricated satellite imagery, see AFP, 'Fake AI Satellite Imagery Spurs US-Iran War Disinformation,' 9 March 2026. On the qualitative collapse of evidentiary adjudication, including the Grok authentication failure and the SynthID-confirmed fabricated imagery, see Mahsa Alimardani, 'The Fog of AI in the Iran War,' The Atlantic, March 2026. On the X demonetisation policy of 4 March 2026, see the platform's Creator Revenue Sharing program update, reported in World Geostrategic Insights, 8 March 2026.

23 Reporters Without Borders (RSF), Propaganda Monitor Season 2, RSF, 2026.

24 Mind the Bridge and Fincantieri, Dual-Use Technologies: Going Beyond the Divide, 2024/2025. Data updated May 2025.

25 Anne Applebaum, "The Longest Suicide Note in American History," The Atlantic, 16 December 2025.

26 Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, Final Report (Hogue Commission), January 2025.

27 Standing Senate Committee on National Security, Defence and Veterans Affairs, Russia's Disinformation: Understanding the Challenge, Strengthening Canada's Response (Senate of Canada, April 2026), sencanada.ca.

28 Marcus Kolga, Jennie Phillips, Brian McQuinn, and Bartel Van de Walle, Decision Making and National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum (DisinfoWatch, Global Centre for Democratic Resilience, Canadian Digital Media Research Network, CASi Labs, and Media Ecosystem Observatory, 6 May 2026), disinfowatch.org.

Chapter 4: What Success Looks Like for the Adversary

Adversaries do not set out to defeat democracies through cognitive warfare. They set out to exhaust them, to create chaos, to weaken and diminish the very trust in democracy. The distinction matters more than it first appears, because it changes what success looks like and therefore what defence requires. A democracy that has been exhausted still holds elections, still maintains institutions, still has a largely free press. But the substance those institutions were built to protect – e.g. a citizen's capacity to form genuine preferences, trust the systems that aggregate them, and sustain collective action in their defence – has been hollowed out. The institutions remain. True, free democracy does not.

The author's field research synthesis drawing on multiple national contexts provides the sharpest formulation of this constraint. Unlike most security threats, where damage can be assessed and recovery can begin once conflict stops, the cognitive damage to democratic trust and to a free society's information ecosystem cannot be easily rebuilt once it is lost. Societies cannot reverse epistemic erosion through an inquiry process. They do not know what you had until it is gone. There will be no moment of awakening. Citizens may feel the fog and still be unable to dispel it. Cognitive warfare does not just degrade a person's ability to navigate reality, it also undermines the collective instruments required to act on what one knows: shared truth, institutional trust, and the political will to respond.

The historical paradigm cases of adversary success are not primarily military. Lithuania's absorption into the Soviet Union in 1940 was accomplished without sustained armed resistance: the cognitive and political conditions for capitulation were prepared before the tanks moved. More instructive still is the earlier disappearance of the Lithuania-Poland Commonwealth, which ceased to exist not through military defeat but through the systematic undermining of the elite consensus and institutional coherence on which its functioning depended. Both cases establish the adversary's true objective: not the destruction of democratic infrastructure but the degradation of the will and capacity to use it. A state whose population has been convinced that resistance is futile, whose elites have been fragmented beyond the capacity for collective action, and whose institutions

have been hollowed of the trust that makes them function, has been defeated without a shot fired.

A further analytical distinction matters for the volume's argument. Russian operations, and the operations of the broader adversary set Russian operations have trained, are conducted with what practitioners across the field research increasingly identify as a criminal mentality rather than an institutional-state mentality. The framing is not rhetorical. It captures something analytically significant about how adversary operations engage cost-benefit calculation. A state operating on institutional logic adjusts operational tempo and intensity in response to operational costs. The Russian Federation does not. The casualty rates Russia has sustained on the kinetic front in Ukraine, currently averaging approximately five thousand soldiers killed and wounded per week for minimal territorial gain, are not the casualty rates of a state calculating cost against benefit in any framework Western analysts recognise. They are the casualty rates of an actor for which operational continuation itself is the strategic objective. The same logic operates in the cognitive domain. Russian operations continue past the point where they have demonstrably failed to achieve their stated objectives because the continuation itself, the demonstration that Russia is willing to sustain operational tempo no Western adversary will match, is itself the cognitive operation. The framework implication is significant: Western frameworks built on rational-actor assumptions cannot match an adversary operating on indifferent-to-cost logic. The defensive task requires recognising that the cost-benefit calculations Western analysts apply to Russian strategic decision-making are not the calculations Russia applies, and that defensive architectures must be designed to operate against indifferent-to-cost adversary continuation rather than against rational-actor cost-imposition expectations.

Five Conditions for Adversary Success

Adversaries are not optimising against any single metric. The author’s field research identifies five conditions that constitute cognitive warfare success, conditions that adversaries track whether or not they name them explicitly.

The first is **epistemic paralysis**. This occurs when citizens doubt their capacity to know what is true. It is not that they believe specific false things, but that they have lost

confidence in their ability to distinguish truth from falsehood. An epistemically paralysed citizenry does not engage in democratic deliberation. It disengages, or it defers to whoever projects the most certainty.

The second is **institutional delegitimisation**: governments lose the perceived authority to act on behalf of their citizens. This is not necessarily through corruption scandals or policy failures, though these accelerate the process, but through the sustained manufacture of doubt about whether institutions represent citizens at all or serve hidden interests instead.

The third is the **collapse of collective action**. Citizens who distrust each other, distrust institutions, and doubt shared reality cannot coordinate. Democratic governance is a collective action problem at every level: voting, compliance, civic participation, political mobilisation. When the social infrastructure that makes collective action possible has been sufficiently degraded, democracies cannot respond even to threats they can see.

The fourth is a **strategic inward turn**. Democracies being to abandon international commitments, withdraw from alliances, and redirect political energy toward internal division and preoccupation. This serves adversary objectives directly, relieving external pressure and fracturing the coalition architecture that makes democratic defence viable.

The fifth, and the most consequential on the longest time horizon, is the **loss of the democratic model's global appeal**. When democracies demonstrably cannot govern themselves, protect their citizens, or sustain coherent policy, the argument that liberal democracy outperforms authoritarian alternatives loses its empirical foundation. This matters not only for geopolitics but also for the domestic legitimacy of democratic institutions: citizens who do not believe democracy works will not defend it. The data confirm this erosion is already underway. Freedom House's *Freedom in the World 2026* documents the twentieth consecutive year of decline of global freedom. Just 21 percent of the world's population now lives in countries rated Free, down from 46 percent two decades ago. *The argument for democratic defence is not abstract. It is a race against a measurable trend.*[1]

The technique by which adversary operations sustain operational continuation past the threshold of demonstrated failure is *mundanisation*: the deliberate routinisation of atrocity,

transgression, and norm violation to exhaust adversary moral and political capacity to respond. Each successive winter campaign against Ukrainian energy infrastructure, each round of mass civilian casualties from missile and drone strikes, each documented violation of international humanitarian law, each documented assassination of a dissident abroad, each act of sabotage against subsea infrastructure in the Baltic Sea, accumulates inside the international response not as a discrete event demanding action but as the new background condition against which subsequent events are measured. The pattern is operational, not accidental. Adversaries produce transgression at sufficient volume and sufficient frequency that allied governments, allied publics, and international institutions lose the capacity to maintain the response intensity that the first instance of any given category of transgression would have triggered. Mundanisation is the temporal technique by which the five success conditions described above are produced over time. Each successive routinised atrocity recalibrates the threshold of what counts as actionable, lowering the institutional and political response the next instance can elicit. The framework implication is significant: democratic response architectures must be designed to interrupt mundanisation rather than to track absolute thresholds, because by the time absolute thresholds are crossed the adversary has already gained the operational space that the cumulative pattern of normalisation produced.

The Mechanisms of Arrival

The Attack Surface: Nine Universal Psychological Needs

Cognitive warfare succeeds by exploiting the psychological needs that every human being carries regardless of political affiliation, nationality, or media literacy. The five needs we identified previously – safety and security, belonging and connection, esteem and dignity, meaning and coherence, and identity and continuity – remain essential. But they do not account for the full architecture of human psychological need. This section expands the taxonomy. Four additional needs represent a documented operational pathway through which adversarial cognitive operations have succeeded where analysts expected resilience, and explains why cognitive warfare reaches citizens who are media-literate, civically engaged, economically secure, and institutionally trusting.

These nine needs do not describe distinct populations. They describe the same citizen, operating in different ways. All nine share one structural feature that adversaries systematically exploit: when any of them goes unmet, the resulting distress produces emotional reactivity that forecloses reflective response. A citizen in that state is not assessing the quality of the narrative being offered. Citizens are reaching for whatever reduces their distress. Cognitive defence must be built to interrupt that mechanism.

1. The Need for Safety and Security

The human threat-detection system is calibrated for survival, not deliberation. Fear captures our attention and impairs the very higher-order faculties democratic participation requires. Adversaries amplify crime, immigration, and terrorism as existential dangers, making the world feel structurally more dangerous than it is. The defence implication runs deeper than media literacy. Emotional self-regulation is cognitive defence infrastructure, and the democracies that have built the most complete cognitive defence architectures, e.g. Finland, Estonia, Lithuania, have each invested in it explicitly, from classroom curricula through to national communications frameworks that model epistemic steadiness under pressure.

2. The Need for Belonging and Connection

Social exclusion registers neurologically as physical pain. Adversaries exploit this by sharpening in-group and out-group boundaries simultaneously. They tell marginalised communities their country does not want them, telling majority communities they are being displaced.[2] The Bicchieri norm cascade mechanism compounds this. Citizens who privately hold democratic values can be made to believe, falsely, that everyone around them has already abandoned them, producing social isolation that makes genuine community impossible to perceive even when it exists.

Belonging is not only a need to receive. A significant portion of any democratic population is primarily oriented toward being needed. They want give care, to contribute, to be of genuine use. Adversaries exploit this caregiving orientation through redirection. They present disinformation ecosystems as spaces of genuine mutual care, where the group demonstrably needs what the individual can provide. Through compassion capture, they channel the care-oriented citizen’s genuine concern toward targets and conclusions that

serve adversary objectives. Field research across the Nordic and Baltic democracies identifies the density of civil society organisations as a structural component of cognitive resilience that institutional defence architecture alone cannot replicate.

3. The Need for Esteem and Dignity

Humans need to feel valued, capable, and respected. Status anxiety is one of the most reliable predictors of political radicalisation. Adversaries exploit dignity wounds inflicted by economic dislocation, social disparity, cultural change, and political marginalisation, amplifying the narrative that elites hold ordinary citizens in contempt. The operation is effective not because the narrative is false but because it is incomplete. It offers the wound without the remedy, the grievance without the constructive outlet. Citizens who experience economic precarity or withheld recognition as a dignity violation, i.e. those who did what the system required and still found themselves marginalised, are not seeking policy solutions. They are seeking the restoration of worth. Adversary operations do not offer them a ladder. They offer an explanation for why the ladder was never real.

4. The Need for Meaning and Coherence

Humans require the world to make sense; uncertainty is intrinsically aversive. Adversaries exploit this not by providing false meaning but by destroying the conditions under which any meaning is possible. They flood the information environment with contradictions, undermining shared epistemic foundations, and positioning conspiracies and scapegoats to fill the void. This is the operational signature of what NATO analytical literature and the broader research community now name *epistemic warfare*: operations whose objective is not to persuade audiences toward a specific false belief, but to degrade the conditions under which confident belief is possible at all. Epistemic warfare targets the cognitive process rather than the cognitive output, and is the form of conflict the resilience-only posture is structurally unable to deter. A related concept in the doctrinal literature is *ontological warfare*: the most advanced form of epistemic attack, directed not at what people believe but at what is permitted to be believable. Where epistemic warfare degrades the conditions under which confident belief is possible, ontological warfare attacks the substrate of possibility itself, controlling what is even thinkable rather than what is currently thought. The two operate on different timescales. Epistemic warfare can

be detected within a single news cycle as a saturation effect; ontological warfare requires sustained operations over years and decades, often through cultural and historical-revisionist channels rather than through current-affairs disinformation. The Russian *vranye* tradition combines both: high-volume contradictory claims in the present operate as epistemic attack, while sustained Russian historical revisionism, including the systematic rewriting of Soviet-era narratives and the contemporary insistence that Ukrainian statehood is itself historically illegitimate, operates as ontological attack on what is permitted to be thought about the boundaries of nations and the legitimacy of independent post-Soviet societies. Where epistemic warfare leaves a population unable to confidently believe true things, ontological warfare leaves a population for whom certain true things become difficult to think at all. Kruglanski's Need for Cognitive Closure theory for Cognitive Closure theory establishes that under stress, individuals become increasingly intolerant of ambiguity and more receptive to definitive answers. The adversary's most architecturally durable success condition is this: unlike influence operations requiring continued maintenance, a preference for false certainty, once established, is self-sustaining. The population carries it forward without further adversary involvement.

5. The Need for Identity and Continuity

Humans need a stable sense of who they are and where they belong in a historical narrative that extends before and beyond them. Adversaries exploit identity by promoting historical revisionism, amplifying the message that a community's identity is under existential attack, and weaponising nostalgia for a past that may or may not have existed as described. The adolescent period of identity formation creates a structurally elevated vulnerability. Young people navigating identity are the segment of the population most likely to accept a distorted answer, and the most susceptible to long-term radicalisation pipelines and cultural influence operations at the Layer 1 socialisation level. Nuance is the first casualty of identity operations, because nuance is psychologically more demanding than the binary clarity the need for continuity is reaching for. Tanna Krewson's 2025 paper for the NATO Allied Command Transformation and University of Cambridge Centre for Geopolitics joint compendium develops the weaponised identity concept as one of the core attack vectors within ACT's cognitive warfare framework, treating identity

not as a peripheral cultural concern but as a primary architectural target. The nine-need taxonomy developed in this chapter extends Krewson's weaponised identity framing into a broader psychological architecture: identity is one of nine needs adversary operations exploit, and the cognitive defence architecture must address all nine rather than treating identity in isolation.

6. The Need for Moral Order and Integrity

This need has no adequate place in Maslow's hierarchy, or in the five-need frameworks derived from it. Its absence is the most operationally significant gap in the existing taxonomy. A substantial portion of every democratic population organises its political life around the need for moral coherence. They desire a world in which wrongdoing has consequences and the gap between how things should be and how they are can be closed through action. Citizens animated by the need for moral order are, in functioning democratic culture, among democracy's most motivated defenders. The adversary weaponises this through three mechanisms. They use weaponised outrage, deliberately surfacing real institutional failures to produce moral outrage and then ensuring no constructive outlet is available. They engage in false moral equivalence, presenting all political actors as equally corrupt until the citizen who needs the world to be organised according to principles disengages rather than accepts a degraded version of the moral order. And they turn values, using the democratic citizen's own moral commitments to fairness, accountability, rule of law, as the argument for rejecting democratic institutions. The argument structure is consistent. A person's integrity requires you to reject institutions that have failed their values. This is the mechanism through which high-integrity citizens who would never accept an explicit authoritarian argument are moved, through individually defensible moral steps, to authoritarian conclusions.

7. The Need for Competence and Understanding

The need to understand, to make sense of the world through one's own analytical effort, is a distinct vulnerability that most cognitive defence frameworks overlook. Citizens for whom epistemic autonomy is primary are targeted through their analytical disposition. When the information environment has been flooded with contradictory claims to the point where sustained analysis produces no reliable conclusion, the citizen who needed to

understand is left with a specific helplessness. They tried, rigorously, and failed. The well-constructed conspiracy theory exploits this by offering what appears to require more thought, hidden connections and systemic patterns that reward investigation. The need for genuine competence is satisfied by a simulacrum of it, which is why dismissing conspiracy adherents as credulous is both wrong and counterproductive. The defence implication is specific: epistemic infrastructure, source authentication, provenance verification, confidence scoring, serves this population in ways that broad-based media literacy campaigns do not.

8. The Need for Autonomy and Self-Determination

The need to exercise genuine agency is exploited covertly. operations targeting the autonomy need succeed precisely because the citizen experiencing them believes they are not being manipulated. Citizens for whom personal agency is a primary orientation reliably reject explicit messaging that tells them what to think. What they cannot as easily detect is an information architecture pre-constructed to ensure the conclusions they reach independently are the conclusions the adversary has already positioned. The citizen who discovers an apparent truth through their own initiative experiences that discovery as validation of their independent judgment, making the resulting belief more durable and more resistant to correction. Independence of conclusion feels like immunity to manipulation. It is not. The defence implication is structural: it must consist of building an information environment in which independent investigation reliably leads to accurate conclusions, a platform architecture problem, a provenance infrastructure problem, and an information ecosystem funding problem.

9. The Need for Freedom and Positive Engagement

The theoretical foundation for this need rests in self-determination theory, the body of work developed by Edward Deci and Richard Ryan establishing that human motivation depends on the conditions under which autonomy, competence, and relatedness can be exercised, and that environments which foreclose those conditions produce disengagement rather than compliance.[3] People want stimulation, variety, and a future that holds something worth anticipating. Citizens for whom this need is primary are rendered politically disengaged not by threat but by the perception that nothing available

is worth engaging with. Saturation strategies overwhelm them with the impression that the political landscape is irredeemably dreary and engagement is not worth the cost. The algorithmic engagement model compounds this by substituting managed stimulation for genuine civic participation. A further mechanism draws this population toward disinformation ecosystems specifically because they offer what official democratic discourse frequently fails to provide: narrative excitement, the pleasure of discovery, and the sense of participating in something consequential. The democratic narrative has a design problem. It has allowed adversaries to claim the interesting story. Reclaiming it is not merely a communications task. Ukraine has demonstrated at scale that making the case for what democracy is defending, through cultural production, civilian courage, and forward-looking identity construction, is Layer 1 cognitive defence, operating through the need for positive engagement.

The Integrated Architecture

These nine needs do not operate independently. The adversary operates across all of them simultaneously, using the same content to activate different needs in different audiences and the same platform architecture to distribute it to all of them at once. The interactions follow predictable psychological logic. The safety need and the belonging need interact to produce compound distress that forecloses deliberation more completely than either alone. The moral need and the autonomy need interact to produce exceptional resistance to correction, as the citizen defends both a conclusion and the independent judgment through which they reached it. The meaning need and the positive engagement need interact to produce political nihilism in its most complete form. These compounding dynamics are the adversary's most powerful force multiplier. A single piece of content can simultaneously activate several needs in a citizen already operating under compound distress.

The social infrastructure that underlies all six operational layers of this framework – e.g. the care economy investment, the welfare state architecture, the civil society density that the Nordic and Baltic democracies have built through deliberate choice – is not merely social policy with incidental security benefits. It is the environment in which all nine needs can be met well enough, consistently enough, that no single adversary operation finds a

population in the acute state of unmet need that exploitation requires. The adversary's operational dependency is on unmet need. The most durable defence is a society in which the adversary's offer of false substitutes finds insufficient purchase.

The argument returns, as it must, to its starting point. Cognitive warfare does not attack information. It attacks the human conditions under which information can be received, processed, and acted upon. The defence cannot operate only at the information layer. It must operate at the human layer beneath it. All nine of these needs are part of that layer. A cognitive defence architecture that addresses five of them leaves four categories of citizen structurally undefended, and in the domain these adversaries have chosen, a vulnerability that has been identified but not addressed is a vulnerability that has already been found. Cognitive defence is not primarily a communications problem. It is a human resilience problem.

Adversary success does not arrive as a visible event. It arrives through the accumulation of conditions that are each individually explicable as something else. Several mechanisms drive this accumulation.

The echo chamber mechanism is structural. Social media has replaced shared information environments where disagreement was unavoidable with filtered feeds that confirm existing beliefs. The adversary need not persuade: it only ensures that confirming content is more available, more emotionally arousing, and more algorithmically reinforced than challenging content.

The dead internet threshold has already been crossed. There is now more AI-generated content than human-generated content online, and the resilience frameworks democracies built were not designed for this environment.

The neurophysiological endpoint is the third mechanism. When citizens are flooded with sustained uncertainty and chaos, the prefrontal cortex goes offline. The adversary does not need to persuade citizens that authoritarianism is good, only to make democracy feel incapable of providing security.

The route from that neurological state to political consequence runs through a mechanism that the threat landscape has not yet named explicitly, which is the conversion of private

unhappiness into public outrage. Individual emotional distress, when sustained and unaddressed, does not remain private. Research on the emotional origins of populist mobilisation demonstrates that adversaries do not need to generate grievances from scratch. They need only to ensure that existing distress finds a political outlet, and that the outlet on offer is one they have pre-shaped. The seizing-and-freezing dynamic social psychologist Arie Kruglanski identifies at the individual level operates collectively: a population whose tolerance for ambiguity has been exhausted reaches for certainty together, and the certainty on offer has been positioned in advance.[4] This is the adversary's most durable success condition, because it does not depend on continued operation. Once the emotional-to-political conversion has occurred, the population carries the infection forward. The implication for democratic defence is one of the report's most consequential arguments. Addressing the information layer alone is insufficient. A citizen who cannot regulate their own emotional reactivity under sustained adversarial pressure remains exploitable regardless of their media or digital literacy. The author's central architectural claim in this manuscript is that emotional self-regulation is cognitive defence infrastructure: a form of resilience that operates at population scale and belongs within a national-security framing, not only within the clinical and educational settings where emotional regulation is more commonly discussed. It is a fundamental part of our collective security and should be treated as such.

A structural warning belongs here. Field research in Lithuania revealed what practitioners there call the passive citizen problem. Highly effective institutional architecture, reliably operated and publicly trusted, can produce a population that delegates cognitive vigilance to institutions rather than maintaining it individually. Citizens who trust that the government is monitoring, attributing, and responding have less personal incentive to develop the individual media literacy and critical thinking capacity that constitute Layer 1 resilience. That trust, if it substitutes for rather than supplements individual capacity, creates a new vulnerability. If the institutions fail, are captured, or are overwhelmed at scale, the population has no reserve to draw on.

The calibration problem compounds the measurement challenge. Without empirical evidence of actual narrative penetration in a democratic population, governments face a binary error risk: over-reaction that produces authoritarian responses to threats that affect

a small minority, or under-reaction that leaves the majority undefended. The Fondation Descartes has produced the only study to date that empirically measures the proportion of a democratic population that has actually adopted specific adversary narratives, testing claims from each major conflict protagonist across 4,000 respondents in France. Its methodology provides the replicable baseline that democratic governments need to move from assumption to evidence on the scale of cognitive threat. Democratic governments that cannot measure the effect cannot calibrate the response.[5]

The Measurement Gap and What Comes Next

The challenge of measurement is epistemological. Cognitive warfare operates on attitudes, perceptions, and decision-making at population scale, and democracies cannot run controlled experiments on their own citizens. Even when adversary operations are detected, the counterfactual is unknowable. What would have happened without the intervention? The honest answer is that certainty is rarely available. What is available is directional assessment: tracking institutional trust over time, monitoring polarisation indices, measuring information ecosystem health, and benchmarking detection speed and response coordination against peer democracies. Is trust trending toward the way of Finland or away from it? Is detection capacity comparable to France? These questions are answerable even when absolute effectiveness is not. Reframing from measuring effectiveness to assessing readiness is not an evasion of the measurement challenge. It is the epistemically honest response to it.

What all of this establishes is why a layered defence is not optional. No single intervention addresses a threat that operates simultaneously on psychology, platform architecture, institutional legitimacy, and political will. The architecture must match the complexity of what it is defending against. Part II builds that architecture.

Endnotes

1 Freedom House, Freedom in the World 2026, Freedom House, 2026.

2 Henri Tajfel and John C. Turner, 'An Integrative Theory of Intergroup Conflict,' in W.G. Austin and S. Worchel (eds.), The Social Psychology of Intergroup Relations (Monterey, CA: Brooks/Cole, 1979), 33–47.

3 Edward L. Deci and Richard M. Ryan, *Intrinsic Motivation and Self-Determination in Human Behavior* (Plenum Press, 1985)

4 Arie W. Kruglanski and Donna M. Webster, 'Motivated Closing of the Mind: "Seizing" and "Freezing,"' Psychological Review 103, no. 2 (1996): 263–283.

5 Fondation Descartes and Laurent Cordonier, *Pénétration en France des récits étrangers sur les conflits contemporains*, November 2024; and follow-up, January 2026, fondationdescartes.org.

Part II: The Defence

Chapter 5: Three Objectives, Six Layers

The three objectives of cognitive defence are protection, detection, and response. The protection-detection-response sequence is established in the NATO Chief Scientist cognitive warfare research programme as the foundational triad for democratic cognitive defence.[1] The six-layer architecture developed in this chapter is the author's own analytical contribution: an elaboration of what protection, detection, and response each require at the level of institutional and social investment, built from the field-research evidence base across fifteen countries and not derived from any existing operational framework. Protection means strengthening citizens' capacity to perceive reality accurately and form genuine political preferences. Detection means identifying manipulation operations in progress, attributing them where possible, and making their methods visible. Response means imposing costs on adversaries, reducing their operational effectiveness, and restoring the conditions for democratic deliberation when they have been disrupted. These three objectives are also the sequence in which the six layers are organised: Layers 1, 2, and 3 are primarily protective; Layer 4 is detective; Layers 5 and 6 are responsive. The architecture is not arbitrary. It reflects the logic of where democratic durability is built, monitored, and defended.

The full-spectrum approach articulated in NATO Allied Command Transformation's working definition of cognitive warfare, which has not yet been approved at the political level by the Alliance, extends this protection-detection-response sequence across the continuum of competition.[2] ACT's working frame integrates military, government, and societal systems through the diplomatic, informational, military, economic, financial, intelligence, and law enforcement (DIMEFIL) toolset to deter, disrupt, or destroy adversary capabilities and influence while building population resilience. The six-layer architecture developed by the author operationalises that full-spectrum framing for democratic conditions: Layer 6 holds the legislative, doctrinal, regulatory, and institutional instruments that engage the DIMEFIL toolset. The lower foundation (social infrastructure) and Layer 1 (the human-relational substrate) are, as the author argues, the operational

substrate of the population resilience clause that the NATO working definition names but no Alliance member has yet operationalised at scale, and this manuscript is the first comprehensive operationalisation built for a NATO member state.

Readers familiar with NATO's cognitive warfare framework will recognise the three objectives as broadly consistent with the protection-detection-response triad that structures ACT's concept development work. The six-layer architecture proposed in this chapter is not a competing framework. It is an elaboration of what protection, detection, and response each require at the level of institutional and social investment. The protection objective maps primarily onto Layers 1 through 3, where the preconditions for cognitive resilience are built before any operation arrives. The detection objective maps onto Layer 4, where detection capacity, attribution architecture, and intelligence sharing create the awareness layer. The response objective maps onto Layers 5 and 6, where active defence, cost imposition, and sovereign legislative capacity translate awareness into action. The two-foundation architecture, social infrastructure below and political will above, reflects the NATO full-spectrum approach definition's insistence that military and non-military activities must be synchronised across the continuum of competition, not activated only in crisis.

Six Layers Between Two Foundations

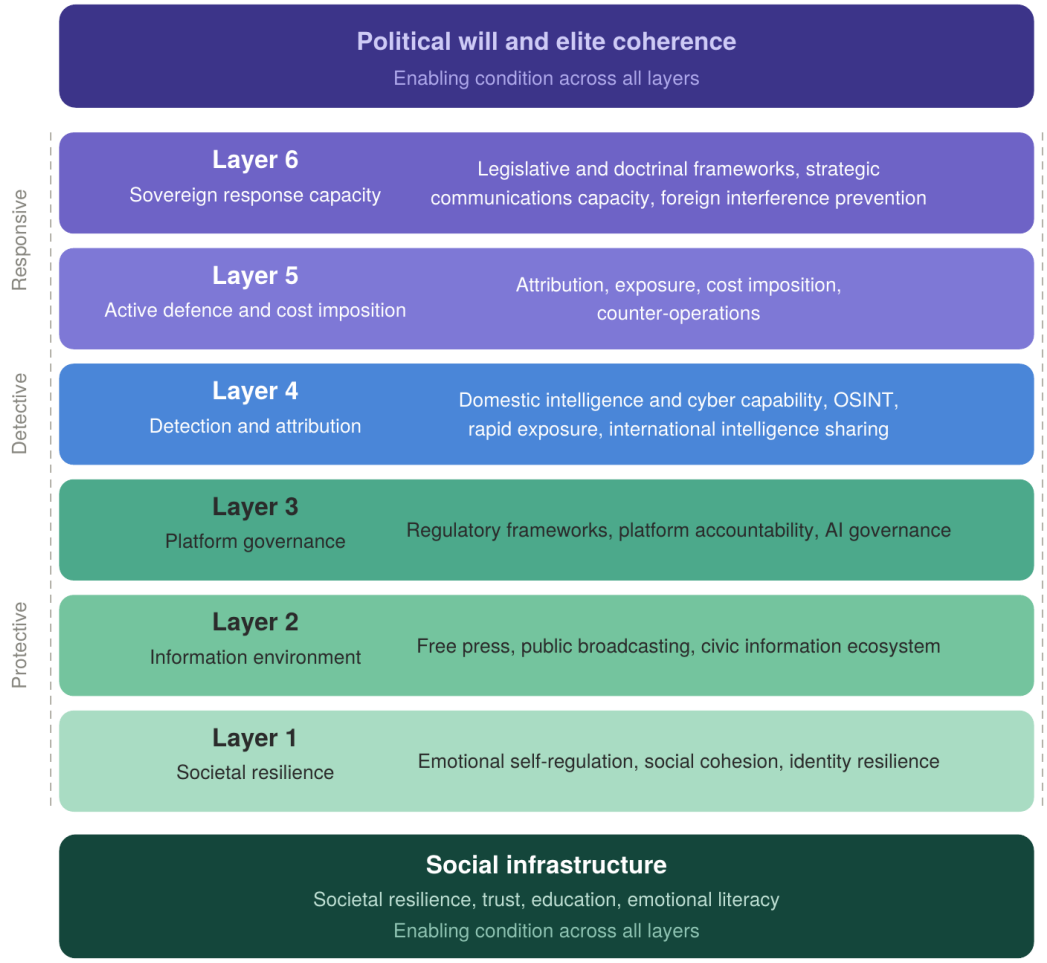


Figure 1: The Six-Layer Cognitive Defence Architecture

The six-layer framework developed in this manuscript rests on two horizontal foundations that bracket the operational layers above and below. The dual-foundation structure, with social infrastructure as the lower foundation and political will and elite coherence as the upper foundation, is original to the author's analytical contribution and is what makes the framework diagnostically useful rather than merely descriptive: it identifies different intervention points for countries with strong social infrastructure but weak political will, and for countries with strong political will but thinner social infrastructure. The lower foundation is social infrastructure: the trust, societal cohesion, and emotional literacy that citizens carry into public life; the civil society organisations, volunteer networks, civic duty,

and national service experience that bind them together; and the quality and equity of education that determines whether citizens across all socioeconomic backgrounds can navigate an adversarial information environment at all.

Social infrastructure cannot be built by any single agency or mandated by legislation. It develops over time through sustained investment in the conditions that bring people together, and it can be allowed to erode. Every country in this research set with a relatively strong cognitive defence architecture also has deep social infrastructure. That is not coincidental, though the causal direction, whether strong social infrastructure produces cognitive resilience or whether the same political culture produces both, warrants further examination. The comparative Nordic evidence base for this relationship is documented in the Hybrid CoE comparative work on Nordic resilience models.[3] The layers describe what democracies must be able to do. Social infrastructure determines whether they actually can.

There is a systems-level explanation for why whole-of-society response is structurally required rather than merely preferred, and it comes from the architecture of the threat itself. Military institutions operating inside democratic societies have developed a relatively hard shell against conventional information security threats. They operate with redundant systems, maintain security clearances and information compartmentalisation, and train their workforce in threat recognition. The cognitive domain is a different matter. Field research from within allied military structures across multiple national contexts reveals a consistent pattern: cognitive warfare as a concept remains institutionally contested, under-resourced, and subordinated to public affairs functions that were never designed to address it. In some allied forces, joint-level information operations officers have been absent for over a decade. In others, the function is pulled between strategic communications, psychological operations, and hybrid threat communities without resolution. One practitioner put the problem precisely: the threat does not say bang, and in institutions built around things that do, that invisibility is structurally disqualifying. The hard shell, on closer inspection, is considerably more porous than it appears. Society, by deliberate democratic design, has a porous and open boundary. Censorship is prohibited; information flows freely; and, the platforms through which cognitive attacks are administered are embedded in daily civilian life. Governments, businesses, media

organisations, and civil society all operate within that open boundary, each representing both a potential vulnerability and a node of potential defence. The relationship between these actors is the whole-of-government and whole-of-society coordination architecture that distinguishes operational total defence from rhetorical total defence. Whole-of-government is the horizontal coordination across federal departments and agencies, and in federal systems like Canada, the vertical coordination across orders of government, that converts dispersed mandates into coherent response. Whole-of-society extends that coordination further to include civil society, the private sector, academia, and citizens themselves. The two are not synonyms. Whole-of-society defence has a whole-of-government precondition: without the government-coordination spine, societal mobilisation has no institutional architecture to convert it into sustained effect. Cognitive warfare exploits precisely this asymmetry. It flows through the societal opening to reach the political level directly and the military indirectly. Political will is the more immediate target. A democracy whose population has been cognitively fractured cannot sustain the consensus that authorises military action, funds defence, invests in its alliances, contributes to international assistance, or absorbs the costs of sacrifice required for continued freedom over time. An armed force whose recruiting base has been eroded, whose political legitimacy has been undermined, and whose population has lost confidence in the purpose of collective defence cannot be defended by any amount of institutional hardening inside the military itself. The very strength of open democratic societies, the free flow of information and the freedom of citizens to form their own views, is simultaneously the attack surface that adversaries have learned to exploit at scale. This is not a flaw to be corrected. It is the condition under which democracy operates. The defence must be designed for it.

The reason the architecture must be whole-of-society is the same reason the threat requires it. Cognitive warfare is total society warfare: citizens are simultaneously the primary target, the primary terrain, and the primary line of defence. Whole-of-society defence requires a whole-of-government coordination architecture as its institutional precondition: the horizontal coordination across departments, agencies, and orders of government that converts dispersed mandates into coherent national response. Without that government coordination spine, societal mobilisation has no architecture through

which to act, and remains aspirational rather than operational. The Nordic and Baltic total defence models examined in Part II are operational because they have built both dimensions: government coordination as the institutional spine, and societal mobilisation extending across civil society, the private sector, academia, and citizens. The manuscript uses “whole-of-society” as the inclusive term throughout, on the understanding that operational whole-of-society defence is always also whole-of-government. Governments cannot defend them by acting on their behalf. They can only build the conditions in which citizens can defend themselves. That is what the lower foundation exists to do, and it is why no government department or agency, however well-resourced, can substitute for it. The country cases in Part II show what this looks like when it is built: Finland, Sweden, Norway, Estonia, Latvia, Lithuania and Ukraine have each developed whole-of-government and whole-of-society total defence frameworks that are not theoretical constructs but operational realities with legislation, budgets, and institutional mandates behind them.

The architecture this chapter proposes requires both whole-of-government coordination and whole-of-society engagement, and the two concepts should not be collapsed. Whole-of-government coordination addresses the institutional problem: the alignment of defence, intelligence, interior, foreign affairs, justice, and communications ministries under coherent political direction. The failure mode of its absence is siloed mandates and inter-agency competition. Whole-of-society engagement addresses the social mobilisation problem: the informed, prepared, and engaged participation of civil society, the private sector, academia, and individual citizens alongside government institutions. The failure mode of its absence is a coordinated state defending an inert population. The six-layer framework requires both. Layers 4 through 6 are primarily a whole-of-government problem. Layers 1 through 3 are primarily a whole-of-society problem. Political will is the enabling condition that makes whole-of-government function. Social infrastructure is the enabling condition that makes whole-of-society function. Neither works without the other.

The upper foundation is political will and elite coherence: the shared commitment among government, institutions, civil society, and the private sector to treat cognitive defence as a continuous obligation rather than an episodic response. A country may have strong

social infrastructure, functional detection systems, and operational resilience programmes. Without sustained political will and cross-sector elite coherence, those systems remain episodic at best and dormant at worst. Political will is the activating precondition, not a co-equal operational layer. The sandwich framing captures this structurally: six operational layers operating between two horizontal foundations.

On these foundations sit six layers. Layer 1 is individual and societal cognitive capacity: the emotional self-regulation, social cohesion, and identity resilience that determine whether citizens can sustain democratic participation under adversary pressure. Layers 2 through 6 are security responses and governance choices that can be built by governments and agencies. Layer 1 is built by economic policy, integration policy, democratic reform, and the sustained delivery of public services over time. If Layer 1 is broken, the layers above it are built on sand.

The lower foundation and Layer 1 are doctrinally anchored in Article 3 of the Washington Treaty, the original NATO obligation that each member "separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[4] The NATO Chief Scientist Research Report on Resilience, released in December 2025 alongside a parallel Chief Scientist Research Report on Cognitive Warfare, outlines the Alliance's evolving approach to resilience as the substrate of deterrence and defence, rooted in Article 3 and examining the role of science and technology in supporting Allied preparedness and recovery from major shocks.[5] Allied Command Transformation's working definition of cognitive warfare uses a different and more operationally specific frame for the same concern, naming "building population resilience" as part of the full-spectrum approach the working definition articulates. Across the Article 3 treaty obligation, the Chief Scientist Research Report on Resilience, and the ACT working definition's population resilience clause, the doctrinal direction is convergent: resilience is the substrate on which cognitive defence and deterrence rest. What remains unsettled, and what no NATO member has yet operationalised at scale, is how to deliver on it. The Nordic-Baltic and Ukrainian cases examined in Part II are the operational answers under different national conditions. The Canadian recommendations in Part V build directly on this doctrinal foundation.

Layer 2 is the integrity of the information environment: the trusted information infrastructure and the population's capacity to navigate it, encompassing media and digital literacy, quality journalism, public broadcasting, and the civic information ecosystem. Layer 3 is platform architecture and algorithmic accountability: the structural regulation of the systems that determine what content reaches whom at scale. Layer 3 encompasses two distinct categories. Content-hosting platforms detect and moderate harm after content is published at scale; AI providers can moderate or constrain output at the generation stage. These are different points of intervention requiring different governance approaches. The Layer 3 regulatory toolkit must address both, and conflating them produces architecture with gaps that adversaries can exploit. Layer 4 is detection and attribution: the institutional capability to identify, monitor, and attribute cognitive operations in progress. Layer 5 is active defence: the attribution, exposure, and cost imposition against adversary operations. Layer 6 is sovereign response capacity: the legislative, doctrinal, regulatory, and institutional instruments that protect democratic decision-making from foreign interference.

A clarification matters here on the relationship between Layers 2 and 3 and freedom of expression. Democratic cognitive defence is sometimes framed by its critics as a restriction on free speech. The opposite is closer to the truth. In most contemporary democracies, freedom of expression is no longer primarily threatened by state censorship but by two compound conditions that erode the conditions under which expression is meaningful. The first is platform algorithmic architecture designed for engagement maximisation, which advantages emotionally arousing content over deliberative content and reaches conclusions about what each user should see in ways that are opaque to the user, to researchers, and to regulators. French President Emmanuel Macron put the argument directly in February 2026: free speech is meaningless if citizens have no clue how the algorithm guiding them is made, tested, or trained, and the democratic consequences of opaque algorithmic bias are structural. Macron's formulation, "we are in favor of free algorithms, totally transparent," reframes the regulatory argument from restriction to enablement.[6] The second compound condition is the flooding of the information environment with inauthentic content, including the AI-generated slop documented across investigative reporting in 2025 and 2026, which drowns out authentic

citizen expression and degrades the signal-to-noise ratio on which deliberative exchange depends. Both conditions limit freedom of expression rather than protect it. Layer 2 (information environment integrity) and Layer 3 (platform architecture and algorithmic accountability) are therefore freedom-of-expression-enabling layers, not freedom-of-expression-restricting layers. The democratic regulatory argument is not a defensive concession to censorship pressure but a positive obligation to maintain the conditions under which expression can be meaningful at population scale. The underlying epistemic condition Layers 2 and 3 are responding to is the liar's dividend developed in Chapter 3. When the question of authenticity becomes structurally unanswerable at population scale, the conditions under which expression is meaningful collapse independently of any specific content moderation regime. Information environment integrity and platform architecture accountability are the institutional answers to that collapse, and they are the layers at which the verification infrastructure citizens depend on can be either sustained or conceded.

Cyber operations are distributed across multiple layers depending on objective, not a discrete layer of their own. Cyberattacks on critical infrastructure are Layer 5; adversary actions with Layer 1 cognitive effects, such as operations that deliberately deepen social fractures or erode institutional trust, belong to Layers 1 and 2; platform manipulation through compromised infrastructure is a Layer 3 concern; signals intelligence feeding the detection function is Layer 4. This is not a gap in the framework. It is the framework's answer to the cyber-cognitive convergence argument detailed in Chapter 3. The integration is structural, not incidental.

Mapping the Cognitive Advantage Triad to the Architecture

NATO Allied Command Transformation defines cognitive advantage as ongoing operations, activities, and efforts to continuously shape the cognitive dimension, and disaggregates it into three components: narrative advantage (the degree of dominance gained over perception and interpretation, including legitimacy and strength); psychological advantage (the degree of dominance gained over an adversary's cohesion, morale, performance, and will to fight); and decision advantage (the degree of dominance gained over an adversary's situational understanding and decision making). The triad

describes what adversaries pursue. The six-layer architecture is the defensive answer to each.

Narrative advantage operates primarily at Layers 2 and 3. It is contested in the information environment (Layer 2) where trusted information infrastructure, journalism, media literacy, and the civic information ecosystem either anchor a society's narrative resilience or fail to, and at the platform layer (Layer 3) where algorithmic amplification and platform governance determine which narratives reach which audiences at scale. A democracy that has built integrity at Layers 2 and 3 denies the adversary the conditions for narrative dominance. A democracy that has hollowed those layers concedes narrative advantage by structural default.

Psychological advantage operates primarily at the lower foundation (social infrastructure) and Layer 1 (the human-relational substrate). The ACT components, cohesion, morale, performance, and will, are not produced by detection systems or regulatory architecture; they are produced by social trust, civic association, emotional regulation capacity, identity resilience, the equity and quality of education, and the conditions of the resilient societies the manuscript names throughout. Adversary operations targeting cohesion and will are operations against the lower foundation and Layer 1 directly. The defensive answer is the deliberate cultivation of the conditions that produce cohesion, morale, and will in the first place.

Decision advantage operates primarily at the upper foundation (political will and elite coherence) and Layers 4, 5, and 6. The ACT component, situational understanding and decision making, requires intelligence-grade detection (Layer 4), active defence through attribution, exposure, and cost imposition (Layer 5), and the legislative, doctrinal, regulatory, and institutional instruments that protect democratic decision-making from foreign interference (Layer 6), all anchored above by political will and elite coherence sufficient to authorise sustained action across the continuum of competition. Decision advantage cannot be denied without the upper foundation in place. A government that does not understand the threat, or that understands it but cannot maintain coherent commitment to acting on it, concedes decision advantage at the apex of the architecture.

The triad-to-architecture mapping clarifies the manuscript's institutional argument. Adversaries pursue the three forms of advantage simultaneously and continuously. The defensive architecture must therefore be simultaneously and continuously built across all six layers and both foundations. Episodic, single-layer, or single-advantage-focused responses are structurally inadequate to the threat the doctrine names.

A Note on Analytical Perspective

The six-layer model is a defensive analytical tool, not a mirror of how adversaries plan. Adversaries think in vulnerabilities and opportunities, not in defensive layers. They scan democracies for the weakest point in the information environment, the most exploitable fracture in social cohesion, the least accountable platform architecture, the most under-resourced detection capacity. A further clarification is important here. Threats differ not only in actor but in volume and consequence. High-prevalence, lower-offline-harm threats, coordinated inauthentic behaviour and volume disinformation, operate primarily at Layer 2 and require Layer 2 responses. Low-prevalence, higher-offline-harm threats, targeted elite operations and critical infrastructure attacks with cognitive objectives, operate at Layers 4 and 5 and require a different response architecture entirely. Conflating the two produces institutions that are neither fast enough for volume threats nor precise enough for capability threats.

The Systems-Theoretic Rationale

Rather than a single catastrophic failure, cognitive warfare works to produce compounding erosions in social trust, institutional legitimacy, and political cohesion that defeat democratic resilience through accumulated weight rather than a decisive blow. The NATO STO's technical baseline for cognitive warfare establishes this cumulative and systemic character. Degradation operates across populations and institutions simultaneously, with no single point of failure capturing what is being lost. NATO analytical discourse has begun describing this trajectory as*cognitive degeneration*: not a single moment of deception but a progressive degradation of the epistemic conditions under which democratic deliberation is possible, manifesting as declining institutional trust, the fragmentation of shared factual baselines, and the growing inability of populations to distinguish credible from non-credible sources. Democracies optimising for

large, visible events systematically under-prepare for the slow-moving failures cognitive warfare actually produces. Michlin-Shapir's analysis of the pathway from private unhappiness to public outrage documents how this cascade operates at the population level: the mechanisms adversaries exploit are also generated endogenously by the conditions of modern democratic life, and the emotional substrate populism mobilises is the same substrate cognitive operations target.[7] Multi-layer defence creates multiple independent intervention points across the cascade, and ensures that no single failure collapses the entire architecture.

The chapters that follow examine, country by country, how the leading democracies have built each layer, where they have failed, and what Canada, Germany, and all other liberal democratic Allies and partners must do differently.

The architectural argument in this report is that the lower foundation (social infrastructure) and Layer 1 (the human-relational substrate) together constitute the operational substrate of the population resilience clause that NATO doctrine names but no Alliance member has yet operationalised at scale. The clause is doctrinally settled. The operationalisation is not built. This manuscript is the first comprehensive operationalisation built for a NATO member, with Canada and Germany as the primary addressees.

Endnotes

1 NATO Science and Technology Organization, Mitigating and Responding to Cognitive Warfare (STO-TR-HFM-ET-356), edited by Yvonne R. Masakowski and Janet M. Blatny (NATO STO, March 2023). On the protection-detection-response triad, see also Bernard Claverie and François du Cluzel, 'Cognitive Warfare: The Future of Cognitive Dominance,' NATO Allied Command Transformation, 2022.

2 NATO Allied Command Transformation, working definition of cognitive warfare and associated definitions of cognitive advantage, narrative advantage, psychological advantage, decision advantage, and full-spectrum approach. Provided to the author by NATO ACT, May 2026. These definitions have not yet been processed through the NATO Standardisation Office.

3 Christian Fjäder and Johan Schalin, Building Resilience to Hybrid Threats: Best Practices in the Nordics, Hybrid CoE Working Paper 31, European Centre of Excellence for Countering Hybrid Threats, 27 May 2024.

4 North Atlantic Treaty, Article 3, signed at Washington, D.C., 4 April 1949.

5 NATO Office of the Chief Scientist, Chief Scientist Research Report on Resilience (NATO STO, December 2025), and Chief Scientist Research Report on Cognitive Warfare (NATO STO, December 2025).

6 Emmanuel Macron, remarks at the All India Institute of Medical Sciences, New Delhi, 18 February 2026.

7 Vera Michlin-Shapir, 'From Private Unhappiness to Public Outrage: The Emotional Origins of Twenty-First-Century Populism,' Defence Strategic Communications, Vol. 16 (Autumn 2025): 245 to 266, DOI 10.30966/2018.RIGA.16.8.

Chapter 6: The Lower Foundation: Social Infrastructure and Societal Resilience

The social infrastructure foundation is not a metaphor. It is the substrate on which every layer of cognitive defence depends. Countries with strong social infrastructure, deep civil society networks, and populations that experience their institutions as caring about their wellbeing are structurally harder to manipulate. Countries where citizens feel unseen, excluded, or abandoned are structurally easier. No detection system, no media literacy programme, and no counter-messaging operation can compensate for that deficit. Democracy is not simply its institutions. It is the fabric of society in which trust exists, and that fabric is extraordinarily hard to build and surprisingly easy to destroy. A population that has lost the common sense that their society cares about them has no cognitive reserve to draw upon when adversaries offer an alternative explanation for their pain. The adversary does not need to persuade them. The adversary only needs to be there when the state is not.

Connection as the Root of Cognitive Resilience

Every psychological need this report identifies as an adversary attack surface, from security and belonging to esteem, meaning, and identity, is fundamentally a need for connection. Adversaries succeed not by providing superior arguments but by exploiting the absence of connection. The citizen who has lost the felt sense of being seen by their government or by other members of society, included in their community, or supported by their economy is not persuaded by adversary narratives. They are offered a mirror for pain they already carry. No amount of counter-messaging can compete with manipulation that validates lived experience.

The biological evidence grounds this claim in physiology rather than sentiment. Research from the University of Cambridge shows that under conditions of social threat show that populations with stronger social bonds demonstrate measurably different physiological responses to stress. In a study of approximately 42,000 adults, the research identified 175 proteins associated with social isolation linked to inflammation, cardiovascular disease, and early mortality.[1] Societies of disconnected people are more than just psychologically vulnerable, they are physiologically weakened. The Layer 1 investment

argument is, at its foundation, an argument about population health. Our argument is that cognitive defence at the foundational layer is a care problem. Governments and societies that care for their people structurally produce citizens who will defend them. Healthcare, accessible childcare, education that is genuinely accessible, that fosters belonging as well as competence, and that builds critical thought alongside knowledge, economic policy that ensures dignity, elder care: these are not soft policy. They are the foundational infrastructure of cognitive resilience and are therefore key to any democratic country's national security in the digital age. The Nordic models this report holds up as benchmarks are, at their core, care economies. Our formulation of the causal chain is that trust follows from care and resilience follows from trust, and that adversary operations systematically target the gap between what democratic institutions promise and what they deliver.

The empirical grounding for this argument is more precise than the general social cohesion literature provides. Time on social media does not reliably predict affective polarisation. Job loss does, with a lag of several years. Economic dislocation, experienced as a breach of the social contract that structures individual dignity and daily meaning, predicts the kind of affective polarisation that adversary operations then amplify and redirect. Counter-messaging and digital literacy programmes cannot close a vulnerability that originates in economic experience rather than information exposure. The care economy argument is not a welfare argument dressed in security language. It is a security argument grounded in the empirical finding that economic precarity is the primary structural condition adversaries exploit.

The structural mechanism by which Layer 1 was hollowed out has been named with precision by Admiral Rob Bauer, former Chair of the NATO Military Committee, and strategic communications advisor Eleanor Russell. Writing in 2025, they observe that democratic societies outsourced security to armed forces in exactly the same way they outsourced healthcare, energy production, and public transport to the private sector, for reasons of efficiency, with the effect that citizens came to believe their tax payments discharged their responsibility entirely.[2] The cognitive consequence is the same as the economic one: when the outsourced function fails or is overwhelmed, the population has no reserve capacity to draw on. Citizens who have been relieved of the felt responsibility

for their own security are not merely passive. They are structurally unprepared. Russell names the resulting condition with equal precision: the problem is not a lack of urgency, but a lack of confidence in the capacity to act. A population that has concluded it cannot affect outcomes is in a fundamentally different cognitive position from one that simply has not been asked. Urgency without agency produces paralysis. This is the condition that adversary operations are specifically designed to exploit and deepen: not to persuade democratic populations of anything in particular, but to confirm their existing conviction that collective action is futile and that nothing they do will matter. The care economy argument this chapter makes is, at its foundation, an argument about restoring the conditions under which citizens can believe that what they do matters. That is not a therapeutic aspiration. It is the precondition for Layer 1 to function at all.

Citizenship is not an administrative status. It is an experience of belonging. Communities without political voice are vulnerable to the narrative that the system is rigged because that narrative describes their experience. When that experience is absent, democratic participation becomes optional in the worst possible way.

Emotional Self-Regulation as Foundational Resilience Infrastructure

In this report, we argue that beneath connection lies a deeper layer: the individual capacity for emotional self-regulation, the ability to distinguish between reacting to a stimulus and responding to it. It is our architectural claim that emotional self-regulation treated at population scale is cognitive defence infrastructure at the deepest available layer, is the load-bearing argument of this chapter. Adversaries design cognitive intrusions not to be analysed but to be felt. The objective is to provoke an emotional reaction that bypasses the deliberative faculties. A citizen in acute fear, outrage, or moral disgust is not evaluating evidence. They are responding to a threat signal that forecloses reflection. The mechanism is what Kruglanski terms ‘seizing and freezing’. Under conditions of acute threat, the mind reaches for the first available certainty and closes off further processing.[3]

When citizens are in acute fear or threat states, the prefrontal cortex disengages, a stress response mechanism documented in C. Sue Carter’s research on oxytocin and threat physiology. Access to logic, reasoning, empathy, and forward thinking are lost. Adversaries design operations to trigger exactly this state because reaction forecloses

reflection. Media and digital literacy address the information layer. Emotional self-regulation addresses the human layer beneath it. A citizen who can notice that they are experiencing a spike of outrage, pause before acting on it, and ask whether that outrage was engineered to produce exactly the reaction they are about to have, is structurally harder to manipulate. This is not therapy dressed as policy. It is the recognition that the attack surface adversaries exploit is emotional before it is informational.

The scale of the underlying problem is considerable. The Sapien Labs Global Mind Health Report, drawing on survey data from more than one million respondents across 84 countries, documents measurable decline in emotional regulation capacity among adults under 35 across the preceding five years, with the trend concentrated in high-income democracies. Canada and Germany perform above the global average on emotional regulation capacity, but the Sapien Labs data show the trend line is nonetheless downward in both countries among younger adults. A measurable decline in the capacity to regulate emotional responses in the very democracies this report addresses represents an expansion of the cognitive attack surface that democratic defence frameworks have not yet systematically addressed.[25]

Denmark provides the institutional proof of concept. Klassens Tid, a long-standing Danish school practice embedded in the structural framework of the Folkeskole, allocates approximately one lesson per week at each grade level to the life of the class. Children from early grades learn to identify and articulate their own emotional states, practice perspective-taking, and navigate conflict through dialogue. It is not framed as security infrastructure. It functions however as security infrastructure at the deepest available level because it intervenes at the precise point where adversary operations succeed.

Canada also has its own example. Roots of Empathy, founded in Toronto in 1996 by Mary Gordon, operates in more than 3,000 classrooms across Canada and internationally. A child who has spent a year learning to identify emotional states in another person, and to distinguish reactive response from deliberate choice, is building exactly the capacity that cognitive warfare is designed to defeat. Most democracies in this research set have foundational pieces of this kind. The gap is framing: none yet treats emotional regulation

as explicit cognitive defence infrastructure, and none has built the institutional mandate to deliver it universally.

Unaddressed private distress migrates into collective pathology. Adversaries do not need to generate grievances, only to ensure existing distress finds a political outlet they have pre-shaped. This is not a substitute for investment in mental health services, which the evidence reviewed here makes clear are both underfunded and structurally linked to cognitive vulnerability at the population level. It is the recognition that the emotional attack surface adversaries exploit requires an institutional response beyond the healthcare system.

During the author’s field research for this report, there was consistent convergence across practitioner and academic sources from different national contexts and disciplinary backgrounds on emotional self-regulation as the most underrepresented dimension in existing democratic resilience frameworks. Sources spanning Norwegian defence research, Canadian clinical psychology, and NATO cognitive warfare concept development each identified the same gap from their distinct disciplinary vantage points. None of the gold-standard Nordic models yet frame emotional regulation as explicit cognitive defence infrastructure. Evidence from practitioners who were central to the NATO cognitive warfare concept development process independently identifies this dimension as the most underrepresented in the entire literature on democratic resilience. No democracy yet treats emotional self-regulation as explicit cognitive defence infrastructure. We recommend that Canada and Germany take up the leadership.

One further mechanism deserves naming here because it is analytically distinct from the rest of the emotional regulation argument and is consistently underweighted in the policy literature: self-censorship as the deepest form of cognitive intrusion. Michlin-Shapir's analysis of the pathway from private unhappiness to public outrage demonstrates how individual emotional distress, when it lacks constructive political outlet, migrates into radicalisation: adversaries do not manufacture this pathway, they find it pre-existing and amplify it. Brute force removal of voices and blocking of content are visible and contestable. Self-censorship is neither. It occurs when individuals modify or suppress their own expression not because they have been directly silenced but because the

information environment has been manipulated to make dissent feel unsafe, isolated, or futile. A citizen who can identify a disinformation campaign may still self-censor if perceived social norms around them have been artificially shifted toward distrust, disengagement, or anger. The intervention point is twofold: timely exposure of the manipulation producing the distorted norm perception, and building confidence and capacity in target populations so that individuals can sustain their own voice under sustained adversarial pressure. This connects directly to the emotional self-regulation argument: adversaries rarely need to change individual beliefs. They need to change what people believe about other people's beliefs. Self-censorship is where that norm shift produces its most durable effect, because the population itself carries the suppression forward without further adversary effort.

Building the Foundation: Education, Culture, Service, and Civilian Capacity

Five institutional mechanisms build and sustain Layer 1 capacity at population scale. Five mechanisms are available to democratic governments. Empathy education, as Klassens Tid and Roots of Empathy demonstrate; critical thinking, as Finland's national curriculum has systematically embedded since its curriculum reform, adopted in 2014 and implemented from 2016; and digital literacy, as Estonia's approach to civic and digital education makes explicit. Each requires a long-term commitment to build, and they are the only interventions that change the baseline resilience of the entire population over time. Arts and cultural production create shared emotional reference points that feel organic rather than imposed. This precisely what cognitive warfare targets. In Canada, Gord Downie, a famous musician, used his final concert to raise awareness of the Secret Path project on the story of Chanie Wenjack, an indigenous victim of Canada's residential school system. This on action did more to shift the national conversation on Indigenous reconciliation than a decade of policy documents had managed to do, because it arrived not as an argument but as an experience. In Germany, a generation of Turkish-German writers including Feridun Zaimoglu have created the shared cultural vocabulary through which integration debates that once felt irresolvable became navigable. Adversaries understand that shared story is the substrate of social cohesion. Defunding arts is not a budget decision. It is a defence vulnerability.

National service creates, through shared experience, the cross-class, cross-community relationships that make whole-of-society mobilisation possible when needed. Finland's comprehensive security model depends on a population that has experienced collective service. Estonia's Kaitseliit, 26,000 volunteer members integrated into total defence, or similarly, Lithuania's Šauliai paramilitary voluntary organisation, demonstrate the distributed civilian reserve capacity that whole-of-society frameworks require. Citizens who have shared an experience of responsibility and contribution are structurally harder for adversaries to fracture along identity lines.

A cautionary counterpoint from the Baltic research demands space here. Lithuania's institutional architecture, the most operationally precise in the research set on calibrated narrative response, has produced alongside its genuine strengths what Lithuanian practitioners call the passive citizen problem: a population that trusts institutions to monitor, attribute, and respond, and which has therefore reduced its own investment in individual cognitive vigilance. If the institution is captured, overwhelmed, or simply absent during rapid escalation, the population trained to defer to it has no individual reserve. The Nordic and Baltic models this report recommends are genuinely transferable. The passive citizen risk is the caveat that must accompany the recommendation: institutional architecture and individual capacity must be built in parallel, not sequentially.

A further capacity-building instrument is civilian reserve capacity in the cyber domain. Estonia's Cyber Defence Unit is the model: IT professionals maintaining civilian careers but activatable for national cyber defence. Most advanced democracies have the private-sector cyber talent to replicate this model. Financial institutions, technology companies, and critical infrastructure operators in every major democratic economy hold in-house expertise that civil society organisations urgently need. The professional expertise exists. The interface architecture that connects it to national defence planning is what is typically missing.

Lithuania's commandant units offer the institutional model for the pre-crisis personnel gap that all democratic militaries face. These volunteer security units are specifically designed to provide trained civilian capacity activatable in the period between the escalation of a cognitive or hybrid threat and the point at which formal military mobilisation would be

authorised. They fill the institutional seam that adversaries specifically target: the window when a threat is clearly underway but has not yet crossed the threshold that triggers formal response. The commandant model is the civilian cognitive reserve equivalent of Estonia's Cyber Defence Unit, not a military force, not a civilian bureaucracy, but a trained volunteer capacity that bridges the gap between the two. Canada's voluntary sector, professional associations, and academic networks provide the raw material for exactly this kind of activatable reserve. What is missing is the institutional mandate and the training architecture.

The report also identifies emotional regulation capacity among those who work most closely with children, and among those in high-stress public-service roles, as an underinvested foundation of societal resilience. Teachers are the clearest example. They spend more waking hours with children than almost any other adult, so investment in their emotional regulation capacity carries a multiplier effect across every student they teach, and its absence compounds across successive cohorts. The wider principle holds beyond the classroom: where a society builds the emotional regulation capacity of the adults its children depend on, and of those it asks to absorb sustained stress on its behalf, it is building civilian infrastructure of cognitive resilience, not delivering a soft social good. Public investment of this kind produces returns that extend across the population over time rather than remaining bounded by any single programme or institution. The recommendations for Canada in Part V develop the institutional architecture for delivering this investment.

Ukraine provides an excellent example of comprehensive resilience. Layer 1 is not a supplement to conventional defence. It is the precondition for conventional defence to function at all. Ukrainian cultural production since 2022 is cognitive defence at its deepest level. First and most essentially, it has helped sustain the civilian population's will to resist through conditions of deliberate terror. Russia's systematic targeting of Ukraine's energy grid across successive winters was both a material strategy and a cognitive strategy: the objective was to break the population's will to resist by making survival incompatible with sustained collective action. The response was to maintain cultural life, community ritual, and collective expression under bombardment. Communities finding ways to gather in the dark, to mark occasions, to create and share art about what they were living through: this

is not sentiment or footnote. It is the mechanism by which civilian will to resist remained available to sustain military capacity through conditions designed to break it. The armies that continued fighting did so, in part, because the societies behind them held. That is the foundational proposition this chapter advances. The secondary function of Ukrainian cultural production, making Ukraine's cause emotionally legible to allied populations and sustaining international political will across electoral cycles in donor countries, is real and important. But it follows from the primary one. Countries that defund their arts, hollow their civic education, and ignore their social fractures are weakening their own Layer 1. Ukraine did not. And that is, in part, why its military capacity held. The same logic applies to the information infrastructure of the civic environment. Canada has lost more than 250 net local news outlets since 2008, concentrated in rural, Francophone, and smaller communities that are precisely the adversary attack surfaces this chapter has described. The Public Policy Forum's analysis of this collapse documents what it calls information vacuums in communities that have lost their local press. Those vacuums do not remain empty. They are filled.

The Vocabulary of Defence and the Whole-of-Society Requirement

A structural vulnerability that appears across multiple national contexts in the research conducted for this report is the semantic stock gap: citizens frequently lack the vocabulary to describe what is happening to them in the information environment. Without shared language to name algorithmic manipulation, cognitive overload, and epistemic fragmentation, it is impossible to build either individual resilience or collective policy responses. Building that vocabulary is a foundational public education obligation, achieved through public communication and civic education curricula.

The vocabulary problem has a deeper structural dimension that the semantic stock gap framing does not fully capture: the gap between what governments know and what they tell their populations. Field research conducted for this report finds the same pattern across the practitioner conversations it draws on: there is a consistent and widening gap between the threat landscape that governments and military institutions understand and the awareness that individual citizens have of how profoundly that landscape has shifted. Most citizens do not know that the information environment they navigate daily is a

domain of active strategic competition and manipulation. Most do not know that the platforms they use for entertainment and social connection are simultaneously the primary terrain on which adversaries are operating. Most citizens do not realise they are under a constant state of cognitive attack. Governments understand this. They are not communicating it. The failure is not always deliberate concealment: it is often structural. Knowledge is siloed within intelligence and defence communities. The analysts who understand the threat in operational detail may have no mandate, no channel, and no budget for public communication. The officials with public communication platforms may not have been briefed to the level of detail that would make the communication meaningful. And the political level may genuinely not know what the public service who report to them knows. Ministers and their staff manager an impossible caseload across myriad files daily. In the absence of an outside signal strong enough to cut through, information is often not relayed to them. That structural reality does not eliminate political responsibility. It names where the intervention point must be: the signal architecture that ensures cognitive threats reach the political level before they reach the public. Things fall through the cracks, are not deemed an operational priority, or simply do not travel up the chain from the analysts who understand the threat to the superiors who brief the ministers. The reasons are often structural rather than malign or negligent. But the cumulative effect is that a concept like cognitive warfare, invisible by design, producing no single catastrophic event that forces its way onto the agenda, rarely acquires the political salience it warrants until the damage is already done. The result is that citizens are expected to be able to defend themselves against a threat they have not been told they are facing, using capacities they have not been helped to build, in an environment they have not been equipped to recognise as hostile. That is an abdication of responsibility. The single most immediately actionable change any democratic government can make to its cognitive defence posture is to close this gap: to communicate clearly, consistently, and accessibly to its own population the nature of the contest that they are already facing.

Cognitive warfare is whole-of-society warfare in a way that previous forms of warfare have not been. In earlier conflicts, citizens were affected by war but were not the primary target, the primary terrain, and the primary line of defence. In cognitive warfare, all three are true at once. Governments cannot defend citizens against cognitive warfare by acting on their

behalf. They can only build the conditions in which our institutions can empower citizens to defend themselves. That is Layer 1. The chapters that follow will show how Layers 2 through 6 can only be built on this foundation. If the foundation is weak, nothing built on it holds.

Endnotes

1 Shen, C., Zhang, R., Yu, J. *et al.* Plasma proteomic signatures of social isolation and loneliness associated with morbidity and mortality. *Nat Hum Behav* **9**, 569–583 (2025). https://doi.org/10.1038/s41562-024-02078-1

2 Rob Bauer and Eleanor Russell, *If You Want Peace, Prepare for War: A Blueprint for Deterrence*, 2025. The "lack of confidence" formulation is Russell's own phrasing, from the FPRI *Ties That Bind* podcast, 2026.

3 Arie W. Kruglanski and Donna M. Webster, 'Motivated Closing of the Mind: "Seizing" and "Freezing,"' Psychological Review 103, no. 2 (1996): 263–283.

Chapter 7: From Resilience to Response

Resilience is necessary but not sufficient. A democracy that invests exclusively in absorbing attacks, building citizen capacity, strengthening institutions, and improving media literacy, without ever imposing costs on the adversaries conducting those attacks, is providing a free laboratory for calibrating what works. Every operation that succeeds teaches the adversary something. Every operation that fails costs it next to nothing. Deterrence in any domain requires that failure hurts. The resilience-only model does not hurt anyone but the democracy it is meant to protect. The very cheapness of cognitive warfare attacks compounds this structural problem: when failure costs an adversary almost nothing, resilience-only posture does not deter, it subsidises.

The second structural problem compounds the first. Russia's shadow warfare is not a strategy but a system: its institutional logic converts every outcome, whether success, failure, or exposure, into justification for more activity. This systemic character, documented by Sam Greene, Andrei Soldatov, and Irina Borogan in their comprehensive analysis of Russian hybrid operations, distinguishes it from strategic campaigns that can be deterred at the operational level. Exposure validates relevance. Disrupted operations demonstrate resolve. A machine that converts disruption into validation is not deterred at the operational level. Effective deterrence requires imposing costs at the strategic level, not at the operational one.

The Resilience-Only Trap

Democratic governments, in the formulation of Latvian politician, historian, and former Minister of the Interior Marija Golubeva, are awake but groggy.[1] Awareness of the threat is present. The institutional architecture to act on it is not. The pattern is consistent: cognitive defence capabilities activate at moments of acute political pressure, typically elections, and stand down when the deadline passes. Sweden's Psychological Defence Agency, Lithuania's eleven coordinating institutions assessing narratives weekly, and Estonia's integrated approach represent genuine advances. What they share with the election-integrity architectures of Canada, Germany, and others is a structural mismatch: machinery built for a threat that intensifies at predictable moments, deployed against one

that does not. Cognitive operations run 365 days a year. Episodic machinery cannot address a continuous threat. The gap is architectural, not one of capability.

The architectural mismatch is a refusal of the continuum-of-competition framing that NATO Allied Command Transformation has now made doctrinally explicit. Cognitive warfare, in ACT's working definition, comprises "deliberate, synchronized military and non-military activities throughout the continuum of competition," which means activities that do not pause between elections, between crises, or between formal periods of conflict. Episodic detection machinery rejects this framing structurally: it is built for discrete events, not for the continuous competition the doctrine describes. The Carney government's March 2026 commitment to year-round Rapid Response Mechanism Canada detection, replacing the election-period-only posture, is the first Canadian institutional acceptance of the continuum framing. It is necessary but not sufficient. The continuum framing applies across all six layers, not only the detection function.

Layer 1 cognitive resilience is built continuously through social infrastructure and emotional regulation capacity. Layer 2 information environment integrity through sustained investment in journalism and media literacy. Layer 3 platform accountability through continuous regulatory engagement. Layer 4 detection through year-round monitoring. Layer 5 active defence through standing attribution and cost imposition capacity. And, Layer 6 sovereign response through legislative, doctrinal, and institutional instruments designed for sustained rather than crisis-mode operation. Each layer either operates on the continuum or it operates not at all. Episodic versions of any of them produce the same architectural mismatch detection-only systems already exhibit. The continuum framing is doctrinally reinforced by the CCDCOE 2026 paper's argument for what its authors call constitutive invisibility: cognitive warfare is invisible by design, not by accident, because the target experiences induced changes as endogenous evolution rather than as external attack.[2]

This is the structural reason the detect-attribute-respond loop fails in isolation. Defence must move upstream to the proactive preservation of institutional coherence before any of its components has been compromised, which is exactly what continuum-of-competition operation across all six layers requires. Marcus Kolga, Jennie Phillips, Brian

McQuinn, and Bartel Van de Walle articulate the Canadian-vernacular version of the same architectural diagnosis in their May 2026 report Decision Making and National Unity Under Threat: “Foreign adversaries systematically exploit these vulnerabilities, moving at algorithmic speed, while Canada’s institutional response remains slower, fragmented, and often reactive.” The speed asymmetry they name is the operational signature of the continuum-of-competition mismatch in Canadian institutional conditions.

The deterrence gap is now acknowledged from within the US military establishment itself. Sam Gray, Chief Technology Officer of the US Strategic Capabilities Office, stated publicly in March 2026 that the United States cannot counter adversarial cognitive warfare at machine speed and is behind from the technology perspective. Gray's disclosure concerns the Basic Information Awareness Operations project, which targets AI-driven population modelling, multimodal synthetic content generation, and adversary behaviour emulation using bespoke models tuned to replicate Russian and Chinese cognitive patterns. The acknowledgment that the most capable Allied nation is technologically behind its adversaries in this domain is the strongest available external validation of this chapter's core argument. It also introduces a tension this framework does not resolve but names: the same government whose military establishment has made this admission is simultaneously conducting influence operations against Allied democracies. A proactive intelligence-led posture is the architectural alternative to the detect-respond-recover model.[3] Every detect-respond-recover cycle begins with a successful adversary operation: failure is the precondition for the mechanism to activate. A proactive posture identifies adversary intent and capability before the operation deploys and disrupts it at the infrastructure layer. A democracy that waits to be attacked before it begins to defend is conceding the ground permanently.

Active Defence: Detection, Attribution, Exposure, Cost Imposition

Before the architecture of active defence can be described, its foundational principle requires stating. Every military textbook opens with the idea that you do not permit the adversary to build infrastructure on your territory. Applied to cognitive defence, the principle is equally direct: the adversary has spent years building networks, embedding within media systems, cultivating political relationships, and establishing amplification

infrastructure inside democratic societies. The first operational priority is not to counter their narratives. It is to deny them the infrastructure through which those narratives travel. Dismantling adversary cognitive infrastructure, the networks, the funding flows, the platform presences, the embedded influence nodes, is area denial at the cognitive layer. It has nothing to do with censorship of legitimate discourse. The adversary is not hiding. The infrastructure is visible. The choice is whether to act on what is already known.

Active defence comprises four sequential components.

Detection means identifying operations in progress, which requires acting on pattern recognition rather than waiting for certainty. One of the author's interviewees, who works in civil society and has monitored Russian information operations continuously since 2014, has named this 'narrative intelligence.' The methodology treats narratives as an intelligence product analogous to SIGINT or HUMINT. Analysts track volume, intensity, and thematic drift across time and language environments, extrapolate to adversary operational intent, and use the resulting picture for both political and military prediction. The practitioner describes predicting Russia's full-scale invasion of Ukraine on the basis of narrative volume and intensity alone, months before the kinetic operation began. The same methodology applied to Donetsk and Luhansk in the preceding years showed that what Russia was saying through its information channels directly anticipated what its military subsequently did on the ground. Narrative intelligence is a practitioner-developed methodology with a decade of operational application. What it requires institutionally is the analytical capacity to treat narratives as intelligence, and the mandate to act on pattern recognition rather than waiting for the evidentiary standard that adversary operations are specifically designed to deny. The practitioner also articulates the system's architecture on two axes simultaneously.

Horizontally, where narratives are connected to each other across language environments, reinforcing and referencing one another, living their own life in communities the originating actors may no longer be actively maintaining; and Vertically, which are narratives connected upward to diplomatic positions, political discourse, and military action on the ground. The vertical integration is what the West missed. Russia was not running parallel tracks of information operations and military operations. It was running a

single integrated campaign in which the information layer directly anticipated, enabled, and followed kinetic action. The Donetsk and Luhansk narrative analysis made vertical integration visible. Democratic detection architecture is built for the horizontal layer. It is almost entirely blind to the vertical one. Most democratic security agencies were built to respond once causation is established, not when probability is sufficient. Adversary operations are specifically designed to exploit that threshold. No single signal may be attributable to hostile intent. But a combination of coordinated amplification across platforms, inauthentic account behaviour, narrative alignment with adversary geopolitical objectives, and unusual timing patterns raises the probability of adversarial involvement to a level that warrants defensive response. Detection institutions must be designed to act on that combined picture rather than waiting for the kind of definitive proof that cognitive operations are engineered to deny.

Attribution means determining responsibility with sufficient confidence to act, not certainty as a precondition. The UK's experience offers a cautionary design principle: after the Chilcot Report, the attribution process was redesigned to require confirmation that can take two years, by which point the operation has achieved its intended effect. Democratic attribution architecture must avoid both failure modes, pre-Chilcot politicisation and post-Chilcot paralysis. The methodological tools now exist. A joint NATO StratCom COE and Ukrainian Centre for Strategic Communications framework provides a structured attribution methodology designed for the epistemological conditions of FIMI rather than for conventional warfare. Democracies must build and share it.

Exposure means making operations public, and the evidence that public exposure works is strong. Lithuania's calibrated narrative response system is the most operationally specific. It features eleven institutions sharing a common methodology rating narrative on a scale from ‘no response’, for low-reach content (debunking amplifies it), through to responses from academic contacts, ministry experts, senior officials, and head-of-state intervention at the highest reach. Not every piece of disinformation warrants an institutional response, and responding to low-reach content does the adversary’s amplification work for it. Ukraine's response to former Hungarian Prime Minister Orbán's sustained narrative against Ukraine and Europe's contribution to its defence illustrates what this looks like at a national scale. In April 2026, Ukraine's Ministry of Foreign Affairs

launched Hungarian Radio Ukraine, a dedicated 24/7 Hungarian-language online broadcast explicitly countering what it described as misleading narratives from the Hungarian government. The platform is a direct application of the detect-and-respond architecture this framework recommends, deployed by a country under active cognitive attack against an adversarial narrative operation conducted through a nominal Ally.

Cost imposition means making adversary operations genuinely expensive through diplomatic, economic, sanctions, legal cases, and regulatory measures. The Estonian model of prompt, calibrated, public attribution demonstrates that exposure itself is a form of cost imposition by degrading the operational credibility of the adversary's next campaign. Lithuania's approach extends this logic further through its coordination architecture to ensure exposure decisions are calibrated, rapid, and authorised at the appropriate level without requiring military approval chains. Demonstrating that speed and democratic accountability are not in tension when the institutional design is right.

The Three-Tier Offensive Framework and Democratic Constraints

One conceptual clarification is necessary before the architecture can be named. As Tanna Krewson, who led the development of NATO's cognitive warfare concept through Allied Command Transformation, has argued, cognitive warfare is the fight, not the tool.[4] Democracies are not doing cognitive warfare to their adversaries. They are defending against the cognitive warfare being waged against them, using tools that already exist: strategic communications, psychological operations, counter-influence, cyber. Those tools need to be upskilled and retooled for the environment in which they now operate. This distinction matters because it resolves the political objection that has paralysed allied investment in this domain. The fear of becoming what we oppose is a fear about narrative operations directed at civilian populations, not about building deeper understanding of adversary societies, removing adversary infrastructure, or developing latent wartime capability that remains dormant in peacetime. When cognitive warfare is understood as the fight rather than the toolkit, the ethical debate that has frozen institutional progress becomes less paralysing and more tractable. Field research from within the Alliance's cognitive warfare concept development process is direct on this point. We are more at risk of doing too little because of these ethical debates than we are of doing too much.

The democratic constraints are real and must be maintained. The paralysis they have generated is not a sign of moral seriousness alone. The fear underlying it is well-founded. Democratic governments that conduct influence operations against their own populations have crossed a line that is genuinely worth defending. But the paralysis that results is also a strategic vulnerability, and the adversary depends on democratic allies never resolving that tension. It is a strategic vulnerability.

The minimum viable capability package for closing the three-of-thirty-two offensive capability gap is neither expensive nor technically complex. Field research from within NATO's operational structure identifies eight components: information environment assessment capacity, to understand the audiences and systems in which operations are being conducted; narrative intelligence analysts, who track narrative volume, intensity, and drift across language environments in real time and extrapolate to adversary operational intent, the function that most closely approximates what intelligence agencies do with signals applied to the information domain; behavioural science expertise, covering the cognitive and psychological levers that determine how people process information and form judgments; clinical psychologists with expertise in adversary population vulnerability and democratic audience resilience, distinct from the academic behavioural science layer and essential for operational application; cultural historians and linguistic analysts who can translate adversary society, memory, and identity into operational understanding; writers and creatives who can produce content that moves through a society rather than content that reads like a government communication, the execution layer that translates campaign strategy into material that finds its audience; information planners who can translate that understanding into coherent campaigns; and effect assessment methodology, to evaluate whether operations are achieving their intended impact. What is missing from twenty-nine Allied nations is not the money to build these components. It is the career streams to develop the expertise, the dedicated institutional homes to house it, and the political will to activate it in peacetime rather than treating it as a wartime-only capability. A further dimension compounds the structural barrier. Many practitioners do not understand the adversary's strategic logic for deploying these tools. Cognitive operations are not designed primarily to change minds. They are designed to paralyse decision-making, fracture social cohesion, and degrade the will to resist.

Practitioners who understand cognitive warfare as an information problem will build information responses. Practitioners who understand it as an attack on the preconditions of democratic governance will build something more adequate to the threat. A country can and should begin building this package before it has resolved every normative question about how it will eventually be used. The capacity-building decision and the deployment decision are fully separate. Not building the capacity now means it cannot be used when needed.

Field research at Allied Command Transformation calibrates the self-limiting concern within the Alliance more precisely than the standard discussion captures. The primary institutional bottleneck on building offensive cognitive capability is not the ethical constraint relating to adversary civilian populations, although that constraint is real. The primary bottleneck is the domestic concern: how cognitive defence capability would interact with allied populations, and the unresolved question of which part of government owns the cognitive defence mandate. Whether the function sits inside the military, the civilian intelligence community, the foreign ministry, the interior ministry, or a dedicated agency is, in most allied capitals, the question that has not been answered. The adversary-facing ethical constraint can be addressed through legislative limits and Tier three doctrine. The domestic mandate question requires institutional architecture that most allied governments have not yet built. Naming the bottleneck precisely is the precondition for resolving it.

Field research conducted at Allied Command Transformation identifies four strands of capability development of which the people and personnel strand addressed above is one. The four are: first, people and personnel, the eight-component package set out above; second, technical capabilities, primarily artificial intelligence, covering the capacity to develop, acquire, operate, protect, and govern AI systems within an ethical framework; third, coordination and synchronisation capacity, addressing how to deliver effects at operational and strategic scale across military and non-military actors; and fourth, cutting-edge science and industry integration, encompassing brain science, wearable technologies, and virtual and augmented reality systems that are already reshaping the cognitive environment of conflict. The minimum viable capability package this chapter

identifies is a necessary starting condition. These four strands represent the full scope of the investment challenge.[5]

The military dimension of active defence operates on three tiers. Tier one is continuous peacetime defence, a dedicated cognitive defence agency conducting open-source monitoring, public education, civil society coordination, and 365-day threat assessment, replacing the current episodic model. Tier two is active response below the kinetic threshold, targeting adversary infrastructure rather than adversary minds. Taking down botnets, sinkholing domains, freezing financial networks that fund influence operations, removing inauthentic accounts at scale. This extends what Allied cyber agencies already do under existing cyber authorities to the semantic layer above the network layer. It removes the plumbing of adversary operations.

Most NATO Allies have already authorised offensive cyber operations. The same logic applies one layer up. Tier two also encompasses something democracies have systematically under resourced: deep knowledge of the adversary. This is not a licence for offensive manipulation. It is an analytical imperative. Adversaries know democratic societies with extraordinary granularity, built on decades of investment in understanding Western psychology, cultural fault lines, historical grievances, and media ecosystems. Democratic governments have chronically underinvested in understanding their adversaries at equivalent depth. The intelligence community collects. The analytical capacity to translate collection into genuine understanding of adversary psychology, cultural belief systems, historical memory, and linguistic nuance is a fraction of what it should be. You cannot detect adversary narratives targeting your society if you do not understand which of not only your society's fault lines but the adversary's strategic logic for weaponising these particular ones, and to what end. Practitioners who understand the fissures but not the intent behind their exploitation build information responses rather than governance responses.

Building this knowledge is the cognitive equivalent of reconnaissance, and it belongs at Tier 2 as the intelligence infrastructure on which effective defence depends. Tier 3 is a distinct category: narrative and influence operations directed at adversary populations, held strictly dormant unless a kinetic threshold is crossed. The capacity-building decision

and the deployment decision are fully separate, and the latter requires explicit political authorisation that the former does not. If Tier 3 capability were ever deployed, it should be understood as the coordinated application of existing tools: strategic communications, psychological operations, public diplomacy, directed toward adversary populations in conditions of open conflict, not as a new category of covert manipulation. The distinction matters because it anchors the capability within democratic norms: transparency about methods where possible, preference for truth over fabrication, and a purpose of informing rather than deceiving.

This distinction matters because the temptation to deploy peacetime cognitive capabilities against adversary populations is exactly what democracies must resist. Cognitive operations directed at foreign civilian populations corrode the democratic norms they are meant to protect. A democracy that abandons those norms in the name of defending them has resolved the tension in the wrong direction. Cognitive defence capability built inside military command structures without clear legal limits on domestic application will expand to fill the operational space available: Two distinct risks must be separated, because conflating them produces bad institutional design. The first is the risk of domestic misuse: cognitive warfare capabilities housed within military command structures without explicit legal limits on domestic application will expand to fill the operational space available. The second is the risk of offensive operations against adversary populations outside wartime, which carries different legal and ethical constraints.

The institutional record demonstrates the domestic misuse risk concretely. The UK's 77th Brigade, established in 2015 with a mandate to counter hostile state actors and extremist organisations overseas, was deployed during the COVID-19 pandemic to monitor domestic social media. A whistleblower investigation by the civil liberties organisation Big Brother Watch, later confirmed through Freedom of Information disclosures, found that the Brigade collated social media posts from British citizens and passed them to the Cabinet Office. Defence Secretary Ben Wallace acknowledged the activity in the House of Commons in January 2023, stating that the unit's counter-disinformation capabilities had been used to assess UK disinformation trends while insisting the Brigade was not intended to police domestic opinion.[6] The episode illustrates what happens when

cognitive defence capability is built inside military command structures without clear legal limits on domestic application: the mandate expands to fill the operational space available. A further design failure compounds the institutional one: approximately 70 to 80 per cent of the Brigade's work was offensive in orientation, the defensive cell grew during COVID but repeatedly overstepped its mandate, a single tweet required eleven days to approve through the chain of command, and private strategic communications company contracting created accountability gaps that no public oversight mechanism could close.

The institutional verdict from field research within the UK national security community is direct: the 77th Brigade is institutionally unfit for rapid defensive response. The approval culture is incompatible with the speed the information environment requires. The problem is architectural, not a matter of individual institutional failure. The structural remedy is not better instructions. It is institutional separation: cognitive defence capability built outside military command structures, with explicit legal constraints on domestic application, parliamentary oversight, and no authority to operate against the democratic public it is designed to protect.

Endnotes

1 Marija Golubeva, "Awake But Groggy: Europe's Shadow Warfare Guardians," *Europe's Edge;* Center for European Policy Analysis; November 19, 2025.

2 Dr Fedir Korobeynikov, Dr Andrii Davydiuk, Prof Volodymyr Mokhor; *Ontological Foundations of Cognitive Warfare*; NATO Cooperative Cyber Defence Centre of Excellence; G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine. Tallinn 2026

3 Pekka Kallioniemi, 'Beyond Defence: A Proactive Strategy for the West,' November 2025.

4 Tanna Krewson, NATO Allied Command Transformation, virtual interview with the author, April 2026. Krewson led the development of NATO's cognitive warfare concept through Allied Command Transformation.

5 Field research at Allied Command Transformation, May 2026.

6 UK Ministry of Defence and The Rt Hon Ben Wallace, "Defence Secretary oral statement on war in Ukraine," UK House of Commons; published January 16, 2023

Part III: Primary Case Studies

Chapter 8: Germany

Germany's most important cognitive defence finding is an inversion. Russian cognitive operations have been more effective on the country's political elite than on its population. The German public adapted rapidly to the post-2022 threat environment. Its political leadership did not. By January 2022, 73 percent of Germans opposed weapons deliveries to Ukraine; within months, the reversal was near-total. Approximately 80 per cent now identify Russia as the aggressor, a figure confirmed across three independent sources. Seventy-four per cent indicated willingness to pay higher energy prices to cut Russian dependence. Eighty per cent indicated they did not trust Russian good-faith negotiation. The German public completed its threat adaptation faster than its political elite, without a coordinated institutional response, and against a backdrop of active Russian influence operations targeting both public and elite opinion.[1]

This chapter argues that the gap between public adaptation and elite response is the structural condition that adversary operations are designed to exploit, and the alt-right political party, *Alternative für Deutschland* (AfD), is its principal institutional vector. The AfD is the third-largest force in the Bundestag, yet its national-level federation is under a formal *Verdachtsfall* designation by the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*) and three of its state federations are classified *gesichert rechtsextrem*, the highest threshold available short of a constitutional ban. Russian information operations have systematically amplified AfD-aligned content, with the Doppelgänger campaign and the Storm-1516 network running through more than one hundred German-language fake news websites during the 2025 federal election cycle.[2] The AfD needs only to remain inside the institutional architecture, holding parliamentary committee positions, contesting elections, and offering adversaries a domestic vector through which the elite-public inversion can be sustained. This makes Germany the parallel to Canada's Alberta Convergence: foreign actors identifying and amplifying existing domestic fault lines through different institutional vectors.

Threat Actors and Methods

Russia is the primary disruptive adversary. The President of the Bundesnachrichtendienst (Federal Intelligence Service, BND) confirmed at the 2026 Munich Security Conference that 321 Russian sabotage incidents were recorded in Germany in the past year, establishing hybrid attacks as systematic at a scale with no peacetime precedent.[3] Cognitive operations run alongside the kinetic and infrastructure dimensions rather than apart from them. The Russian threat picture targeting Germany combines documented sabotage incidents, sustained FIMI campaigns identified in the European External Action Service's Fourth FIMI Threat Report, and the systematic exploitation of historical and political fault lines that the AfD vector then amplifies institutionally.

The historical inheritance complicates the picture in ways adversary operations are designed to exploit. The accommodation posture toward Russia that characterised life in the eastern *Länder* under the German Democratic Republic was not ideological sympathy but learned fatalism about a power too large to challenge. That fatalism did not dissolve with reunification. It became a residual cognitive orientation that Russian operations are designed to find and amplify. The memory of the Wehrmacht's war against the Soviet Union also fosters a lasting sense of historical responsibility and caution about confronting Russia, particularly among older cohorts. Russia exploits existing fractures rather than creating them, a finding confirmed independently across multiple field-research sources. Closing the fractures requires not counter-messaging but the social and economic investments that address the underlying conditions.

The Doppelgänger campaign illustrates the operational evolution with precision. First publicly exposed in August 2022 by T-Online and the Süddeutsche Zeitung, and subsequently attributed by EU DisinfoLab and other researchers to the Russian Social Design Agency and Structura entity, the campaign used typosquatting and impersonation techniques to run cloned versions of *Der Spiegel, Die Welt, Bild*, and other German outlets, carrying narratives designed to align with AfD-adjacent positions on Ukraine support, energy policy, and migration. Initial analysis showed the operation pausing during Russian national holidays and overnight, the human fingerprint visible in the working week's rhythms. A second analysis one year later showed the pattern had entirely

disappeared. High-level automation had replaced the manual operation. The campaign infrastructure was partially dismantled in November 2024, but was reactivated in modified form during the February 2025 German federal elections, demonstrating that the FIMI threat against Germany is not a series of discrete events but a continuously operating system.[4]

The Storm-1516 network represents the second documented evolution. Attributed to former Internet Research Agency personnel operating with GRU-connected infrastructure, Storm-1516 ran more than one hundred German-language fake news websites with approximately six thousand bot accounts and twenty-plus impersonated organisations active during the 2025 federal election cycle. The network's content map aligned with positions taken by the AfD parliamentary delegation across the same period. Russian information operations targeting the German brigade in Lithuania are expected to intensify in 2026 and 2027, aiming to exploit historical sensitivities, test societal resilience, and undermine public and political support for the deployment.[5]

Türkiye presents a distinct and under-discussed challenge. The DITIB and Diyanet mosque network, encompassing roughly one third of German mosques with imams effectively state-appointed through Türkiye's religious ministry, is the most institutionalised documented case of foreign-controlled influence operations in Germany. It is largely absent from strategic literature on cognitive operations against Germany despite its scale and its public verifiability. Türkiye is not the only state actor operating through diaspora institutional networks, but the DITIB case is the most operationally legible. China is building a long game with infrastructure that does not yet match Russia's operational tempo but whose language capability is improving, and whose strategic patience exceeds either Russia's or the new American dimension.[6]

A parliamentary disclosure in early 2026 sharpened this picture. The German federal government acknowledged in a formal parliamentary response that it holds no central statistical data on sensitive German-Chinese research cooperations in artificial intelligence, quantum technologies, and robotics, and has no complete overview of dual-use risk in nationally funded German-Chinese research. The absence of a clearing house for dual-use research risk is not a gap that China will wait for Germany to close. It is the

structural condition that makes Germany’s research universities a soft target at Layer 5, the layer of active defence and adversary cost imposition: not the site of active espionage operations but of slow, patient knowledge transfer that no institution is currently tracking at the national level.[7]

The American dimension is the categorical change. Until 2024, the United States operated as Germany's primary strategic partner on counter-FIMI questions, with intelligence sharing, joint attribution work, and coordinated responses to election-period operations as standing features of the bilateral. From 2025, public criticism by senior US officials of the Verfassungsschutz's gesichert rechtsextrem designation of the AfD, combined with the broader European-democracy-criticism posture set out in the February 2025 Munich Security Conference address by Vice-President JD Vance, has introduced a vector that existing attribution frameworks were not designed to read. The Verfassungsschutz framework is anchored in domestic constitutional law and reads foreign criticism of its designations as a diplomatic matter. The cognitive-defence framework would read sustained public criticism by senior officials of an allied government, when that criticism systematically aligns with the messaging of a domestic party under formal extremism designation, as a foreign-amplification dimension of a domestic constitutional question. The institutional architecture has not yet been built to hold both at once. The current US administration's posture has also introduced friction into the bilateral counter-FIMI relationship that did not previously exist, and Germany does not yet have the working-level depth with the United Kingdom on counter-FIMI that France maintains, leaving an operational gap.

The cumulative finding from the threat landscape is that adversary operations against Germany are not aimed primarily at reshaping public opinion. The public has, despite being among the four most-targeted countries in EEAS monitoring, completed its threat adaptation. The operations are aimed at sustaining the gap between public adaptation and elite response: amplifying the AfD's parliamentary presence, fragmenting elite consensus on Ukraine support and Russia policy, and creating the political-cultural conditions in which the institutional architecture the Zeitenwende requires cannot be built

at the speed the threat environment demands. The inversion is the strategic objective, not a side effect. The institutional response has to be built to address it as such.

The AfD as Parliamentary Vector

The AfD is the institutional form through which the elite-public inversion is sustained against the public's own threat assessment. The party entered the Bundestag in 2017 with 12.6 per cent of the vote. It became the largest opposition party after the 2025 federal election with approximately 20.8 per cent. It is the largest party in five of the eastern *Länder* by voting share.

The Federal Office for the Protection of the Constitution placed the national-level AfD under formal *Verdachtsfall* (suspected case) designation in March 2021, upgraded the assessment to *gesichert rechtsextrem* (confirmed right-wing extremist) in May 2025, and has classified the AfD federations of Saxony, Thuringia, and Saxony-Anhalt as *gesichert rechtsextrem* at the state level. The classification framework, anchored in Germany's *streitbare Demokratie* (militant democracy) constitutional doctrine, authorises intelligence surveillance, restricts civil-service eligibility, and lays the evidentiary foundation for the constitutional ban procedure. The AfD has challenged each designation through the administrative courts. The Münster Higher Administrative Court upheld the *Verdachtsfall* in May 2024. The *gesichert rechtsextrem* upgrade was challenged, and on 26 February 2026 the Cologne Administrative Court ordered the Federal Office for the Protection of the Constitution to refrain from labelling the federal party gesichert rechtsextrem pending the main proceedings, suspending the federal designation; the state-level classifications remain in force, and the Saxony classification has been confirmed by the courts.[8]

What the framework was not designed for is the foreign-amplification dimension. The Verfassungsschutz designations rest on the AfD's domestic conduct: the party's relationship to Identitarian movements, the use of *völkisch* rhetoric, the contestation of Germany's post-1945 constitutional order. The framework does not yet read the AfD as the institutional vector through which foreign cognitive operations achieve domestic political resonance. This is where adversary operations have the most latitude.

The empirical record on foreign amplification, set out above, has accumulated quickly across the Doppelgänger and Storm-1516 campaigns. Both are AfD-aligned in content, with the network's content map tracking positions taken by the AfD parliamentary delegation across the same period. The Doppelgänger campaign was active during the 2024 European Parliament and 2025 federal election cycles. The Storm-1516 network ran more than one hundred German-language fake news sites, often supporting the AfD. The AfD provides the institutional vehicle through which that orientation is given parliamentary expression. The Konrad-Adenauer-Stiftung Canada's own analytical work on right-wing extremism and democratic resilience documents this convergence, and confirms that the institutional conversation is already underway.

The American dimension has emerged more recently. Vice President Vance's address criticising, and the US criticism of the Verfassungsschutz's *gesichert rechtsextrem* designation of the AfD, mark this change. This is the second adversary operating through the same institutional vehicle, with no coordination required, because the underlying logic is the same: identify the existing fault line, amplify it through whatever channel is available, allow domestic actors to sustain the operational consequences. The structural feature of cognitive warfare against pluralistic democracies is that it propagates through inter-layer connectivity rather than through any single dominant channel. The Korobeynikov, Davydiuk, and Mokhor framework names this precisely: in democracies with high irreducible multiplexity, effective cognitive operations subvert coherence across layers rather than injecting entropy into a dominant interpretative layer.[9] The AfD is the connector node through which subversion of inter-layer coherence becomes operational across epistemic, axiological, identificatory, and teleological dimensions simultaneously.

The comparison with Canada's Alberta Convergence sharpens the structural finding. The Alberta vector runs through a citizen-initiated referendum mechanism, a third-party advertiser registered with the provincial electoral authority, a stolen voter list, and the operational mobilisation of staff connected to the governing United Conservative Party caucus. The AfD vector runs through a parliamentary delegation, Verfassungsschutz designations, judicial review proceedings, and a federal election in which the party became the largest opposition force. The underlying logic is identical: foreign actors

identify existing domestic fault lines, amplify them through cross-border information infrastructure, and rely on domestic political vehicles to sustain the operational consequences without requiring continuous external direction. Both cases are most operationally legible at the subnational level, where the political contest has the least national-security oversight: Alberta in the Canadian case, Saxony, Thuringia, and Saxony-Anhalt in the German case.

The two cases also illustrate the similarities between Canada and Germany. Both are federal architectures with constitutional protections distributing capture risk across multiple orders of government. Both have civil society and academic capacity ahead of their institutional architecture. Both face threat environments in which the United States operates as a vector. Both have new political leadership, with mandates explicitly framed around the rupture in the international order.

The institutional response to the AfD vector is, at the time of writing, primarily judicial and administrative. The Verfassungsschutz framework is doing the work for which it was designed. The cognitive-defence dimension, which would treat the AfD vector as a foreign-amplification problem in addition to a domestic constitutional one, is not yet integrated into the institutional architecture. The Hybrid Threat Response Law and the BND Act reform discussed in the coordination architecture section below are the closest existing policy instruments. Neither is structured to address the parliamentary vector directly, because doing so requires institutional and analytical capacity at the intersection of constitutional protection, foreign-interference attribution, and platform-accountability enforcement that no single existing German institution currently houses.

The parliamentary vector is not the only domestic surface adversary operations work on. The Reichsbürger movement, a network of actors who reject the legitimacy of the Federal Republic itself, claim that Germany has remained an occupied territory since 1945, and deny the lawful authority of the state including its taxing power, represents the threshold at which domestic ideological rejection becomes a national-security matter. The movement has grown materially over the past decade, is under standing surveillance by the Federal Office for the Protection of the Constitution, and produced a thwarted coup attempt in December 2022 in which a network of Reichsbürger-aligned actors plotted to

violently overthrow the federal government. The movement's largest organisational subgroup, Königreich Deutschland (Kingdom of Germany), was formally banned in 2025 and its leader arrested. The Reichsbürger case illustrates a category of cognitive-domain threat that the German federal government treats through its constitutional-protection architecture rather than through its foreign-interference architecture: domestic actors whose ideological rejection of the state's legitimacy creates a security exposure that foreign cognitive operations can subsequently exploit. The Doppelgänger and Storm-1516 campaigns documented earlier in this chapter operate, in part, on the receptivity that ecosystems like Reichsbürger have already created.

What Makes Germany Distinctive: Three Pillars

Germany's most transferable strengths are not its scale or its resources. They are three specific institutional and social assets that have no precise equivalent elsewhere in the democratic world, built deliberately after catastrophe. Each is a foundation other countries are now being told to construct. All three explain why Germany sits where it does in the manuscript's comparative architecture.

The first pillar is the Bundeszentrale für politische Bildung (Federal Agency for Civic Education, BZpB). It is the only institution in any democracy specifically designed from the ground up around the lived experience of what state propaganda can do to a population. Founded in 1952 as part of post-1945 democratic reconstruction, the BZpB has spent seven decades publicly funding civic education and democratic literacy as a standing government obligation, with a parallel infrastructure of Landeszentralen operating at the *Länder* level. Politische Bildung is the doctrinal frame: the deliberate, publicly funded cultivation of the epistemic and civic foundations of democratic life. The institution's pedagogical scope spans schools, adult education, professional development, and the federal-funded political foundations (Stiftungen) attached to the major parties, of which Konrad-Adenauer-Stiftung is one. The BZpB does not yet operate explicitly within a cognitive-defence frame. Yet its function is the foundation that cognitive defence requires and something that no other comparator democracy has.

The second pillar is the constitutional architecture itself. Distributed federal power prevents executive capture: no single central authority exists to be seized. Germany has,

by design, no single node whose control would deliver the state. The Basic Law's allocation of competences between the Bund and the *Länder*, combined with the Bundesrat's legislative role and the *Länder's* autonomous administration of education, broadcasting, and police powers, distributes capture risk across sixteen subnational governments and a federal layer that cannot override them on the substrate questions cognitive defence depends on. The architecture also produces friction at the operational level: federal-state coordination on FIMI response is uneven, and the Verfassungsschutz operates simultaneously at federal and Land levels with assessment frameworks that do not always align. The structural feature is therefore a foundation and a complication at once. It is the foundation against executive capture that adversary operations targeting elite cognition cannot dissolve, and it is the operational complication that slows the institutional response to those operations. The same feature appears in the Canadian case at a different layer of the same problem. Both cases confirm that federal architectures distribute capture risk and complicate response speed, and that the cognitive-defence question turns on whether the architecture is operated as a connected system rather than as parallel jurisdictions.

The third pillar is the civil society ecosystem, which is ahead of the institutional layer in ways directly comparable to Ukraine and Poland. Organisations are not waiting for the state to lead. The defence start-up ecosystem, exemplified by Helsing, is producing AI-integrated defence tools primarily for Ukraine, operating almost entirely separately from official policy. The Institute for Strategic Dialogue's policy sprint convening practitioners across Berlin, Paris, Warsaw, and London, is coalition-building at the working level that formal institutions have not yet attempted. The political foundations attached to the major parties operate transnationally with established office networks across more than a hundred countries, conducting research, convening, and democratic-resilience work at a scale that no comparable democracy maintains. Konrad-Adenauer-Stiftung Canada's own research programme on cognitive resilience and FIMI sits within that ecosystem. Germany's civil society has the analytical capacity, the operational reach, and the international networks. The institutional layer needs to catch up to what civil society is already doing.

The three pillars together explain why the elite-public inversion is sustainable rather than terminal. Germany has built, deliberately, the foundations on which a serious cognitive-defence architecture can rest. What it has not yet built is the political-cultural reflex of treating those foundations as security assets, or the institutional architecture that connects them to the operational layers above.

Coordination Architecture

The Zeitenwende happened as a speech. The institutional architecture has been catching up to the rhetorical event for four years and is, under the Merz government, finally moving at the speed the threat environment demands.

The National Security Council (Nationaler Sicherheitsrat), constituted in November 2024 under the previous Scholz government, held its first meeting that month and adopted a classified hybrid threat action plan as its first act. The Council brings together the Chancellor, the Federal Ministers of Foreign Affairs, the Interior, Defence, Finance, and Justice, with the Chief of the Federal Chancellery as standing chair. Its mandate is strategic coordination across the ministerial layer, with a permanent staff function inside the Chancellery to support continuous operational tempo between Council meetings. The resourcing does not yet match the mandate.

The legislative pivot under the Merz government is the strongest signal yet that the institutional response has reached the layer where it can begin to function at threat-environment speed. Two legislative reforms are advancing under the Merz government. A comprehensive reform of the BND Act would authorise offensive cyber operations abroad, reversing the post-1945 inheritance that limited the Federal Intelligence Service to collection rather than effects; as of mid-2026 it remained at the draft stage, with the government seeking a Cabinet decision ahead of introduction to the Bundestag. A parallel Interior Ministry cybersecurity reform would authorise active cyber defence, reversing the Scholz-era prohibition on hackbacks and permitting disruption of adversary infrastructure even outside German territory.[10] The Peace Research Institute Frankfurt's analysis of the 2025 federal election documented the institutional gap this shift addresses: Germany still lacked a VIGINUM equivalent or centralised attribution capacity at the time of the election. The legislative pivot is the direct response.

A VIGINUM-style agency, the Zentrum zur Abwehr von Einflussoperationen und Manipulation (ZEAM, Centre for Countering Influence Operations and Manipulation), is being stood up within the Federal Ministry of the Interior, with Foreign Office secondees and preceded by study trips to France, Sweden, and the United Kingdom. An inter-ministry task force on hybrid threats includes every federal ministry, with a working group linking federal and state-level (Länder) authority. The architecture is built. The scale at which it will operate is the open question.

A formalised attribution process operates with Eckpunkte (threshold criteria for attribution decisions), standardised intelligence tasking, and an inter-ministry agreement on reactive steps. The Foreign Office leads attribution because the response is primarily diplomatic. Two attributions were completed in the year preceding this research. The Doppelgänger automation finding is publishable Alliance-wide and is now drawn on by other Allies in their own detection methodologies.

At the working level, the most operationally effective coordination format currently functioning is the Weimar Triangle, the trilateral cooperation between Germany, France, and Poland: near-weekly Signal exchanges, common communication lines, and joint campaign execution including the Shadow Fleet campaign. Its value is at the working level.

At the political level, strategic decisions revert to the Germany-France bilateral or the E3 (France-Germany-United Kingdom) diplomatic format. The Weimar Triangle is the closest existing approximation of the kind of standing operational coordination the corridor argument in Chapter 13 proposes Germany also build with Canada and the EU.

The civil-service and defence-industrial layers were ahead of the political elite in recognising the problem. Mid-level officials, the BND analytical product, the Foreign Office assessment, and the defence start-up ecosystem were all operating on an updated threat model before the political elite caught up to it. The political elite is the laggard layer, not the civil service, the public, or industry. The Merz government's posture closes that gap rhetorically. The institutional and resource gap remains.

The domestic political dimension complicates the institutional pivot in ways the inversion thesis predicts. When European Commission President Ursula von der Leyen announced the European Centre for Democratic Resilience in her 2025 State of the Union address, the announcement was interrupted by dissenting AfD members of the European Parliament. The institution intended to address the parliamentary vector for cognitive operations was disrupted, on the floor of the European Parliament, by the parliamentary vector itself. The EU DisinfoLab's October 2025 analysis documents the broader pattern: practitioners in the counter-disinformation field now face hostile external actors on one side and an increasingly adverse domestic political environment on the other.[11] Germany is on the front line of both. The institutional pivot the Merz government has authorised is moving at the speed the cognitive-defence problem requires. The political environment in which that pivot has to land is moving in the opposite direction at comparable speed. Whether the institutional architecture closes the inversion before the political environment widens it is the open question the chapter cannot answer at the time of writing.

The Bundeswehr's Cognitive Doctrine

Germany sits at the opposite end of the Alliance's cognitive-warfare-adjacent capability spectrum from Canada. Field research at Allied Command Transformation Norfolk identified Germany as one of the small number of Allies investing across the four strands ACT uses to assess cognitive-warfare capability: people and personnel; technical capabilities and artificial intelligence; coordination and synchronisation; and cutting-edge science integration. Germany is exemplary specifically because investment runs across all four rather than concentrating in any single strand. Germany is one of the working examples, alongside the United States, the United Kingdom, and France.

The Alliance-wide picture is one of acute asymmetry. Three of thirty-two Allies maintain dedicated offensive cognitive capability. Twenty-nine do not. The minimum viable capability package is not technically complex: information environment assessment capacity, behavioural science expertise, information planners, established channels, and effect assessment methodology. What is missing in the twenty-nine is career streams, dedicated expertise, and the political will to activate the tools in peacetime. The legislative

pivot under the Merz government is the closest existing signal that the authorisation is forthcoming.

The Bundeswehr's *Kommando Cyber- und Informationsraum* (CIR, Cyber and Information Domain Command) is the institutional home for cognitive-warfare-adjacent capability. Established in 2017 as the Bundeswehr's sixth military organisational area, CIR consolidated cyber, information operations, geoinformation, and signals intelligence functions into a single command structure. The CIR concept was ahead of NATO's J10 consolidation, which brought public affairs, psychological operations, and key leader engagement into a single Alliance structure. However, Germany now needs the doctrinal framework that treats cognitive warfare as the operating environment within which all CIR functions take place, rather than as a subset of psychological operations within it.

CIR has invested in a dedicated career pipeline with specialised training pathways and reserve acquisition routes that allow direct commissioning of civilian specialists at officer rank. The reserve path is particularly distinctive: computational social scientists, behavioural economists, communications professionals, and digital analysts can be brought into the Bundeswehr at officer rank without the full military training pathway. The pipeline is underused. The defence start-up ecosystem, exemplified by Helsing's AI-integrated defence tools developed primarily for Ukraine, is producing the analytical talent the reserve path is designed to bring in. The Bundeswehr has the legal and institutional authority. The connecting tissue between the start-up ecosystem and the CIR career pipeline has not yet been built.

On the technical capabilities and artificial intelligence, German investment has run primarily through CIR's signals intelligence and information operations functions, with growing integration of AI-enabled tooling for both defensive monitoring and analytical work. The Helsing example illustrates the broader pattern: German defence-industrial AI capacity is operating at the frontier of what military cognitive tools can do, but the formal relationship between government and the start-up ecosystem remains underdeveloped. The capability exists. The integration is the open question.

On coordination and synchronisation, CIR's institutional architecture is among the most developed in the Alliance. The single-command structure connecting cyber, information

operations, geoinformation, and signals intelligence avoids the inter-service coordination friction that constrains comparable capability in other militaries. The connection between CIR and the civilian-side coordination architecture treated above (the National Security Council, ZEAM, the inter-ministry task force on hybrid threats) is functional but not yet at the operational tempo cognitive operations require. Coordination across the military-civilian boundary is the strand most exposed to the wider institutional pivot the Merz government has authorised.

On cutting-edge science integration, German participation in the NATO Science and Technology Organization has been substantial. Germany is one of the five leading contributors to cognitive warfare research over the past five years, alongside the United States, Norway, the Netherlands, and Sweden, with primary engagement through the Human Factors and Medicine panel. The translation problem from STO research output to operational doctrine is the same in Germany as in other Allied forces. The CIR doctrinal framework has the institutional home to absorb STO outputs at the speed the threat environment requires. Whether it does so is a question of doctrinal will rather than institutional capacity.

The Bundeswehr cannot resolve where to place cognitive capabilities until the conceptual framework has been built internally. The opportunity is operationally available and politically legible. The Bundeswehr's task is to take it.

Honest Limitations

Germany lacks a clearing house equivalent to Britain's Joint Intelligence Committee (JIC). The perspectives from the Foreign Office and the Ministry of Defence exist as separate streams without an integrating mechanism. Intelligence and politics have been kept deliberately separate as a postwar inheritance. The threat level no longer justifies the separation. The honest finding here is that the institutional gap is the most significant single constraint on Germany's capacity to operate at the tempo cognitive operations require.

The communication inhibition is real and structurally distinctive. German authorities declined to publicly confirm drone overflights of northern critical infrastructure for months after the incidents were first reported, a pattern that contrasts directly with the proactive

disclosure approach of the Baltic states. Estonia has established a pattern of proactive public attribution, including the disclosure that one third of its citizens' digital IDs contained a security vulnerability, a decision that prioritised public trust over operational security optics.

The German inhibition is rooted in a specific national trauma: Germany's history of state-directed information operations creates a precise historical constraint on what German governments feel they can legitimately do in the information environment. The consequence is a public prevented from developing the threat awareness its own instincts have already begun to form. The solution is not concealment but prompt, calibrated, public attribution that trusts the population to process information without panic. Doing so requires institutional confidence the political culture has not yet built.

The strategic culture limitation runs through every other constraint in this chapter. Germany's relationship to strategic weight is distinctive and requires precision. The European Union has long been understood as driven by the Franco-German engine. Since the 2008 financial crisis, Germany has increasingly emerged as the EU's primary institutional anchor: the economic engine, the consensus builder within the Council, and the actor whose domestic political choices most directly determine the pace and direction of European integration. Germany sees itself in this role, exercising it through the European project with growing confidence. What the postwar democratic reconstruction did not produce is the reflex of projecting that weight beyond the European frame, of acting as a global strategic actor whose dispositions and investments shape the security environment outside the EU. In the cognitive defence domain, this manifests as a tendency to work within EU and NATO institutional frameworks rather than to define and lead strategic concepts. Konrad-Adenauer-Stiftung’s own work on a more defensive democracy, ‘Wehrhaftere Demokratie’, sits in this same conversation: the question Germany’s domestic democratic-resilience discourse has been asking is how a state with Germany’s historical inheritance learns to defend the democratic order without reproducing the instruments of the regimes that historical inheritance teaches it to avoid. The cognitive defence problem is one expression of this larger institutional question.[12]

The Körber-Stiftung's *Berlin Pulse 2025/2026*, the leading annual survey of German public opinion on foreign policy, documents the tension directly. While 72 percent of Germans support doubling defence spending over ten years, and 47 percent assess the Russian military threat as very high, 61 percent continue to reject a German military leadership role in Europe, and 54 per cent express concern about Russian attempts to influence German public opinion. A population simultaneously willing to pay for defence and unwilling to lead is the precise strategic culture condition that makes Germany's cognitive defence architecture gap politically difficult to close. Fifty-four per cent of G7 publics perceive Germany as a great power. Only 22 per cent of Germans hold that view of themselves.[13] The Baltic states invest heavily in security architecture precisely because their threat exposure is immediate and inescapable. The calculus for Germany, insulated by geography and history from that immediacy, has not yet produced the same institutional urgency.

Brookings analyst Constanze Stelzenmüller has argued that the new National Security Council is structurally inadequate to serve as Germany's strategic nerve centre, lacking both the political weight to coordinate across ministries and the operational tempo that cognitive domain threats require.[14] Field research for this report is consistent with that assessment. The Council's resourcing, currently at fewer than twenty-five permanent staff, does not match the mandate set out in the November 2024 hybrid threat action plan, nor the scale the institution's own ambition implies. The honest finding here is that the institutional architecture is built. The political will to scale it to the threat environment is the open question.

The cognitive defence architecture cannot be built faster than the political culture that has to authorise it. The public has adapted, the civil service has adapted, the defence-industrial base has adapted, and the political class is finally moving under the Merz government. Whether the pace of political-cultural adaptation matches the pace at which adversary operations are amplifying the inversion through the parliamentary vector remains the central open question.

Layer Mapping

Applied to the six-layer framework with its dual foundations, Germany's profile reveals genuine strengths at the foundational layers, moderate-to-developing capability across the operational layers, and political will as the binding constraint.

The social infrastructure foundation is moderate. The BZpB, the strong civil society tradition, and the constitutional architecture preventing executive capture are genuine assets. Social cohesion is under strain from economic grievance and the persistent East-West gap, with the eastern *Länder* carrying disproportionate exposure to both. Layer 1, individual cognitive capacity and emotional regulation, is moderate to strong: the BZpB's seven decades of *politische Bildung*infrastructure, the *Landeszentralen* operating at the *Länder* level, and the Stiftungen's transnational networks together constitute the most developed Layer 1 architecture in any comparator democracy. War-anxiety rhetoric has rebounded domestically in ways that complicate sustained mobilisation, but the foundation is built.

Layer 2, integrity of the information environment, is moderate: well-funded public broadcasters, the FIMI attribution process with *Eckpunkte* criteria functioning are strengths; the VIGINUM-style ZEAM agency remains under construction, and the communication inhibition from propaganda trauma is a structural constraint.

Layer 3, platform architecture and algorithmic accountability, is mixed. The Network Enforcement Act (NetzDG) placed Germany ahead of EU frameworks on platform legislation[15], but platform accountability remains the outstanding structural weakness, as the Reporters Without Borders *Focus 2026* report on Germany documents. Political actors are actively using digital platforms to pit citizens against one another, persistent legislative inaction on platform accountability continues despite documented harm, and the current US administration’s open support for tech platforms’ resistance to EU regulation has introduced external pressure on the very regulatory instruments Germany needs to protect its information environment. The legislative pivot under the Merz government addresses part of this gap.[16]

Layer 4, detection and attribution, is moderate: the formalised attribution process, Doppelgänger and Storm-1516 attributions, and ZEAM under construction represent real

progress; the absence of an integrated situational awareness clearing house and the intelligence-politics separation remain limiting.

Layer 5, active defence, is limited but pivoting: no offensive cognitive capability exists, Bundeswehr doctrine still treats this as psychological operations only, and the CIR command is the right institutional home but the doctrinal framework is not yet built; the BND Act reform and the Hybrid Threat Response Law are the legislative pivot.

Layer 6, sovereign response capacity, is moderate: the new KRITIS-DACHG critical infrastructure law and the NSC classified hybrid threat action plan are in place, and the National Security Council, the inter-ministry task force on hybrid threats, and the Weimar Triangle at the working level provide real coordination architecture; the JIC-equivalent gap remains and the NSC is under-resourced relative to its mandate. Political will, the upper foundation, is the binding constraint. The Merz government's forward posture is genuine and the legislative pivot is the strongest signal yet. The political elite continues to lag behind both the public and the civil service.

Partner Landscape

Germany's most active working partnerships in the cognitive and FIMI domain are concentrated within Europe and skew bilateral. France and Poland are the operational anchors through the Weimar Triangle, with near-weekly working-level exchange and joint campaign execution. The format is the closest existing approximation, in any European context, of the operational tempo cognitive operations require. Strategic decisions revert to the Germany-France bilateral or the E3 diplomatic format at the political level.

The European External Action Service StratCom architecture is the primary EU institutional relationship. Germany sits among the four most-targeted countries in EEAS monitoring within the EEAS perimeter. The relationship runs at working level rather than at strategic level, with German engagement on the EEAS Foreign Information Manipulation and Interference Information Sharing and Analysis Centre (FIMI ISAC) and on the FIMI Toolbox processes consistent rather than leading. The ISD policy sprint convening practitioners across Berlin, Paris, Warsaw, and London is the closest operational approximation of a standing civil society coalition. Within Germany, the institutional anchor of civil-society monitoring capacity is the Centre for Monitoring,

Analysis and Strategy (CeMAS), a Berlin-based non-profit that combines systematic monitoring of digital platforms with interdisciplinary expertise on conspiracy ideologies, disinformation, antisemitism, and right-wing extremism. CeMAS produces the analyses on which much of the German policy-research community and a portion of the federal government's situational picture now relies, and its operational tempo significantly exceeds that of the federal institutions discussed elsewhere in this chapter.

Lithuania is the partner where cognitive defence cooperation has deepened most rapidly in the past two years. The German brigade deployment in Lithuania, currently scaling to a permanent forward presence, has driven a parallel deepening of cooperation on hybrid threats and information operations. The cooperation combines intelligence sharing, strategic communication, and joint monitoring of the information environment to detect and respond to hostile influence operations targeting the brigade and the host nation. Both countries are investing in societal resilience in the form of media literacy, coordinated public messaging, and institutional responses to ensure that attempts to undermine the brigade's presence or NATO cohesion are identified early and countered effectively. The Germany-Lithuania bilateral on cognitive defence is the working example of what a deeper bilateral architecture can look like when one party is forward-deployed and the other is hosting.

The United Kingdom is a notable absence. Germany does not have the working-level depth with London on counter-FIMI that France maintains.

The current US administration's public criticism of the Verfassungsschutz's *gesichert rechtsextrem*designation of the AfD has introduced friction into the bilateral relationship that did not previously exist.

Germany does not yet use the term cognitive warfare institutionally; FIMI remains the operative frame, which limits the depth of engagement possible with partners who have advanced further on the conceptual architecture.

Canada is the partner the corridor architecture treats as the structural complement to Germany. Germany has the *politische Bildung* infrastructure, the cognitive-warfare-adjacent military capability, and the EU institutional anchor that Canada is now beginning

to construct. Canada has the G7 Rapid Response Mechanism convening capacity, the Five Eyes intelligence backbone, and the Media Freedom Coalition platform that Germany's bilateral and EU-anchored architecture cannot replicate.

Endnotes

1 Munich Security Conference, Munich Security Report 2026: Under Destruction (Munich Security Conference, February 2026); Körber-Stiftung, The Berlin Pulse 2025/2026 (Körber-Stiftung, November 2025); and European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference Threats (EEAS, March 2025).

2 Institute for Strategic Dialogue, Alliance4Europe, and FIMI-ISAC, Foreign Information Manipulation in the 2025 German Federal Election (October 2025), available at alliance4europe.eu.

3 Bundesnachrichtendienst President, address to the 62nd Munich Security Conference, Munich, 13 to 15 February 2026, reported in Munich Security Conference, Munich Security Report 2026: Under Destruction (Munich Security Conference, February 2026).

4 CORRECTIV, NewsGuard, and Gnida Project, 'Disinformation Operation: Russian Meddling in German Election Campaign Exposed,' CORRECTIV, January 2025, correctiv.org; and Digital Forensic Research Lab, EU DisinfoLab, VIGINUM, EEAS, CheckFirst, Cassini Insights, and Auswärtiges Amt, 'Building a Common Operational Picture of FIMI: Using the Information Manipulation System,' Digital Forensic Research Lab, January 2026.

5 Institute for Strategic Dialogue, Alliance4Europe, and FIMI-ISAC, Foreign Information Manipulation in the 2025 German Federal Election (October 2025); and CORRECTIV, NewsGuard, and Gnida Project, 'Disinformation Operation: Russian Meddling in German Election Campaign Exposed,' CORRECTIV, January 2025.

6 Field interview, 2026. The DITIB and Diyanet relationship is publicly verifiable: DITIB operates under the religious authority of Türkiye's Diyanet İşleri Başkanlığı (Presidency of Religious Affairs), with imams deployed through the Turkish religious ministry. The cognitive-operations dimension of this state-appointed network has not been the subject of academic study comparable to research on Russian information operations, and the present analysis draws on field interviews and public-record documentation.

7 German federal government, parliamentary response on sensitive German-Chinese research cooperations, Bundestag, 2026, as reported by CORRECTIV, April 2026, correctiv.org.

8 Cologne Administrative Court, decision of 26 February 2026 ordering the Federal Office for the Protection of the Constitution to refrain from classifying the federal AfD as gesichert rechtsextrem pending the main proceedings.

9 Fedir Korobeynikov, Andrii Davydiuk, and Volodymyr Mokhor, 'Ontological Foundations of Cognitive Warfare' (NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2026).

10 Deutscher Bundestag, "Regierung will das BND-Gesetz systematisch reformieren," heute im bundestag (hib), 3 March 2026, reporting the Federal Government's answer confirming the Chancellery's draft is under inter-ministerial coordination; on the Cabinet-decision timeline, see interface (interface-eu.org), 2026.

11 EU DisinfoLab, 'Documenting the Setbacks: The New Environment for Counter-Disinformation in Europe and Germany,' EU DisinfoLab, October 2025, disinfo.eu.

12 Konrad-Adenauer-Stiftung, Wehrhaftere Demokratie (The More Defensive Democracy), Konrad-Adenauer-Stiftung, kas.de.

13 Körber-Stiftung, The Berlin Pulse 2025/2026 (Körber-Stiftung, November 2025), koerber-stiftung.de.

14 Constanze Stelzenmüller, 'Germany's National Security Council Isn't Up to the Task,' Financial Times, 28 August 2025.

15 Lisa-Maria Neudert, "Reclaiming Digital Sovereignty: Policy and Power Dynamics Behind Germany's NetzDG," Journal of Information Policy 14 (2024): 417–470.No

16 Reporters Without Borders, Focus 2026: Germany (Reporters Without Borders, 2026), rsf.org.

Chapter 9: Canada

Canada built a robust intelligence and information apparatus during the Cold War, which it subsequently dismantled throughout the 1990s. Canada does not have the institutional knowledge that should have grown out of its historical memory, the coordinated capability those choices set aside, nor the political recognition that cognitive warfare is the threat the rest of its sovereignty building agenda depends on getting right.

On the night Prime Minister Carney won the Liberal leadership in March 2025, the Prime Minister set the frame for his foreign policy: 'America is not Canada. And Canada never, ever will be part of America in any way, shape, or form.'[1] At Davos on 20 January 2026, he gave the shifting world order its most quoted articulation: 'we are in the midst of a rupture, not a transition.'[2] In a YouTube video released on 19 April 2026, he extended the diagnosis to the bilateral relationship: 'many of our former strengths, based on our close ties to America, have become weaknesses, weaknesses that we must correct.'[3] At the eighth European Political Community Summit in Yerevan in May 2026, he gave the rupture its locating move, observing that 'integration is being used as a weapon' in the contemporary international order, identifying seven domains of strategic autonomy in which Canada and Europe should now build sovereign capabilities together: 'space-based communications, semiconductors, digital sovereignty, critical minerals, independent payment systems, clean energy, and vaccines,' and concluding that 'the international order will be rebuilt, but it will be rebuilt out of Europe.' Canada, in his framing, is part of that rebuild.[4]

The March 2026 announcement by the Carney government is the first sign it may be starting to wake up to the part FIMI plays in shaping the world view and the sovereignty-building agenda the Prime Minister has now articulated. This includes: the *Strong and Free Elections Act* amending the *Canada Elections Act*; C$31.5 million for Rapid Response Mechanism Canada to detect foreign information threats at all times rather than only during election periods; and, a new Cabinet Directive on the Coordinated Response to Threats to Elections. The announcement is a genuinely good start. Canada continues to have further to go.[5]

This recognition has not yet reached the cognitive domain. The Prime Minister has been using the language of digital sovereignty since at least September 2025, when he directed

the Major Projects Office to develop a sovereign computing cloud as part of Canada's nation-building agenda.[6]

Cognitive sovereignty has not yet entered the political vocabulary, even as Canadian civil society analysts have begun to use it explicitly: the May 2026 *National Unity Under Threat* report names Canada's cognitive sovereignty as 'being actively contested by foreign actors seeking to shape Canada's democratic future.'[7] Digital sovereignty is the technical precondition; cognitive sovereignty is the human precondition. The infrastructure dependency problem and the epistemic dependency problem are the same problem at different layers of the stack. Political recognition of one has begun without the architecture to deliver on it; political recognition of the other has not yet started.

The political failure runs across decades and across both of Canada's traditional governing parties. Canada established CSIS in 1984 in response to wrongdoing rather than to a strategic threat assessment. The post-2003 Public Safety architecture meant to coordinate the federal security and intelligence community on the public safety side has not delivered.[8] Canada operates on the basis of one comprehensive national security strategy, *Securing an Open Society*, tabled on 27 April 2004; it still names SARS as a contemporary threat.[9] Andrew Coyne, writing in *The Globe and Mail*, characterised Canada as 'almost suicidally complacent' on national security, with the country 'exposed and vulnerable, to a degree no other democratic state would tolerate.'[10] Russia's 2014 hybrid operations against Ukraine, which shifted threat assessments in Poland, the Baltics, and the Nordic countries, did not produce a corresponding institutional response in Canada. The final report from the Foreign Interference Commission found that information manipulation poses the single biggest risk to Canadian democracy and constitutes an existential threat.[11]

The recognition by the Carney government about the changing world order is real, and substantively further along than in some comparator countries. The recognition of FIMI as a discrete national security threat still lags behind, let alone the broader cognitive warfare problem of which FIMI is one part. The institutional architecture has not caught up to either, unlike comparator countries that have begun to align political commitments with institutional and financial frameworks for cognitive defence.

Threat Actors and Methods

The Canadian government and parliamentary debate use the terms foreign interference, FIMI, transnational repression, and disinformation. The Canadian Security Intelligence Service (CSIS), in its CSIS Public Report 2025, released in May 2026, identified the People's Republic of China, India, Russia, Iran, and Pakistan as the principal state actors conducting foreign interference and disinformation operations against Canada, adding Pakistan to the previous year's list and noting that with shifting geopolitical realities and an increasingly multipolar global environment these are not the only states interfering.[12]

The PRC remains the dominant state threat actor: PRC operations target political, economic, technological, and diaspora cognition simultaneously through cultivation of community proxies and covert relationships with current and former politicians, civil servants, journalists, and academics. India has cultivated covert relationships with politicians, journalists, and members of the Indo-Canadian community, and engages in transnational repression. Russia, since its full-scale invasion of Ukraine, has 'carried out several information and malign influence operations against Canada, exploiting various contentious social topics aimed at discrediting the Government of Canada's position on Ukraine by polarizing segments of both political and public spectrums. The Standing Senate Committee on National Security, Defence and Veterans Affairs, in its April 2026 report *Russia's Disinformation: Understanding the Challenge, Strengthening Canada's Response*, found that Russia's disinformation poses an urgent threat to Canada's national security, democratic institutions, and social cohesion, that the Government's current approach lacks coordination among federal entities, and that no strategic plan exists to address the threat.[13] Iran continues lethal transnational repression: multiple plots against Iranian dissidents and opposition figures in Canada were disrupted in 2025, and Canada is party to the July 2025 multinational joint statement condemning Iranian state activity. Pakistan, newly named in the 2025 report, conducts foreign interference primarily in support of the Khalistan movement.[14]

Former CSIS Director David Vigneault, testifying before the Foreign Interference Commission in September 2024, identified what he called the emergence of cognitive warfare against Canadian populations. New techniques leverage psychology, brain function research, and social media to penetrate population-level cognition, with the

People's Republic of China and Russia identified as the principal practitioners. Director Dan Rogers, in a public speech from November 2025, characterised the contemporary threat environment in unprecedented terms: never in the agency's combined histories had it faced threats of such magnitude simultaneously.[15]

The United States

The sixth threat actor, unnamed in any government public assessment and the most controversial, is the United States. Until 2024, the Government of Canada often referred to the United States as 'Canada's closest friend, partner, and ally.' The two countries share the world's longest undefended border, the binational North American Aerospace Defense Command, and the economic integration that NAFTA in 1994 and CUSMA (or USMCA) in 2020 progressively deepened. That bargain is gone. The president's 51st-state rhetoric, the 'Tariff Day' announcements, and the rapid succession of threats against Canadian sovereignty produced a national awakening: where much of Europe was woken to its security exposure by Russia's full-scale invasion of Ukraine in 2022, Canadians were woken to theirs by their closest neighbour. Nanos Research polling fielded between 31 January and 4 February 2026 found that 76.1 per cent of Canadians do not view the United States as a trustworthy ally.[16]

In the cognitive domain, the public record now establishes that the United States is interfering in Canadian politics. The accumulating evidence has been substantively named in *The Globe and Mail*, *Policy Magazine*, the *Financial Times*, *The Guardian*, *Reuters*, *The New York Times*, and the United States Department of Justice indictment in *United States v. Kalashnikov and Afanasyeva*. The single political question on which that evidence has converged is Alberta independence.

The Alberta Convergence

The Alberta Convergence is the author's analytical framing for what has emerged as the most operationally legible Canadian case of cognitive sovereignty under threat. Russian narrative infrastructure, US official engagement, cross-border influence amplification, and domestic operational mobilisation have converged on a single political question. The framing is complementary to but independent of the May 2026 Kolga, Phillips, McQuinn, and Van de Walle report, which advances a related cognitive sovereignty argument on the same case using a distinct analytical vocabulary; the author developed the Alberta

Convergence framing across the field-research programme that produced this manuscript, with the supporting evidence base set out below.

Alberta has emerged as the operationally most legible Canadian case, where Russian narrative infrastructure, US official engagement, cross-border influence amplification, and domestic operational mobilisation have converged on a single political question. The convergence has been enabled by genuine and durable Albertan grievances over federal energy and climate policy, by decades of structural Western alienation predating any current government, and by federal opposition rhetoric in recent years characterising Canada as broken or failing. Foreign actors did not manufacture Albertan separatism. They identified, amplified, and operationalised existing fault lines. The puzzle the convergence resolves is why support for Alberta separatism, at twenty-seven percent as of a May 2026 poll by Pollara Strategic Insights, sits in close parity with Quebec separatism at twenty-eight percent, on a similar demographic profile, but on a radically different political character. Alberta separatism is grievance-driven and right-coded, Quebec separatism is identity-driven and language-coded, and the structural difference matters for what each case requires from Canadian institutions. [17]

The public record has accumulated quickly across four convergent vectors of foreign engagement. The cross-border financial vector was first established by the September 2024 Tenet Media indictment, which set out that nearly US$10 million in covert Russian government funding had flowed through Tenet Media to American influencers Tim Pool and Benny Johnson, both of whom have since amplified Alberta separatist and US annexation narratives. Two Canadians, Lauren Chen and Liam Donovan, were also named as alleged platform operators.[18] Bob Rae, in a December 2025 edition of *Policy Magazine*, observed that the new US National Security Strategy puts Canada on notice that the current administration will actively support political parties and movements in Canada whose objectives align with US strategic interests.[19]

On 22 January 2026, US Treasury Secretary Scott Bessent, on the podcast *Real America's Voice with Jack Posobiec*, called Alberta 'a natural partner for the U.S.'[20] One week later, the *Financial Times* reported on 29 January 2026 that US State Department officials had met three times with the Alberta Prosperity Project between April 2025 and January 2026, with a further joint meeting between State, Treasury, and the Alberta

Prosperity Project planned to discuss a $500 billion credit facility upon Albertan independence.[21] Andrew Coyne reported in *The Globe and Mail* in March 2026 on publications recommending US support for provincial secessionist movements in Canada, exploitation of Indigenous reconciliation processes, and targeting of regional cleavages to achieve the dismemberment of Canada rather than annexation, which is the operational mirror of the Russian Panarin and Patrushev fragmentation doctrine.[22]

In late March 2026, a diplomatic cable signed by US Secretary of State Marco Rubio directed US embassies and consulates worldwide to engage in counter-influence operations, recruit local influencers and academics, and coordinate with US military psychological operations units.[23] The April 2026 *Slopaganda* report, by the Media Ecosystem Observatory at McGill University and the Canadian Digital Media Research Network, identified a coordinated network of twenty inauthentic YouTube channels promoting Alberta separatism and US annexation that accumulated approximately forty million views over the previous year through paid actors and AI-generated content.[24] The May 2026 *National Unity Under Threat* report identified the Russian Pravda News Network as the most systematic evidence of sustained Russian narrative infrastructure targeting Canada, with 'Alberta,' 'Albertans,' and '51st state' the subject of sixty-seven articles in the network's Canada section between December 2025 and April 2026, compared with fourteen mentions of Ontario.[25]

The domestic operational mobilisation has run on parallel tracks. “Take Back Alberta,” founded by David Parker, anchors the broader separatist movement; the Centurion Project, also founded by Parker, was registered as a third-party advertiser in Alberta and campaigned in support of the Stay Free Alberta and Alberta Prosperity Project citizen initiative petition for an independence referendum. Provincial legislation has moved in step. Bill 54, passed in 2025, lowered the citizen-initiated referendum threshold to approximately 178,000 signatures. Bill 14, the *Justice Statutes Amendment Act*, received royal assent in December 2025 in direct response to a Court ruling earlier that month that an independence referendum proposal does not guarantee Aboriginal and treaty rights to the same extent as section 35 of the *Constitution Act 1982*, because those rights only exist within Canada. Bill 14 amended the *Citizen Initiative Act* and *Referendum Act* to permit unconstitutional citizen initiatives to proceed and to relieve the government of any

obligation to implement unconstitutional binding referendum results, with retroactive application to the existing separatist petition. Pollara polling identifies the structurally significant overlap inside Alberta itself: ninety-two percent of Alberta separatists are United Conservative Party (UCP) voters, against sixty-five per cent of Quebec separatists who are Parti Québécois voters. The Alberta separatist movement and the governing party share an electoral coalition in a way Quebec separatism and the PQ do not.[26]

On 30 April 2026, CBC News reported that the Centurion Project had compiled a database of millions of Alberta voters' personal information from an electoral list it had received; on 1 May 2026, *The Globe and Mail* reported that the RCMP was probing the alleged distribution of the list.[27] On 7 May 2026, Elections Alberta confirmed that Chief Electoral Officer Gordon McClure had issued 568 cease-and-desist letters: twenty-three to recipients identified as having received full copies of the voter list, with a signed declaration of compliance required within forty-eight hours, and 545 to recipients identified as having accessed the searchable database while it was active. The database covered nearly three million Alberta voters, including senior politicians, election officials, judges, Crown prosecutors, and journalists. The breach is subject to three concurrent investigations: by Elections Alberta, the Royal Canadian Mounted Police, and Alberta Information and Privacy Commissioner.

The only Canadian institutional response that has so far halted any element of the operational mobilisation is the Crown-indigenous treaty framework rather than the federal security architecture. Sturgeon Lake Cree Nation filed against the Government of Alberta, the Government of Canada, and Alberta's Chief Electoral Officer in January 2026, one of four parallel First Nations challenges that argue that the Government of Alberta is not party to the treaties signed between the First Nations and the Crown of Canada; only treaty parties have jurisdiction to alter or terminate treaties; and therefore Alberta cannot unilaterally proceed toward secession. On 10 April 2026, a judge granted a temporary stay preventing Alberta's Chief Electoral Officer from certifying the Stay Free Alberta petition signatures or referring the matter to the provincial government. As of July 2026 the process has advanced despite the stay: the petition was submitted on 4 May 2026 with the proponent reporting roughly 301,000 signatures against a threshold of approximately 178,000; the petition’s issuance was subsequently quashed and is under

appeal; and following a judicial decision of 29 June 2026, Elections Alberta began signature verification on 6 July 2026, with results expected by 27 July. Premier Danielle Smith has called a referendum for 19 October 2026, at which Albertans will be asked, among other questions, whether to begin a process toward a binding vote on separation. The underlying treaty-rights challenge remains unresolved.[28] Sturgeon Lake Cree v. Alberta is the only Canadian institutional proceeding to date in which foreign interference has been formally adjudicated as a constitutional harm requiring a court-ordered remedy. Federal security architecture has been silent on Alberta separatism. Treaty constitutionalism is doing the work no federal architecture has been built to do.[29]

Foreign-aligned narrative infrastructure, US official engagement at the highest levels, cross-border amplification networks, and a domestic separatist mobilisation using stolen electoral data have aligned on a single political question, with the operational vector running through a member of the governing party's caucus. Russian narrative infrastructure has produced sixty-seven articles on Alberta and the 51st state to Ontario's fourteen across a single network.

US engagement has reached the Treasury Department. The cognitive operation against Canada is, at this moment, more advanced in its operational specificity in Alberta than in any other Canadian province, and the institutional response capable of meeting it is operating from treaty constitutionalism rather than the federal security architecture that should be carrying it.

The Quebec parallel, often raised reflexively as the available analogue, sharpens rather than dilutes the Alberta case. Pollara's recent measurement of provincial cultural distinctiveness places Quebec at seventy-six per cent and Alberta at forty-eight per cent: Quebec separatism rests on an identity claim Alberta separatism does not have. Quebec also has institutional containment architecture Alberta does not have, including *Loi 25* on data sovereignty and a normalised political vehicle in the PQ that Quebec separatism does not need to share with the governing party.[30] The cognitive layer is the most operationally exposed and least institutionally defended of all Canada's vulnerabilities to its closest neighbour.

What Makes Canada Distinctive: Three Pillars

Three structural features distinguish Canada's position on cognitive defence from its closest comparators: a federal architecture, a population and ecosystem operating in advance of institutional architecture, and a record of leadership in adjacent areas not yet carried through to the cognitive layer. Each pillar is a foundation Canada has not yet recognised it has, and that the Alberta moment is making visible.

The first is the federal-provincial-territorial (FPT) architecture with Indigenous treaty rights integrated as both vulnerability and asset. Canadian federalism distributes capture risk, as Germany's federal architecture does, but Canada adds a constitutional dimension Germany does not. Stéphane Dion, the former Minister of Foreign Affairs and Ambassador to both Germany and France, characterised Canada as 'the federation of federations.' His framing identifies four constitutional features that make Canadian intergovernmental relations distinctive: provinces with broad legislative jurisdictions including treaty implementation authority; a parliamentary system producing strong executive governments at both orders; and the presence in Quebec of a national minority that constitutes a provincial majority, giving intergovernmental relations an existential character unknown in other federations.[31] Provinces and territories deliver education, healthcare, and social services. These are the systems on which population-level cognitive resilience rests. FPT coordination, the working architecture through which the federal government and the ten provincial and three territorial governments align across overlapping jurisdictions, is therefore the operational substrate of Layer 1 cognitive defence rather than a constitutional formality. Field research across this study confirmed the absence of any FPT coordination table at which FIMI has been substantively discussed; the gap is most acute at the municipal level, where local political contests with the least national-security oversight are also where foreign interference has the most direct operational impact.[32] Treaty rights, as the Sturgeon Lake Cree case has now made operationally visible, are not a parallel vulnerability to the FPT axis but the constitutional layer through which the FPT architecture has been holding the line where federal security architecture has not.

The second is a population, civil society ecosystem, and academic capacity that already operate in advance of Canadian institutional architecture. The Prime Minister told Davos

that Canada has 'the most educated population in the world,'[33] and Canadian civil society and academia are producing the analytical work needed. Civil society examples include DisinfoWatch and Digital Public Square, along with the Atlantic Council's Digital Forensic Research Lab and the Rapid Response Mechanism Canada Detection Academy, which operate as a hybrid civil society-government partnership delivered with Global Affairs Canada.[34] Academic examples include McGill's Centre for Media, Technology and Democracy and Toronto Metropolitan University's the Dias, with the Rogers Cybersecure Catalyst at Toronto Metropolitan University now also functioning as a convening platform for civil society work on not only cyber security but also foreign interference.[35] The May 2026 *National Unity Under Threat* report, produced by DisinfoWatch with the Global Centre for Democratic Resilience and the Canadian Digital Media Research Network, is the most recent evidence that Canadian civil society analytical capacity is already producing the kind of structured threat assessment and forecasting that institutional architecture, when it arrives, will need to coordinate.

The second pillar extends to private-sector and doctrinal capacity, anchored in one of the strongest cyber security ecosystems among comparator democracies. Canada is consistently ranked in the top tier of the International Telecommunication Union's Global Cybersecurity Index, alongside the United States, United Kingdom, France, Germany, and the Nordic countries.[36] Private-sector cognitive defence capacity has grown directly out of this cyber strength: firms including Sapper Labs Group on the cyber-and-cognitive defence side and eQualitie on the open-source platform integrity side anchor a wider Canadian capability that has supported counter-FIMI operations against Russian and other adversary networks. Canadian doctrinal capacity, anchored in Dave McMahon's Cognitive Forechecking Doctrine paper, articulates the cyber-to-cognitive convergence: adversaries operate cyber and cognitive operations as one ecosystem, while Canada's institutional separation between cyber security agencies and information environment work is itself a vulnerability.[37] The convergence reframes existing Canadian capacity as already substantially in place. Canada has the capability. What it lacks is coordination and authorisation.

The third is Canadian leadership in international institutions and convening platforms adjacent to cognitive defence, where Canada has historically convened, coalition-built,

and standard-set in ways that distinguish it from peer democracies. The clearest example is the G7 Rapid Response Mechanism (RRM), which Canada built and continues to chair, established at the 2018 Charlevoix Summit before any equivalent national agency existed in any G7 country; France's VIGINUM, now the Alliance's reference standard, was established three years later in 2021 and was modelled off of the RRM. Hosted at Global Affairs Canada, the RRM coordinates G7 information sharing and joint attribution of foreign interference and information manipulation operations. The mechanism issued collective response statements three times across 2025 and conducted joint monitoring of Moldova's October 2025 parliamentary elections.[38]

Additionally, in May 2026, the RRM endorsed the Information Manipulation Set (IMS) framework developed by VIGINUM and the European External Action Service as the common analytical standard for foreign information manipulation analysis across G7 members and associate members including Australia, New Zealand, Poland, Sweden, and the Netherlands.

Canada co-founded the Media Freedom Coalition with the United Kingdom in July 2019, now comprising over fifty member states across six continents. Canadian parliamentarians, along with United Kingdom counterparts, also co-founded the International Grand Committee on Disinformation and 'Fake News' in 2018, which brought parliamentarians from twenty-one democracies together to question platform accountability for disinformation; Canada hosted its second session in Ottawa in May 2019.[39] Field research at NATO institutions reveals an uneven Canadian footprint: substantive engagement on the science and research side through the NATO Science and Technology Organization, with Canada among the more active contributing nations and proactive national representation in domains including command and control and artificial intelligence, but near-absence at the institutions that translate research into doctrine and operations. At Allied Command Transformation, leading the Alliance's cognitive warfare concept development, Canada engaged only one doctrine specialist, and only during the final review round; engagement at Supreme Headquarters Allied Powers Europe is similarly limited. ACT, the briefing concluded, is 'not especially aware of Canada's capabilities.'[40] The pattern is consistent: Canada has repeatedly convened and led at the adjacent edges of the cognitive defence file, but has not sustained those

institutions or carried them through to the cognitive layer at the centre. The pieces of leadership exist. The argument has not been fully made.

Coordination Architecture

Canada has political-level coordination architecture for national security broadly. The Cabinet Committee on National Security, established under the Trudeau government in the wake of the foreign-interference scandal of 2022 and 2023 and continued under the Carney government, is the highest-level political body with a national security coordination mandate. Its membership includes the Prime Minister, the Minister of Public Safety, the Minister of Foreign Affairs, the Minister of National Defence, the Minister of Justice and Attorney General, and others with national security-relevant portfolios. Beneath the Cabinet Committee, the legislated reporting relationships are narrow: CSIS reports to the Minister of Public Safety, the Communications Security Establishment to the Minister of National Defence. What Canada does not have is an integrating mechanism for cognitive defence specifically. The Cabinet Committee's membership excludes the Minister of Canadian Identity and Culture (the renamed Heritage portfolio), whose responsibilities include broadcasting policy, cultural industries, and the federal response to online harms and disinformation; the exclusion is consequential because the cognitive warfare file sits operationally inside that portfolio's substantive responsibilities. There is no legislation requiring intelligence assessments or threat advisories to be provided routinely to the Prime Minister, the Minister of Foreign Affairs, the Minister Responsible for Democratic Institutions, or any other minister whose portfolio engages cognitive defence.[41]

Honest Limitations

Put bluntly, the structural absence is sharpest in foreign intelligence. Canada is the only G7 country without a foreign intelligence agency. The *CSIS Act* gives CSIS a domestic mandate with residual foreign collection authority under Section 16; the Communications Security Establishment conducts signals intelligence; no Canadian agency performs the foundational function of clandestine human intelligence collection abroad. Canada cannot independently assess the origins, objectives, or operational methods of foreign influence campaigns targeting its population, and depends on allies to tell it what is happening. In an environment where the United States can be assumed to be neither a reliable nor a

disinterested intelligence partner in this domain, that dependency is a sovereignty problem.

Canada's digital sovereignty exposure operates at every layer of the stack. As Prime Minister Carney said in Canberra: 'strategic autonomy requires sovereign intelligence infrastructure including secure clouds, data, large language models, and enterprise applications.'[42] The structural exposure runs from trade architecture through cloud infrastructure to data governance. The digital provisions of the Canada-United States-Mexico Agreement, which the *Financial Times* described in 2018 as a 'big winner' for Silicon Valley, constrain Canadian regulatory authority over cross-border data flows, source code disclosure, and platform liability.[43] Canadian federal-government workloads run substantially on Microsoft and broader American cloud infrastructure subject to the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act; senior Microsoft executives admitted under oath to the French Senate in June 2025 that the company cannot guarantee the sovereignty of European data stored in its services.[44] The Upper Harbour Data Sovereignty Policy Scorecard of March 2026 grades the Canadian federal government at F; subsequent Upper Harbour analysis of more than 750 software-as-a-service platforms used by Canadian organisations finds two-thirds operated by companies subject to the CLOUD Act and only seventeen per cent Canadian-owned. Quebec is the partial federal exception: *Loi 25* data localisation, earlier engagement with sovereign cloud capacity through pioneer Canadian platforms such as cloud.ca, and the federal Major Projects Office's identification of Quebec, Manitoba, and British Columbia as the provinces with the export-ready electricity capacity required to support sovereign computing place Quebec several years ahead of the federal posture, though Quebec's own flagship public-private digital sovereignty arrangements raise their own governance questions.[45] The federal failure on digital sovereignty is therefore a choice rather than an inevitability of geography or scale.

That choice has played out in concrete decisions over the past year. The *Online Harms Act* of 2024 (Bill C-63) was never passed, dying on the Order Paper at prorogation in January 2025; its successor, Bill C-34, remains before Parliament and unpassed. The Digital Services Tax rescission of June 2025 traded Canada's most concrete digital-sovereignty fiscal instrument as an early concession to the United States in advance of

the broader trade negotiations it was meant to support. The advisory committee Prime Minister Carney established for the upcoming CUSMA review excludes representation from Canada's digital and innovation economy, a sector now constituting approximately ninety-two per cent of S&P 500 value.[46]

Canada's June 2026 AI for All strategy shows the same pattern.[47] It is built around sovereign compute and infrastructure, a homegrown supercomputer and an adoption target, but the governance architecture to match it remains incomplete. The two instruments meant to supply it, the *Safe Social Media Act* (Bill C-34) and the accompanying privacy reform, have been tabled but not passed; C-34 was tabled shortly before the summer recess, did not advance past first reading, and is not expected to receive Royal Assent before the end of 2026.[48] The gap was visible from within the government's own process: a member of the federal AI Strategy Task Force had already argued that a sovereign AI agenda built on infrastructure is insufficient without the governance capacity to sustain public confidence and democratic accountability.[49] Even the tabled bills, however, address platform and consumer harms rather than the security dimension. Canada still lacks an AI foreign policy: a framework spanning alliances, export controls, access to advanced computing, and the risks of military and dual-use systems.[50] That gap, between a sovereignty ambition and the security architecture required to defend it, is the one this report identifies across Canada's cognitive defence posture more broadly.

The social infrastructure foundation is the third honest limitation. The local news ecosystem has eroded significantly: Canada has lost over 250 net local news outlets since 2008, with about half of the closures concentrated in communities of 20,000 people or fewer, producing the information vacuums adversaries fill.[51] Beneath the local journalism collapse sits a wider erosion of the social services that COVID-19 exposed as cracks in the social contract Canadians believe in. Lars Osberg of Dalhousie University, writing in the *Financial Post* at the end of 2025, characterised Canada's safety net as the 'big missing link,' with stagnant real wages and growing economic insecurity going unaddressed at the federal level.[52] YMCA Canada national survey research, conducted with the Angus Reid Forum in late summer 2024, found that sixty per cent of Canadians feel disconnected from their community, with sixty-eight per cent of 18 to 34-year-olds

and seventy-six per cent of unemployed Canadians reporting acute disconnection, and thirty-six per cent reporting no third place outside home or work.[53] The substrate on which Layer 1 cognitive resilience rests is not the layer adversaries target. It is the layer that determines whether the layers above hold.

Beneath these specific failures sits the question of whether the political recognition that has reached the rupture and the sovereignty stack will reach the cognitive layer. At an April 2026 gathering of party loyalists, Prime Minister Carney told the audience that 'we are no longer relying just on the strength of our values. We are also building the value of our strength.'[54] The framing is the right one for the moment. The work that remains is to ensure that social policy, the social services that underwrite Layer 1, and cognitive defence itself are not classed on the values side of the ledger but recognised as integral to the value of Canadian strength. Cognitive defence is enabling condition for all of it: the Defence Industrial Strategy, the half-trillion-dollar investment, the trilateral AI initiative with Australia and India, the Canadian-led low-Earth-orbit satellite constellation. None of these capabilities will be sustained if the information environment through which Canadians consent to fund them has been compromised.

Layer Mapping

Applied to the six-layer framework with its dual foundations, Canada's profile reveals fragments at every layer and coordination at none. The social infrastructure foundation is eroding; the safety net has stagnated; and a majority of Canadians feel disconnected from their communities. Layer 1, individual cognitive capacity and emotional regulation, is structurally undersupplied: Canada has no consistent emotional regulation, critical thinking, or digital literacy mandates across provincial and territorial education systems, leaving the foundational psychological skills required for cognitive resilience to vary by jurisdiction. The June 2026 National AI Literacy Initiative announced under AI for All offers federal AI-literacy training but does not address the absence of consistent provincial and territorial mandates, so the jurisdictional variation this layer identifies persists. Layer 2, integrity of the information environment, is structurally inadequate at the data-sovereignty level, with the Upper Harbour federal grade of F. Data sovereignty straddles Layers 2 and 3, bearing on both the integrity of the information environment and the structural

regulation of platforms; it is treated here at the point where it most directly affects the information environment.

Layer 3, platform architecture and algorithmic accountability, is undeveloped. The original Online Harms Act (Bill C-63) died on the Order Paper when Parliament was prorogued in January 2025. Its successor, Bill C-34, the Safe Social Media Act, was introduced in June 2026 and, notably, would extend regulatory duties to AI chatbot services alongside social media platforms, but it was tabled shortly before the summer recess, did not advance past first reading, and is not expected to receive Royal Assent before the end of 2026. Canada therefore still lacks the structural platform-regulation architecture this layer requires.

Layer 4, detection and attribution, rests on Rapid Response Mechanism Canada, currently insufficient even with the March 2026 announcement's expansion, and on intelligence dependencies the foreign intelligence absence makes acute. Layer 5, active defence, runs through the General Election 2025 (GE45) model and the new Cabinet Directive on the Coordinated Response to Threats to Elections, which extends the Critical Election Incident Public Protocol Panel of Five to a whole-of-government election-period coordination architecture. Layer 6, sovereign response capacity, is incomplete. Institutional coordination operates continuously at the senior bureaucratic level but breaks at the political level, with the Cabinet Committee on National Security excluding the portfolio in which the cognitive warfare file substantively sits. As the Alberta convergence has now demonstrated, there is no integrated Canadian institutional response to cognitive operations targeting domestic political mobilisation, with treaty constitutionalism currently doing the work no federal architecture has been built to do. Political will, the upper foundation, is the binding constraint on the institutional architecture, even as the political-rhetorical recognition is advancing with haste.

Partner Landscape

Canada partners primarily through the G7, the organising body for first-call coordination of international responses, and the Five Eyes intelligence backbone. Both have been compromised in different ways because of the United States. The G7 Rapid Response Mechanism, which Canada built and chairs, comprises the G7 states plus the European

Union, with Australia, the Netherlands, New Zealand, NATO Public Diplomacy Division, Sweden, and Poland as associate members.

France is Canada's deepest bilateral partner on cognitive defence. Cooperation runs through Rapid Response Mechanism Canada, intensified during the G7 French presidency, with a bilateral counter-FIMI working-level meeting currently in development. France's weekly public electoral threat bulletins around its 2026 municipal elections were developed from discussions with the Office of the Privacy Commissioner of Canada about lessons from Canadian general elections. The methodological lineage between Rapid Response Mechanism Canada and VIGINUM, France's vigilance and protection service against foreign digital interference, is operational.[55]

The United Kingdom is Canada's deepest partner on the diplomatic and policy framework that surrounds cognitive defence. The Media Freedom Coalition, co-founded by Canada and the United Kingdom at the July 2019 Global Conference for Media Freedom in London, now comprises over fifty member states across six continents. The UK-Canada bilateral relationship within the Five Eyes architecture continues to operate at working level on cognitive defence and counter-FIMI cooperation, even as both countries face parallel challenges in their relationships with the United States.[56]

Ukraine is Canada's closest partner on operational depth. The Canada-Ukraine Strategic Security Partnership of 24 February 2024 is the only bilateral security agreement Canada has signed, and the only such agreement any G7 partner has signed with Ukraine, that explicitly names 'Strengthening Information Security and Countering Disinformation' as a cooperation domain.[57] The agreement records both governments' acknowledgement that Ukraine has unprecedented experience and knowledge in countering disinformation that Canada has more to learn from than to teach. Operation UNIFIER, Canada's military training mission for Ukraine since 2015, was extended on 24 February 2026 to 2029.

Poland, through the Strategic Partnership of 25 August 2025, is the only one of Canada's bilateral strategic partnerships to explicitly name FIMI as a discrete enhanced cooperation domain. The Canada-Sweden, Canada-Finland, and Canada-EU partnerships name 'hybrid threats' and 'cyber' as cooperation domains, which conventionally encompass FIMI but do not name it as a discrete focus. The inaugural Canada-Poland High-Level

Steering Group meeting in Ottawa in April 2026 included FIMI resilience as an agenda item.[58]

Latvia is the partner where Canadian institutional commitment is most operationally embedded and where the cognitive threat environment is most acute. Canada has been the NATO framework nation in Latvia since 2017, leading the multinational battlegroup at Camp Adazi as part of NATO's enhanced Forward Presence; in July 2023, Canada and Latvia signed the Roadmap to scale the battlegroup to a brigade-size formation, and the resulting Multinational Brigade Latvia is now the largest sustained Canadian military deployment abroad. Latvia has been a consistent target of Russian cognitive operations since well before the 2022 full-scale invasion of Ukraine, and Latvia's response has been one of the most institutionally developed in the Alliance. The Prime Minister's identification of the Latvia mission at Yerevan as an instance of the value of Canadian strength is the rhetorical recognition; the substantive partnership opportunity is in connecting operational integration on the ground to the cognitive defence file at the policy level.[59]

The Canada-European Union Security and Defence Partnership of 23 June 2025 names cyber, hybrid threats, and emerging disruptive technologies as cooperation domains, with the annual Canada-EU Security and Defence Dialogue, ongoing since 2015, as the operational mechanism. Canada has also increasingly partnered with the Nordic 5 (Denmark, Finland, Iceland, Norway, and Sweden) on Arctic security, hybrid threats, and economic security. The Joint Statement of the Prime Ministers of the Nordic Countries and Canada, issued in Oslo on 15 March 2026, commits the six countries to enhanced cooperation across hybrid threats, technology cooperation in quantum, AI, satellite, and space, and economic security in a context where 'technology and international trade [are] increasingly being used as a coercive tool,' and commits the parties to meeting more regularly.[60]

Canada's Unique Opportunity

Canada is the furthest behind among the developed democracies studied at the level of institutional architecture for cognitive defence. The political-rhetorical recognition has, on certain dimensions, moved faster than in some comparator countries: the Prime Minister has named the rupture, the sovereignty stack, and the strategic autonomy imperative within three months. The gap is now operational, not conceptual. Because Canada has

yet to establish coordinated cognitive defence architecture, it has the rare advantage of learning from its partners. The Prime Minister's 'variable geometry' framework names exactly the principle on which Canada can integrate the best of what each country has to offer while replicating none of them in full. The window is narrow. The moment is ripe for the taking.

Endnotes

1 Prime Minister Mark Carney, Liberal leadership victory speech, Ottawa, 9 March 2025.

2 Prime Minister Mark Carney, '*Principled and Pragmatic: Canada's Path*,' address to the World Economic Forum Annual Meeting, Davos, Switzerland, 20 January 2026.,

3 Prime Minister Mark Carney, *Forward Guidance* video series, inaugural episode, released 19 April 2026. See also David Coletto, 'Mark Carney, Forward Guidance, and the Politics of Reassurance,' *inFocus*, 19 April 2026.

4 Prime Minister Mark Carney, opening plenary remarks, eighth European Political Community Summit, Yerevan, Armenia, 4 May 2026.

5 Government of Canada, 'Government of Canada Introduces Measures to Further Protect Canada's Electoral Processes and Strengthen Democracy,' announcement by the Honourable Steven MacKinnon, Minister of Transport and Leader of the Government in the House of Commons, Ottawa, 26 March 2026. Bill C-25, Strong and Free Elections Act, was introduced in the House of Commons on the same date and addresses recommendations from the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions (PIFI, the Hogue Commission).

6 Prime Minister Mark Carney, sovereign cloud announcement at the Major Projects Office, Edmonton, September 2025; reported in BetaKit and *The Quantum Insider*, September 2025.

7 Marcus Kolga, Jennie Phillips, Brian McQuinn, and Bartel Van de Walle, National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum (DisinfoWatch, Global Centre for Democratic Resilience, Canadian Digital Media Research Network, CASi Labs, and Media Ecosystem Observatory, 6 May 2026), p. 4, disinfowatch.org.

8 On the McDonald Commission, see Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police (Justice David McDonald, Chair), *Second Report: Freedom and Security under the Law*, 1981.

9 The Honourable Anne McLellan, *Securing an Open Society: Canada's National Security Policy*, Government of Canada, 27 April 2004.

10 Standing Senate Committee on National Security, Defence and Veterans Affairs, Russia's Disinformation: Understanding the Challenge, Strengthening Canada's Response (Senate of Canada, April 2026), sencanada.ca.

11 Andrew Coyne, 'Canada Is Uniquely Unprepared for the Dire National-Security Crisis We Are Now In,' *The Globe and Mail*, 6 February 2026.

12 Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *Final Report* (Hogue Commission), January 2025.

13 Canadian Security Intelligence Service, *CSIS Public Report 2025*, 1 May 2026, https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2025.html

14 Joint Statement on Iranian State Threat Activity in Europe and North America, issued by the United States, the United Kingdom, Albania, Austria, Belgium, Canada, Czechia, Denmark, Finland, France, Germany, the Netherlands, Spain, and Sweden, 31 July 2025; and Canadian Security Intelligence Service, CSIS Public Report 2025 (Canadian Security Intelligence Service, May 2026), canada.ca, on the Pakistan naming.

15 David Vigneault, testimony before the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, 27 September 2024

16 Nanos Research, weekly tracking poll on Canadian-American relations, fielded 31 January to 4 February 2026, published 23 February 2026.

17 Dan Arnold, 'Bye Bye, Mon Cowboy,' Pollara Strategic Insights Substack, 7 May 2026.

18 United States Department of Justice indictment, *United States v. Kalashnikov and Afanasyeva*, September 2024, on Tenet Media and the alleged covert Russian funding of US influencers

19 The Honourable Bob Rae, 'Canada and the New US National Security Strategy,' *Policy Magazine*, 9 December 2025.

20 Scott Bessent, interview with Jack Posobiec, *Real America's Voice*, 22 January 2026

21 ibid

22 Andrew Coyne, 'MAGA's plan for Canada: not annexation, but dismemberment,' *The Globe and Mail*, 27 March 2026.

23 Joseph Gedeon, 'US Directs Embassies to Team Up against Foreign Hostility, and Use X to Counter Anti-American Propaganda,' *The Guardian*, 30 March 2026

24 Media Ecosystem Observatory, Canadian Digital Media Research Network, *Slopaganda: A Coordinated Network of Inauthentic YouTube Channels Promoting Alberta Separatism and US Annexation*, McGill University and University of Toronto, April 2026

25 Marcus Kolga, Jennie Phillips, Brian McQuinn, and Bartel Van de Walle, *Decision Making and National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum*, DisinfoWatch, the Global Centre for Democratic Resilience, the Centre for Artificial Intelligence Data and Conflict, the Canadian Digital Media Research Network, and CASi Labs, 6 May 2026 26

26 Dan Arnold, 'Bye Bye, Mon Cowboy,' The Pollara Substack, Pollara Strategic Insights, 7 May 2026, pollarastrategicinsights.substack.com.

27 Patrick Lennox, 'How Did an Alberta Separatist Group Get Its Hands on the Voter List?' *The Walrus*, May 2026

28 Elections Alberta set to begin verifying signatures on separatist referendum petition, CBC News, 6 July 2026.

29 Jesmeen Gill, 'Judge orders pause on signature validation process for Alberta independence petition,' CBC News, 10 April 2026

30 Dan Arnold, 'Bye Bye, Mon Cowboy,' The Pollara Substack, Pollara Strategic Insights, 7 May 2026, footnote 4, pollarastrategicinsights.substack.com.

31 Stéphane Dion, 'Canada: The Federation of Federations,' remarks delivered during the panel 'Canada's Levels of Government and the Diplomatic Community,' organised by the Forum of Federations and the Parliamentary Centre, Ottawa, 16 April 2026

32 Field research synthesis. Attribution to research programme, not to individual interviewees

33 Mark Carney, '*Principled and Pragmatic*.'

34 Atlantic Council, 'Atlantic Council's DFRLab Delivers the G7 RRM Digital Transnational Repression Detection Academy,' press release, November 2025

35 Toronto Metropolitan University, *Sovereignty at Stake: Online Disinformation and Canadian Democracy*, Rogers Cybersecure Catalyst, Toronto Reference Library, 6 May 2026

36 International Telecommunication Union, *Global Cybersecurity Index 2024*, Geneva, 2024.

37 David McMahon, 'Cognitive Forechecking: A Canadian Doctrine for the Cognitive Domain,' Sapper Labs Group, 2024

38 Group of Seven Rapid Response Mechanism, collective statements: response to Russian influence campaign, January 2025

39 Media Freedom Coalition, founded at the Global Conference for Media Freedom, London, 10 to 11 July 2019; International Grand Committee on Disinformation and 'Fake News,' inaugural meeting London, 27 November 2018, and second meeting hosted by the Standing Committee on Access to Information, Privacy and Ethics of the House of Commons of Canada, Ottawa, 28 May 2019.

40 Field research at NATO Allied Command Transformation. Attribution to research programme, not to individual interviewees

41 Privy Council Office, Cabinet Committee on National Security, mandate and membership documentation. *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23; *Communications Security Establishment Act*, S.C. 2019, c. 13, s. 76.

42 Prime Minister Mark Carney, address to both Houses of Australia's Parliament, Canberra, 5 March 2026.

43 Shawn Donnan and James Politi, 'Silicon Valley Is Big Winner from Trump's New Trade Deal,' *Financial Times*, 2 October 2018

44 French Senate, Commission of Inquiry on the Influence of Foreign Consulting Firms, hearings of June 2025

45 *An Act to modernize legislative provisions as regards the protection of personal information*, National Assembly of Quebec, 2021

46 Joshua van Es, 'Canadian Data Sovereignty Policy Scorecard,' Upper Harbour Research, March 2026

47 Innovation, Science and Economic Development Canada, Canada's National Artificial Intelligence Strategy: AI for All (Government of Canada, 4 June 2026), https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all.

48 Parliament of Canada, LEGISinfo, Bill C-34, Safe Social Media Act, 1st Session, 45th Parliament, https://www.parl.ca/legisinfo/en/bill/45-1/c-34.

49 Taylor Owen, "Final Report to the AI Strategy Task Force," Centre for Media, Technology and Democracy, January 2026.

50 Branka Marijan, "Canada's AI Strategy Is Missing a Foreign Policy," Centre for International Governance Innovation, 8 June 2026.

51 Andrew Phillips, Edward Greenspon, and Alison Uncles, *The Lost Estate: How to Put the Local Back in Local News*, Public Policy Forum, Rideau Hall Foundation, and Michener Awards Foundation, 4 February 2025.

52 Lars Osberg, quoted in 'Millions of Canadians Struggling as Social Safety Net Lags Behind Federal Priorities: Economist,' *Financial Post*, 31 December 2025

53 YMCA Canada, national survey conducted with the Angus Reid Forum, 29 August to 3 September 2024

54 Prime Minister Mark Carney, remarks at the 2026 Liberal National Convention, Montreal, 11 April 2026.

55 Government of Canada, *Canada-France Declaration on Ethical Artificial Intelligence*, 7 June 2018

56 Media Freedom Coalition founding documentation; Foreign, Commonwealth and Development Office (UK) and Global Affairs Canada (Canada) joint communications, July 2019

57 Government of Canada and Government of Ukraine, *Canada-Ukraine Strategic Security Partnership*, signed in Kyiv, 24 February 2024.

58 Government of Canada and Government of Poland, *Canada-Poland Strategic Partnership*, announced in Warsaw, 25 August 2025.

59 NATO enhanced Forward Presence Battle Group Latvia, established 2017 with Canada as framework nation; Canada-Latvia Roadmap, signed July 2023, scaling the battlegroup to a brigade-size formation

60 Government of Canada and European Union, *Canada-European Union Security and Defence Partnership*, signed at the 20th Canada-EU Summit, Brussels, 23 June 2025

Chapter 10: The EU and NATO

A senior official at Supreme Headquarters Allied Powers Europe offered the author this assessment during the research: "We have done reasonably well on narrative advantage, and we are hopelessly losing on psychological and decision advantage, and we are doing nothing about it." The three-part cognitive advantage framework – narrative, psychological, decision – is the operational scaffold the rest of the Alliance's cognitive-defence work is built around. It is also the framework against which both the EU's regulatory architecture and NATO's doctrine should be assessed. Korobeynikov, Davydiuk, and Mokhor argue that cognitive warfare differs ontologically from information warfare because it targets the structures through which knowledge is constructed rather than what people know. In democracies, cognitive operations subvert coherence across multiple layers of the social-technical system; in centralised regimes, they inject informational entropy into a single dominant interpretative layer.[1] Cognitive warfare is the condition within which contemporary politics now operates, not a separate domain alongside it.

The EU and NATO are the two hemispheres of the democratic cognitive-defence architecture. The EU is the world's most consequential regulatory power for the information environment. NATO is leading the effort to define cognitive warfare as a military concept.

NATO ACT defines cognitive warfare as "activities conducted in synchronization with other Instruments of Power, to affect attitudes and behaviours by influencing, protecting, and/or disrupting individual and group cognitions to gain an advantage." What the Alliance has not yet politically approved is the broader concept that operationalises this definition.

Neither hemisphere is complete without the other. The EU is developing deterrence-adjacent instruments through the FIMI Deterrence Playbook, sanctions architecture, counter-hybrid measures, and the sword framing HR/VP Kallas has now institutionalised, but it cannot generate the military cognitive capability or the binding Alliance commitments that deterrence at scale requires. NATO has no regulatory mandate over platforms and cannot compel governments on information-environment governance, but it exerts

political signalling through the StratCom board and embeds whole-of-society requirements in its doctrine. Neither is moving fast enough.

A senior NATO official offered the sharpest conceptual framing available during field research: if Clausewitz held that war is the continuation of politics by other means, cognitive warfare dissolves that distinction entirely. Adversaries are not attacking democracies from outside the political space. Democracies designed their security institutions around a boundary between war and politics that cognitive warfare has rendered obsolete. The fight is not something that can be switched on in crisis and off in peacetime. It is the permanent condition of open societies in an era of great-power competition in the digital age.

The EU as Regulatory Power

The EU's regulatory instruments for countering cognitive threats, the Digital Services Act (DSA), the Digital Markets Act (DMA), the European Media Freedom Act (EMFA), and the FIMI Deterrence Playbook, are best understood as an integrated approach rather than as standalone instruments. The DSA and DMA represent the democratic world's most consequential framework for platform accountability. Three years into enforcement, the DSA has produced genuine behavioural change in platform design and risk-assessment cycles. The TikTok preliminary findings on addictiveness are the landmark. They concern design rather than content, setting a precedent to inform further action. The 2025 enforcement cycle has produced its first formal non-compliance decision: a 120 million euro fine on X in December 2025 for breaches of transparency obligations under Articles 25, 39, and 40, with ongoing preliminary findings against TikTok now suggesting the enforcement cycle has moved from anticipated to operational.[2]

The EU's most significant analytical contribution is its methodological choice in FIMI response architecture. The ABCDE framework, i.e. structuring responses by Awareness, Building resilience, Countering threats, Deterring adversaries, and Engaging partners, deliberately prioritises behaviour over content.

Content-first framing reduces the contest to a battle of narratives and hands adversaries the freedom-of-expression argument. Behaviour-first enables a legally compelling attribution case without reference to what is being said and unlocks response options

beyond strategic communications. Visible content is the narrow tip of the iceberg; the infrastructure behind it, coordinated account networks and servers behind look-alike websites, is where the manipulation is actually happening.

Press freedom protection is the regulatory architecture's third leg. In force since August 2025, the EMFA addresses the kind of state media consolidation documented in Hungary, where government-aligned ownership was used to convert independent outlets into vehicles of political propaganda. The instrument's implementation capacity at member-state level is uneven. Without operational capacity, the EMFA is the Code of Conduct on Disinformation problem in a different domain: a regulatory architecture without enforcement is voluntary self-regulation by another name. The European Fact-Checking Standards Network's March 2026 white paper, 'The Great Retreat', documents the consequence: in the period following the 2024 US election, Google, YouTube, LinkedIn, and other major platforms have unsubscribed from or significantly scaled back their commitments under the EU Code of Practice on Disinformation. The voluntary regime is collapsing in the direction of withdrawal rather than scaling, which is the specific evidence that supports moving the EMFA, the Code, and platform accountability mechanisms onto binding rather than voluntary architecture before the regulatory window closes. [3]

Limitations remain. The constructive-dialogue approach to DSA enforcement tends toward malicious compliance Platforms are sophisticated actors, with every incentive to appear cooperative while minimising actual behavioural change. The data layer underneath both instruments is inadequately protected: if data-protection rules are not properly enforced, interoperability remedies and competition interventions are built on sand. No European leader has yet publicly reclaimed the freedom-of-expression narrative from the Musk-Vance framing that portrays EU content governance as censorship. That counter-narrative is entirely available, factually grounded, politically deliverable, and the window for making it is closing.

NATO's Cognitive Warfare Doctrine: From Concept to Capability Gap

The NATO doctrine architecture sits across three institutional layers: ACT for concept development, STO for the scientific foundation, and SHAPE for operational integration. ACT has carried the cognitive warfare concept development since 2020, with the concept

now received military-level approval but remaining politically stalled within the Alliance. The 2026 Cognitive Warfare Paper, which formalises ACT's operating concept, addresses what one analyst has characterised as the crisis of discovery: the gap between the conceptual frameworks ACT has articulated and the operational capabilities Allies are willing to fund.

STO has been building the scientific foundation since 2007 and was advocating for cognitive warfare as a domain concept by 2010. The research community spans five to six thousand scientists across thirty-two Allies and five S&T Enhanced Partnership nations.

The Human Factors and Medicine panel carries the primary cognitive warfare research load and is ranked the second most active panel across all STO work. The five leading contributors over the past five years are the United States, Norway, Germany, the Netherlands, and Sweden. Norway initiated the cognitive warfare challenge within the Human Factors and Medicine panel, making it the initiating nation for the Alliance's most substantive research agenda.

SHAPE operates the implementation layer, with the StratCom coordination board bringing eighteen of thirty-two Allies into monthly coordination on a three-month planning horizon, capable of issuing guidance within hours before major announcements. The Nexus platform operates with close to one hundred personnel across Allied Command Operations. The methodological foundation on which attribution at the Alliance level rests has been most recently advanced by the NATO StratCom Centre of Excellence in partnership with the Ukrainian Centre for Strategic Communications: their February 2026 joint report, ‘Attributing Russian Information Influence Operations’, tests an information-influence attribution framework against real-world Russian cases and provides the operational methodology democracies need before they can expose, sanction, or impose costs on adversary information operations. Attribution capacity is the precondition for every active-defence response measure the Alliance might choose to deploy.[4]

The offensive capability gap is NATO's most consequential acknowledged deficit. Field research within NATO's operational planning community assessed that only the United States, the United Kingdom, and France currently maintain dedicated military capability

to conduct influence operations directed at audiences inside an adversary state. Twenty-nine Allies do not. The minimum viable capability package is not technically complex: information environment assessment capacity, behavioural science expertise, information planners, established channels, and effect assessment methodology. What is missing is career streams, dedicated expertise, and the political will to activate the tools in peacetime.

NATO does not conduct offensive cognitive operations at the Alliance level, and the case for that restraint is strong. Cognitive operations directed at foreign civilian populations corrode the democratic norms they are meant to protect. The appropriate posture for sustained great-power competition below the kinetic threshold is proactive capacity that remains latent until the threshold is crossed. The resolution is not to abandon restraint but to invest seriously in proactive latent capacity: developing deep analytical understanding of adversary societies, their political pressures, their vulnerabilities, and the architecture of their information operations.

The Convergence and the Gap

FIMI and cognitive warfare are converging at the operational level. The EEAS gave its own clearest institutional signal of this shift at its 4th annual Counter FIMI Conference in March 2026, where HR/VP Kallas delivered the keynote under the title 'From Insight to Impact': the framing the EEAS itself chose to signal a deliberate move from diagnosis to deterrence operations. The DISARM framework (Disinformation Analysis and Risk Management), which cross-references the MITRE ATT&CK taxonomy (the US-government-backed catalogue of adversary tactics, techniques, and procedures originally developed for cybersecurity), makes this convergence technical rather than rhetorical. DISARM developed from the Cognitive Security Collective, a civil society organisation that applied cybersecurity methodology to information operations, which approached manipulation the way cybersecurity approaches attacks, treating the human brain as hackable infrastructure. The EU Disinfo Lab's work on building a common operational picture of FIMI using Information Manipulation Sets (IMS) provides a structured format for describing FIMI threats that allows cross-system sharing, analogous to how cyber threats are described with TTPs and indicators of compromise. NATO and EU institutions are

working toward DISARM as a shared situational awareness tool. That IMS is still a new EEAS term illustrates the central tension: the aspiration for common language and the reality of continued terminology proliferation coexist. The Konrad-Adenauer-Stiftung Canada's own work on democratic resilience confirms that the institutional conversation this chapter describes is already underway.

What is working? The Ukraine Communications Group is the clearest operational coordination success in the EU FIMI ecosystem, running without US participation and keeping the door open for return. The FIMI ISAC (Foreign Information Manipulation and Interference Information Sharing and Analysis Centre) operationalises evidence in a common format using OpenCTI, an open-source threat intelligence platform. The EEAS analytical methodology has been exchanged with the United Kingdom to near-interoperability, with monthly working-level exchanges. Blue Sky cooperation closed down the Doppelgaenger and Matrioshka operations on that platform. The same approach with X did not succeed. The deeper structural gap is administrative: FIMI sits under a different directorate than hybrid and cyber inside the EEAS, which a well-placed source described as stemming from a wrong institutional understanding of the threat. The ideal structure would place Hybrid Threats and Cyber as an overarching designation covering all hybrid domains, including cognitive warfare.

The national layer is the bottleneck for both institutions. The DSA requires national digital services coordinators, the officials each member state must designate to oversee platform compliance and enforce the regulation domestically, and most member states do not yet have adequate capacity in these roles. NATO's StratCom coordination board works only when Allies show up. The STO's research depends on national champions to develop outputs into doctrine and procurement. Information sharing standards represent the foundational unsolved technical problem: there is no FIMI equivalent of the cyber domain's taxonomy of tactics, techniques, and procedures that would allow cross-system sharing of threat descriptions. Chapter 29 returns to these findings in cross-case comparison.

Honest Limitations

NATO’s honest limitations begin with the gap between institutional awareness and operational readiness. Practitioners working inside the Alliance describe the situation with a consistent formulation: cognitive warfare is understood as a concept, but most member states are still fighting the last war, still prioritising the last threat environment over the one that is already here. One interviewee positioned within NATO confirmed that the cognitive warfare concept has received military-level approval within the alliance but remains politically stalled, blocked in part by officials who have not engaged with the concept itself. They assessed that the term has nonetheless achieved sufficient currency across allied militaries and public discourse that it is now effectively irreversible regardless of formal political ratification, and that the risk facing the alliance is not ethical overreach in the offensive domain but paralysis through inaction. Even the most advanced NATO members are nowhere near where they need to be. The Alliance has built genuine capability in the J10 structure, the StratCom coordination board, and the Nexus platform, but those capabilities are concentrated in a small number of Allies and accessed unevenly across the other twenty-nine. The offensive capability gap is the sharpest expression of this, but the asymmetry runs through every layer. The STO's research pipeline is producing analysis that exceeds what most national capitals are able to absorb, process, or fund. The translation problem from scientific output to national doctrine and procurement is structural, not incidental.

NATO also faces the endogenous threat from within its own membership. Hungary’s systematic obstruction of collective action under the Orbán government, documented in leaked recordings published in April 2026 as including the near-real-time provision of intelligence from EU Council meetings to Russian counterparts, and Slovakia’s parallel alignment with Russian positions on Ukraine, represent a categorically different threat from the difficult but ultimately Alliance-committed posture of other NATO members whose interests are complex. Field research draws the distinction precisely: Türkiye uses its NATO membership as leverage to advance bilateral interests, and its domestic political discourse overlaps with Russian anti-Western narratives through shared Eurasianist sentiment rather than by design. Its strategic interest is nonetheless in a strong Alliance. Türkiye has not blocked Ukraine support, has not coordinated with Russia against

Alliance decisions, and views NATO as an indispensable counterweight to Russian power. It belongs in a separate analytical category: a difficult partner whose interests require careful management, not a disruptive force aligned with adversary strategic goals in the manner of the Orbán-era Hungarian government and Slovakia. The April 2026 Hungarian election, in which Péter Magyar's Tisza party defeated Fidesz with 141 of 199 parliamentary seats, may mark a tide-turning moment: within a week of the result, European Commission officials had travelled to Budapest to discuss the unblocking of frozen EU funds, and the new government has signalled support for the EU's position on Ukraine and a clear pivot away from Moscow. Whether the Hungarian shift holds, and whether Slovakia follows, is the open question on which the Alliance's endogenous-threat picture will turn over the next twelve months.[5]

Most acutely, the restraint that Allies rightly maintain on offensive cognitive operations, while normatively correct, is used by those who oppose investment in the domain to limit ambition across the board. Proactive latent capacity, built in peacetime but held in reserve, is the architecture that resolves this tension without abandoning it.

One final honest limitation deserves naming: the NATO cognitive warfare concept, despite years of development, has not yet been approved at the political level within the Alliance. The institutional and military layers have moved, however the political layer has not yet caught up. Until it does, the concept lacks the formal authorisation that would unlock sustained resourcing and cross-ally commitment.

External partnerships with Canada, Norway, the United Kingdom, Australia, and Japan are strategically important rather than diplomatically decorative. The Coalition for Defence of Democracy (CDN), a civil society organisation dedicated to identifying and countering foreign information manipulation operations, methodology was developed for approximately €500,000 over three years and adopted by NATO and EU institutions at no cost. It is the largest active FIMI takedown operation in Europe and operates on a shoestring. Practitioners assess the cognitive dimension as a larger long-term threat than the cyber domain, yet resources flow through cyber because that is where the political capital sits.

Layer Mapping

The EU and NATO operate across the six layers with very different footprints. Social infrastructure is outside both institutions' direct remit: it is member state and Ally responsibility, though the EU can fund capacity building in less-prepared states and NATO sets the whole-of-society conceptual frame without being able to deliver it. Societal resilience is moderate at the EU and NATO level: the Niinisto Report, ‘Safer Together’ (October 2024), commissioned by Commission President von der Leyen from former Finnish President Sauli Niinisto, formally recommended the Finnish comprehensive security model to the EU as a whole, with the report’s central argument being that whole-of-society resilience, citizen engagement, psychological preparedness, and private sector readiness are not optional add-ons to deterrence but its foundation; the European Centre for Democratic Resilience, launched in February 2026, is the institutional response to that recommendation, with its mandate still forming and its political weight still to be established.[6] NATO embeds the whole-of-society requirement in its cognitive warfare concept while depending entirely on national delivery to achieve it. Information environment integrity is strong via the EU and developing via NATO: the DSA and DMA represent a global standard, the Code of Conduct on voluntary self-regulation is now demonstrably weakening as platforms retreat, and NATO's Nexus platform with close to one hundred personnel represents genuine operational capability. Detection and attribution are strong: the EEAS FIMI toolbox with its four lines of defence framework, EUvsDisinfo, the FIMI ISAC using OpenCTI, and NATO's StratCom COE Nordic-Baltic monitoring network are all operational, though crisis coordination remains case-by-case rather than standing. Active defence is limited for both: the FIMI Deterrence Playbook published March 2026 and HR/VP Kallas's sword framing are the strongest signals yet, but NATO's three-of-thirty-two offensive capability gap and the Alliance-level prohibition on developing offensive cognitive operations mean the deterrence layer remains the most underdeveloped. Sovereign response capacity is partial: the DSA is an enabling framework whose effectiveness depends entirely on national digital services coordinator capacity that most member states do not yet have, while Baltic states represent the most advanced use of existing legal frameworks, a model most Allies have not yet followed. Political will and elite coherence are uneven: the Democracy Shield is a political signal,

eighteen of thirty-two allies are on the StratCom coordination board, but the Hungary ceiling limits EU collective posture and Alliance cohesion remains what adversaries are most actively targeting, and what NATO is most afraid of losing.

Partner Landscape

The EU and NATO cooperate with external partners at very different depths. For the EEAS, the United Kingdom is the benchmark: near-methodological interoperability on FIMI analysis, monthly working-level exchanges, and the FIMI Forum co-organised with the Foreign, Commonwealth and Development Office. No other external partner is at that level. Norway sits one tier below: a Security and Defence Partnership exists and there are occasional exchanges, but operational cooperation is minimal. Canada has moved from being absent from the EEAS FIMI equation four years ago to clearly visible, with the Canada-EU Security and Defence Partnership signed in June 2025 naming cyber, hybrid threats, and FIMI as explicit cooperation domains, and Canada demonstrating operational capacity through the DFRLab and Global Affairs Canada G7 Rapid Response Mechanism Digital Transnational Repression Detection Academy in November 2025. Canada is closer to Norway than to the UK in current operational depth on FIMI cooperation with the EEAS, with the gap representing a choice rather than a structural constraint. The eighth European Political Community Summit in Yerevan in May 2026, where Carney articulated the seven domains of strategic autonomy, is the political-authorisation moment the operational deepening can build on.

The Norway comparison requires a precision: in the NATO STO research pipeline, Norway is a leader, having initiated the cognitive warfare research challenge within the Human Factors and Medicine panel and driven the Alliance's most substantive scientific work in the domain. The two pictures are not contradictory. Norway invests heavily in the S&T research layer and lightly in the EEAS operational partnership layer; Canada is the inverse. Both gaps are choices. The EU SDP portfolio covers virtually all like-minded partners on hybrid threats and FIMI, with the EU-India partnership the sole exception, reflecting India's distinct threat posture and continued engagement with Russian information architecture. For NATO, Ukraine is the most operationally integrated external partner given the active conflict; the Ukraine Communications Group is the proof of

concept for what genuine working-level partner integration produces. The AP4 partners engage on conventional defence and emerging technology rather than cognitive warfare doctrine.

Endnotes

1 Fedir Korobeynikov, Andrii Davydiuk, and Volodymyr Mokhor, "Ontological Foundations of Cognitive Warfare" (NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2026).

2 European Commission, decision imposing a €120 million fine on X for breaches of Digital Services Act transparency obligations under Articles 25, 39, and 40 (Brussels, 5 December 2025), ec.europa.eu. On TikTok preliminary findings on addictive design, see European Commission, Digital Services Act enforcement proceedings against TikTok, ec.europa.eu.

3 European Fact-Checking Standards Network, *The Great Retreat*, policy white paper, EFCSN, 3 March 2026, efcsn.com.

4 NATO Strategic Communications Centre of Excellence and Ukrainian Centre for Strategic Communications, *Attributing Russian Information Influence Operations: Testing the Information Influence Attribution Framework with Real-World Case Studies*, joint publication, NATO StratCom COE, Riga, 12 February 2026, stratcomcoe.org.

5 VSquare, FRONTSTORY, Delfi Estonia, The Insider, and the Investigative Centre of Jan Kuciak, 'Kremlin Hotline: How Hungary Coordinates With Russia Blocking Ukraine From the EU,' VSquare.org, April 8, 2026.

6 Sauli Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, report by the Special Adviser to the President of the European Commission, European Commission, October 2024, commission.europa.eu.

Part IV: Collective Security for the Cognitive Domain

Chapter 11: The Fracturing Alliance

There are moments in history when the future is genuinely undetermined and the past is definitively gone. Not transitional moments, in which one configuration of power gives way to another within a stable frame, but rupture moments, in which the frame itself breaks. Fawaz Gerges, professor of international relations at the London School of Economics, speaking in April 2026, described the current conjuncture as the most dangerous moment in world history since the end of the Second World War in 1945, and attributed this assessment not to personal alarm but to relative consensus among historians and students of international relations. The United States, he observed, built the international system after 1945. It is now disrupting the very system it built.[1] The assessment is harsh. It is also, on the available evidence, accurate.

The liberal international order that emerged from 1945 was not a natural equilibrium. It was a constructed one, underwritten by a hegemon that was simultaneously the world's largest economy, its dominant military power, and, critically, a state committed to a set of values, rule of law, democratic governance, freedom of expression, and the protection of individual rights against the power of both states and demagogues, that it was willing to spend blood and treasure defending. The application of those values was, from the outset, selective and geographically uneven. Much of the Global South experienced the same order as a structure of dependency, Cold War proxy conflict, and extractive economic relationship rather than the rules-based system its architects proclaimed. The Soviet Union and China built their legitimacy partly on that hypocrisy, and adversary cognitive operations continue to exploit it accurately. What the order provided to those within its embrace, however, was real: liberal democracies that accepted its architecture built wealth, stability, and rights protections that were genuinely distinctive. The critique of the order's selective application does not dissolve the value of what it protected where it was applied; it names the gap between the promise and the practice that adversaries have always found most effective to weaponise. Adrian Wooldridge, writing in 2026, frames the historical arc precisely: Britain played the role of liberal hegemon through the

nineteenth century, until its economy could no longer sustain the commitment. The United States assumed that role after 1945, cooperating with international institutions while writing the checks and enforcing the order through its alliances. What we are witnessing now, Wooldridge argues, is the first time a country has voluntarily abnegated that position, not because it lacks the economic or military capacity to sustain it, but because its domestic politics have fractured to the point where the political will to sustain it has collapsed.[2] President Alexander Stubb of Finland offers the more optimistic counterpoint: distinguishing an ideological MAGA strand hostile to the liberal international order from a transactional America First strand that simply ranks Europe third geographically, he argues the rupture is real but navigable and that the institutions of democratic order retain adaptive capacity.[3] The roots of America's global irresponsibility, in his formulation, are domestic. A structural counterargument demands acknowledgment before proceeding. John Mearsheimer's offensive realism holds that the liberal international order was never a genuine expression of American values but an artefact of unipolarity, a hegemonic project that served US interests when the United States was strong enough to impose it, and which recedes as multipolarity reasserts itself.[4] On this reading, what looks like abandonment is structural adjustment, not political choice, and no amount of allied coalition-building can substitute for the gravitational pull of great power competition. The evidence assembled in this report does not support that conclusion. The causal mechanism is domestic political fracture, not structural multipolarity: the United States retains the economic weight and military capacity to sustain its hegemonic role, and its withdrawal is a choice made by a particular political coalition, not a structural inevitability. Stubb's two-strand analysis reinforces this: the ideological strand is a political project, not a geopolitical constraint. But the realist prediction, that middle power coalition-building will face superpower resistance and structural limits, deserves the weight it carries.

The forces shaping this moment operate at a scale beyond any single democracy's control, and this report does not pretend otherwise. The fracturing of the liberal international order is not primarily a product of Russian information operations, though Russia has exploited the fracture with skill and persistence. It is not primarily a product of Chinese strategic competition, though China has positioned itself to benefit from the vacuum. It is, at its deepest level, a product of the internal contradictions of democratic

capitalism in the digital age: the platform economy that has concentrated wealth and fragmented attention, the information environment that has made shared truth contingent rather than foundational, and the political economy of grievance that has made authoritarian simple answers more attractive than democratic complicated ones. Wooldridge identifies the tech companies as the greatest threat to the liberal world order precisely because they are generating this condition from within: a world in which attention is fragmented, misinformation is structural, and citizens are systematically less capable of the sustained, informed, deliberative engagement that self-government requires.

What distinguishes a rupture moment from a merely difficult one is that the decisions made in it are load-bearing in a way that ordinary policy decisions are not. The institutional architecture built after 1945 has shaped the conditions of democratic life for eighty years. The institutional architecture that democratic allies build, or fail to build, in the decade ahead will shape those conditions for the decades that follow. This is not an argument for panic. It is an argument for clarity. The future is not written. Ukraine has demonstrated that democracies can resist authoritarian aggression with a tenacity that no intelligence assessment predicted. The European Parliament's 482-to-108 vote for deeper EU-Canada cooperation in March 2026 demonstrates that democratic institutions are still capable of choosing the West, deliberately, under pressure. The question this report asks is whether democratic allies will make those choices with the urgency the moment demands, or whether they will manage the rupture with the incrementalism that rupture moments have always, eventually, consumed.

This report does not traffic in false reassurance, because the moment does not permit it. What it offers instead is a clear-eyed account of the threat, a precise analysis of what democratic allies have already built, and a specific argument for what they must now build together. The chapters that follow begin with the fracturing of the existing architecture, because nothing useful can be constructed on a foundation that has not been honestly assessed.

Collective Defence, Collective Security, and the Rupture

General James Mattis, who commanded 200,000 troops across the Middle East and served as United States Secretary of Defense, argued "Nations with allies thrive, and

those without them wither and die."[5] That argument rested on an assumption of reliable alliance: that the largest member would remain committed to the values that gave the alliance its purpose. That assumption no longer holds unconditionally. The question this chapter addresses is not whether alliances matter. They do. The question is whether the architecture those alliances were designed to provide is the architecture cognitive warfare requires, and what democracies must build when the answer is no.

The distinction between collective defence and collective security is not terminological. It is structural. Collective defence, as NATO embodies it, is reactive by design. It requires an attack threshold, demands consensus on attribution, and is organised around state-centric threat actors whose actions can be named and legally characterised. It was never designed for cognitive warfare, which requires proactive, continuous action operating below any threshold NATO was built to recognise, and targeting the values-based foundations NATO was designed to protect. NATO can fulfil its collective defence mandate in every legal and institutional sense and still fail to protect the epistemic foundations on which democratic governance depends. These are not the same problem, and they do not share the same solution.

A Finnish conflict mediator with direct exposure to both sides offered the most precise formulation available from the primary research for this report: Russia and the current US administration agree on very little, but they agree the EU should be weakened and fragmented.

Disaggregating the US Paradox

The policy implications of the US paradox differ across its dimensions, and the response depends on keeping them analytically distinct. The temptation to treat "the US" as monolithic produces strategic paralysis. The disaggregation produces actionable options.

In December 2025, the State Department issued instructions directing consular officers to deny H-1B visas to anyone who had worked in fact-checking, content moderation, combatting disinformation, trust and safety, or online compliance, characterising this work as "censorship" of American speech.[6] By late December, Secretary Rubio had imposed named bans on five Europeans, including Thierry Breton, the former EU Commissioner who enforced the Digital Services Act against Musk's X, and the leaders of organisations

focused on countering digital hate and disinformation, including HateAid Germany.[7] A legal challenge was filed in March 2026. The United States is using immigration law as a weapon against the cognitive defence workforce of its own Allies. The deeper purpose, as legal scholars have documented, is threefold: to perpetuate the conservative censorship victimhood narrative that disables content moderation; to shield European far-right parties from DSA transparency requirements that would expose their use of disinformation; and to remove EU regulatory obstacles to American platform dominance.[8]

The current administration's rejection of democracy and rule of law as organising values is now quantified. Three independent assessments published in March 2026 document the scale of democratic backsliding. V-Dem dropped the United States from 20th to 51st in its global democracy rankings, in a process its researchers characterised as the most rapid democratic backsliding recorded in the modern era; Freedom House issued a concurrent downgrade; and, Bright Line Watch, drawing on surveys of more than 500 US scholars, concluded that the US system now falls nearly midway between liberal democracy and dictatorship. Gary Sick, who served on the National Security Council under three presidents and is the most senior living US official with direct experience of the Iranian file, characterised the current administration's conduct in an April 2026 interview as that of a rogue nation, one that is flouting the laws of war, humanitarian procedure, and the institutional commitments on which American credibility rests.[9]

Two dimensions of the US relationship remain worth maintaining despite the above. At the working level, intelligence community professionals, career officials, Congressional actors committed to alliance relationships, and state and sub-national connections represent institutional ties with value independent of the current political leadership. US-based platforms require a different approach entirely: regulatory accountability through the DSA and DMA framework, treating these actors as subjects of democratic governance rather than partners in democratic defence. The visa bans targeting DSA enforcers confirm the leverage is real: actors under genuine regulatory pressure do not ban the regulators unless the regulation is working. When the EU fined Musk’s X in December 2025 for failing to meet basic Digital Services Act transparency requirements, Musk responded by calling for the abolition of the EU itself.[10]

Structural US polarisation creates a further problem that outlasts any single administration. Policy continuity on the core questions of democratic governance and collective defence has become unreliable regardless of which party governs. Allies who assume a reliable return to the pre-2024 posture are planning against what the evidence supports. The administration formalised this values position institutionally on 7 January 2026, withdrawing from 66 international organisations including the International Institute for Democracy and Electoral Assistance and the UN Democracy Fund.[11] The hedging strategy this requires is not improvised. Middle power hedging in a fragmenting order follows identifiable logic: maintain working relationships at the sub-political level, build independent capacity in domains where dependency creates vulnerability, use regulatory and institutional leverage where it exists, preserve optionality, and conduct quiet contingency planning for scenarios previously treated as hypothetical.[12]

The Endogenous Threat: Cognitive Stress from Within

A senior NATO source consulted for this report named the threat they found most alarming not as direct Russian operations but as internal alliance polarisation, extreme political division, and the prospect of allied-on-allied cognitive interference. Adversaries did not create the fires burning inside democratic alliances. They have poured accelerant on fires that were already smoldering.

Hungary represents the systemic form of the endogenous threat. Whether it is captured media, surveillance tools deployed against journalists and EU officials, or systematic obstruction of collective EU and NATO action, Viktor Orbán built a governance model that uses the institutions of democratic alliance from the inside to serve interests antithetical to those institutions. The pattern is not idiosyncratic to Hungary. Systematic research on democratic backsliders in international institutions documents how such actors engage in selective contestation, continuing to endorse the liberal international order broadly while systematically opposing its more intrusive mechanisms, aligning with autocratic actors on norm-sensitive decisions, and using established membership to shield domestic governance from external scrutiny, while retaining the legitimacy and security guarantees that membership confers.[13] The results for Hungary's own citizens are measurable. After sixteen years in office, Orbán's governance record sits at the bottom of the European Union on the metrics that matter to ordinary citizens. Hungary ranks worst in the bloc on

corruption indicators, near the bottom on standards of living, and last on most independent press freedom and rule of law assessments. Fidesz captured higher education, the senior civil service, and the judiciary, while an allied network of oligarchs took ownership of most domestic print and broadcast media and a substantial share of the economy.[14] The economy expanded just 0.4 percent in 2025, with industrial production in sustained multi-year decline.[15] Faced with a domestic record he could not defend, Orbán turned to what Anne Applebaum, writing in The Atlantic in March 2026, called the world's first post-reality campaign. "Pay attention," Applebaum writes, "because this may be the future of electoral politics: Multiple politicians from several countries are shoveling propaganda at an electorate in order to build terror of an enemy that doesn't exist at all."[16] Backed by Russian propagandists, the European far right, and the Trump administration, Fidesz flooded Hungary's information environment with AI-generated deepfakes portraying an imminent Ukrainian invasion: an entirely false threat, with the Ukrainians rather occupied defending their own territory.[17] The post-reality formulation Applebaum identifies is the electoral expression of the liar's dividend developed in Chapter 3. Fidesz did not need Hungarian voters to believe the deepfakes. It needed them to be unable to authenticate what was real, which is the condition under which a fabricated threat can displace the entire question of governing record. The United States responded to this record with systematic embrace. Trump hosted Orbán at the White House in November 2025, calling him a "great leader" and granting Hungary a full exemption from US sanctions on Russian energy. Trump endorsed Orbán in Hungary's April 2026 elections, and Vice President JD Vance publicly campaigned for Orbán just prior to the election. Despite these efforts, Hungarians voted the Orbán government out of office on April 12, 2026. Despite this rebuke of these methods in Hungary, it has not slowed down efforts elsewhere.

The US administration has publicly attacked Germany's domestic intelligence service for designating the far-right Alternative for Germany as an extremist organisation, a designation reached after a three-year review, with Secretary Rubio calling it "tyranny in disguise."[18] The pattern is not incidental. The NSS's explicit goal of fostering resistance to the EU's "current trajectory" from within finds its clearest operational expression in

Washington's systematic embrace of the actors most actively pursuing that objective inside the Alliance.

The United States dimension of the endogenous threat has moved beyond the institutional into the operational. The Wall Street Journal reported that Putin, studying Trump's inner circle through Russian intelligence, effectively selected his own preferred American negotiator. Steve Witkoff was chosen because he would come without CIA officers, diplomats, or a translator, and because the alternative, Keith Kellogg, had a daughter working with Ukraine, which Moscow viewed as a disqualifying conflict.[19] Witkoff has made multiple trips to Moscow and none to Kyiv.

Alberta separatism was named independently by two primary research sources as a specifically identified Russian cognitive warfare target: white, wealthy, oil-driven, and conservative, with a receptive ideological community for amplification from multiple directions simultaneously. What converted this from analytical observation to current operational concern was US Treasury Secretary Scott Bessent publicly stoking Alberta separatism, with the Financial Times reporting that US State Department officials had met the Alberta Prosperity Project on three separate occasions, during the research period for this report. When a senior official of an allied government uses the public platform of that office to amplify a separatist narrative that Russia has independently targeted, the endogenous threat and the external threat have become functionally indistinguishable. The analytical convergence runs deeper than coincidence. The Defense Analyses and Research Corporation, a US think tank that has demonstrated a pattern of publishing positions that subsequently emerged as administration policy, including the revival of letters of marque and the Trump Corollary to the Monroe Doctrine, has published a strategy for Canadian fragmentation that recommends US support for provincial secessionist movements, exploitation of Indigenous reconciliation processes to demoralise Canadian elites, and targeting of regional cleavages to achieve dismemberment rather than annexation. DARC's reasoning mirrors Russian strategic doctrine almost exactly: overt annexation would unify Canada against the US, whereas fragmentation achieves the strategic objective without triggering that response. When Russian and American strategic doctrine arrive at the same recommendation through the same analytical logic, the compound nature of Canada's cognitive defence challenge

becomes precise. The implication for Canadian defence architecture has been named with unusual precision by Patrick Lennox, a former senior intelligence officer with the RCMP. Writing in *The Walrus* in April 2026, Lennox argued that Canada's entire defence concept has been built on a premise of who the good guys are, and that interoperability, the capacity for the Canadian and American militaries to operate seamlessly across air, sea, and land domains, assumes a benevolent American hegemon. Those guardrails, in his assessment, are disappearing. The observation carries specific analytical weight that general commentary on democratic backsliding does not: it comes from a practitioner who has spent decades working inside the security architecture whose foundational assumption is now in question. Canada did not choose interoperability as a strategic preference. It inherited it as a structural condition, and built every procurement decision, command arrangement, and intelligence relationship on it. Reassessing that architecture is not a theoretical exercise. It is the most consequential strategic decision Canada has faced since the Cold War, and it must begin before the guardrails are entirely gone.[20]

The distinction between an administration and a democratic ecosystem matters for what follows. Experts across the ideological spectrum, including Brookings scholars Norman Eisen and Jonathan Katz, characterise the United States at the federal level as a backsliding democracy, while identifying civil society, state institutions, and the broader democratic ecosystem as the resilient layer that allied investment should target.[21] The United States military and policy apparatus on cognitive defence remains active and capable: American practitioners are among the architects of NATO’s cognitive warfare concept, the Senate Armed Services Committee is actively examining cognitive defence requirements, and American researchers and civil society organisations working on democratic resilience represent some of the field’s most advanced capacity. The administration’s political choices have not erased that ecosystem. They have placed it under pressure.

The operational consequence is already materialising. Ukrainian civil society counter-disinformation organisations, some of which have operated continuously since 2014 and built the most extensive practitioner-developed methodology in the democratic world, are scaling down or closing due to US funding withdrawal. Through the author’s field research, the report identified organisations that have operated for a decade now doing

nothing because capacity is gone. The US government was responsible for approximately 90 per cent of the $3 billion annual global democracy support budget, including $268 million specifically for counter-disinformation and press freedom programming. That funding has been withdrawn. The organisations being hollowed out are the operational civil society layer on which government counter-FIMI architecture depends. When they close, the institutional memory, the methodology, the practitioner networks, and the early warning capacity close with them.

The coalition's response to US political unreliability should include active investment in that American democratic ecosystem: sustaining research partnerships, funding civil society organisations working on democratic resilience and information environment integrity, and maintaining the working-level relationships that political disruption at the top has not severed. The long game is not to replace the United States in the liberal order. It is to hold the space, and invest in the Americans holding it from within, until American democratic politics reconstitutes itself.

What the Fracturing Alliance Is Destroying

A Nanos Research polling commissioned by the *Globe and Mail*, fielded January 31 to February 4, 2026, found that 76.1 percent of Canadians disagree or somewhat disagree that the United States is a trustworthy ally, with 49.2 percent disagreeing outright. This was enough to lead pollster Nik Nanos to judge them to be "probably the worst numbers in any era where polling was done".[22] Opinion polling in the United Kingdom in January 2026 found that 32 percent of Britons now regard the United States as a threat, against 42 percent who still regard it as an ally.[23] These are not temporary sentiment shifts. They represent a structural reorientation in allied publics' perception of the actor on which their defence architecture has been primarily designed to depend.

The USAID withdrawal and the defunding of Voice of America and Radio Free Europe/Radio Liberty have eliminated the primary US-funded infrastructure for independent media in contested information environments. France is attempting to fill the resulting void in Africa and the Middle East through AFP partnerships with local outlets, but does not have an equivalent budget.[24] The information vacuums created by US disengagement are being filled by actors who are positioned, resourced, and motivated

to fill them. The clearest assessment of what this means for the rules-based order came not from European critics but from within the American defence establishment itself. Chuck Hagel, Republican, and Leon Panetta, Democrat, both former Secretaries of Defense, published a joint essay in the *New York Times* concluding that the war in Iran has further undermined the credibility of the United States to maintain the rules-based international order that we helped establish after World War II, and characterising the conflict as a terrible miscalculation launched without informing Congress or Allies, by a president acting alone without a strategy.[25]

The 1956 Pearson report, produced by Lester B. Pearson, Gaetano Martino, and Halvard Lange as NATO's "Three Wise Men," established that NATO's political and values dimension is a constitutive element of the alliance. Pearson argued that the alliance existed to create conditions under which democratic governance could sustain itself. The current US administration has effectively abandoned what Pearson argued in 1956 was the point. What the fracturing alliance is destroying is the assumption that the largest member shares the foundational commitment that made the alliance worth maintaining. That the reconstitution is already underway at the level of heads of government was made explicit by French President Emmanuel Macron in Seoul on 3 April 2026. Speaking at Yonsei University, Macron called explicitly for a coalition of medium-sized powers, naming Australia, Brazil, Canada, and India alongside South Korea and Japan, to cooperate on artificial intelligence, space, nuclear energy, defence, and security. His formulation was precise: our objective is not to be the vassals of two hegemonic powers, not to depend on the dominance of China and not to be too exposed to the unpredictability of the United States.[26]

Building for Resilience: What the Coalition Architecture Requires

The democratic coalition is not passively fracturing. At the parliamentary level, it is actively reconstituting around demonstrated values. The European Parliament's Recommendation on Enhanced EU-Canada Cooperation, adopted on 11 March 2026 by 482 votes in favour to 108 against, is not a procedural gesture. Its rapporteur, German Social Democrat MEP Tobias Cremer, described Canada as perhaps the most European country outside Europe, and called for the relationship to be elevated "at a moment of global rupture, marked by Russian aggression and increasingly erratic rhetoric from

Washington."[27] The resolution explicitly names Russia's war against Ukraine, hybrid attacks, foreign interference, AI, and cybersecurity as the shared threat landscape requiring deeper cooperation. This is institutional evidence of reconstitution, not diplomatic aspiration. Ikenberry has argued that such coalitions of democratic states represent the most viable mechanism for upholding liberal international order when the hegemon defects, operating as exclusive groupings within the wider international system rather than replacements for it.[28] A coalition organising around demonstrated democratic commitment, and explicitly conditioning deeper integration on it, is the architecture this report recommends. There is a genuine tension here that should be named directly.[29] A procedurally inclusive rules-based order admits all comers regardless of governance model; a values-based democratic defence coalition admits only those whose demonstrated commitment to democratic governance warrants the trust that sensitive cooperation requires. These are not the same architecture, and pretending they can be reconciled without cost produces neither. This report takes the position that cognitive defence cooperation requires the selective architecture, and that the cost of that selectivity, the friction it creates with inclusive multilateralism, is preferable to the cost of admitting actors whose interests are structurally antithetical to the mission.

The Hybrid Centre of Excellence in Helsinki, from which the United States has withdrawn, has become a more viable venue for like-minded cooperation precisely because that withdrawal removes a source of friction for partners who wish to cooperate on sensitive information without simultaneously managing American politics simultaneously.[30] Norway's research community has identified cognitive defence as the domain where like-minded democratic partners, including Canada, the United Kingdom, and Norway, can cooperate outside the NATO framework without the US dependency problem that affects conventional military deterrence.[31] Canada's diplomatic presence across the Global South, including Africa, Asia, and Latin America, extends the coalition's reach beyond the European perimeter. Canada's specific comparative advantage in this architecture is convening capacity: its relationships across the Global South, its francophone presence in Africa, and its Indigenous diplomacy in Arctic and Pacific contexts give the corridor reach that EU-only formats cannot replicate.[32]

Admiral Bauer's formulation sharpens the analytical precision: what is being lost is not the institutional architecture of NATO, which is more durable than any single administration[33], but the assumption that its largest member shares the values that gave the alliance its purpose. These are different losses requiring different responses.

Alliances have historically coalesced when genuinely tested, and they look weak until they are. Macron declared NATO "brain dead" in 2019. The withdrawal from Kabul in 2021 fractured allied trust. When Russia launched its full-scale invasion of Ukraine in February 2022, few predicted the response that followed: NATO Allies moved with a unity not seen in decades, Ukraine was invited as a guest of honour to Leaders, Foreign Affairs, and Defence Ministers' Summits, and Putin's calculation that the war would break the Alliance proved to be among the most consequential strategic miscalculations of the era. More recently, when the United States applied concerted pressure over Danish sovereignty in Greenland through a cumulative 2025 sequence of covert influence activity, intelligence escalation, and direct public demands, Denmark responded through the *rigsfællesskab* and through NATO. The Arctic Endurance exercise in January 2026 marked the inflection point at which escalation risk was contained, and the mechanism of deterrence was diplomatic: the prospect of fracturing the American relationship with Germany, France, and the United Kingdom, which issued statements of solidarity with Denmark that were unprecedented in their directness. Chapter 12 develops the case. Democratic alliances galvanise under genuine pressure. The design challenge is to build the architecture before the galvanising moment arrives, not after it. Chapter 13 proposes the specific instruments.

Endnotes

1 A. Fawaz Gerges, interview with Leslie Vinjamuri, “Is the Middle East Heading Toward a Much Bigger War?” Deep Dish, Chicago Council on Global Affairs, April 2026.

2 Adrian Wooldridge, "Those Who Believe in Liberalism Must Now Fight for It," The Spectator, 14 March 2026; and Wooldridge, Centrists of the World Unite!: The Lost Genius of Liberalism (Allen Lane, 2026).

3 Alexander Stubb, "The Triangle of Power," *Foreign Affairs* (2025); Stubb, interview, *Foreign Affairs* podcast, February 2026.

4 John J. Mearsheimer, The Tragedy of Great Power Politics, updated edition (W. W. Norton, 2014); and Mearsheimer, "Bound to Fail: The Rise and Fall of the Liberal International Order," International Security 43, no. 4 (Spring 2019): 7 to 50.

5 James Mattis and Bing West, *Call Sign Chaos: Learning to Lead* (Random House, 2019).

6 Shannon Bond, "State Department to deny visas to fact checkers and others, citing 'censorship'," NPR, 4 December 2025, reported from State Department internal memo also obtained by Reuters.

7 "U.S. bars Europeans it says pressured tech firms to censor American viewpoints online," NPR, 24 December 2025.

8 David Kaye, "The Trump Lie About Europe and Why it Matters," Tech Policy Press, 9 January 2026, techpolicy.press.

9 V-Dem Institute, *Democracy Report 2026*, University of Gothenburg, March 2026. Freedom House, *Freedom in the World 2026*, March 2026. Bright Line Watch, survey of more than 500 US scholars, March 2026, reported in NPR, 20 March 2026.

10 "Elon Musk X EU fine," *Washington Post*, 5 December 2025. Musk called for the abolition of the EU following the fine.

11 Presidential Memorandum, "Withdrawing the United States from International Organizations, Conventions, and Treaties that Are Contrary to the Interests of the United States," 7 January 2026, whitehouse.gov.

12 Field research synthesis on middle power hedging strategy, 2025 to 2026. For published treatments, see Brendan Taylor, "Hedging in the Indo-Pacific," Survival 62, no. 4 (2020): 89 to 108; and Cheng-Chwee Kuik, "Getting Hedging Right: A Small-State Perspective," China International Strategy Review 3 (2021): 300 to 315.

13 For the typology of selective contestation by democratic backsliders within international institutions, see Anna Meyerrose, "The Unintended Consequences of Democracy Promotion: International Organizations and Democratic Backsliding," Comparative Political Studies 53, no. 10 to 11 (2020): 1547 to 1581; and Tom Ginsburg, "Authoritarian International Law?," American Journal of International Law 114, no. 2 (2020): 221 to 260.

14 Anne Applebaum, "The First Post-Reality Political Campaign," The Atlantic, 27 March 2026.

15 Hungarian Central Statistical Office (KSH), GDP data for 2025, released 3 March 2026, ksh.hu; on industrial production decline, see KSH industrial production series, 2024 to 2025. For analysis, see European Commission, Economic Forecast for Hungary (November 2025), economy-finance.ec.europa.eu.

16 Anne Applebaum, "The First Post-Reality Political Campaign," The Atlantic, 27 March 2026.

17 Ibid.

18 Anton Shekhovtsov, "From Moscow to MAGA: AfD's Markus Frohnmaier and the Transnational Far-Right Convergence," The Insider, 15 December 2025.

19 "Putin effectively chose Witkoff as US negotiator with Russia," Wall Street Journal, December 2025.

20 Patrick Lennox, "The US Torpedoed an Unarmed Ship. Who Are the Good Guys Again?" The Walrus, 6 April 2026.

21 Norman Eisen and Jonathan Katz, Brookings Institution analysis on US democratic backsliding, 2025 to 2026. See, for example, Norman Eisen, "The Trump Administration and Democratic Backsliding: A Mid-Term Assessment," Brookings, 2026.

22 "Canada's great American breakup: Most now see U.S. as a risk, not an ally, poll finds," Globe and Mail, 23 February 2026.

23 Opinion polling, January 2026, cited in field research, UK Source 1, interview conducted 2026.

24 Field research, France Source 1, interview conducted 2026.

25 Chuck Hagel and Leon Panetta, op-ed on the Iran war, The New York Times, 1 April 2026.

26 President Emmanuel Macron, remarks to students at Yonsei University, Seoul, 3 April 2026.

27 European Parliament, Recommendation A10-0035/2026, 11 March 2026, Rapporteur Tobias Cremer, S&D, Germany, europarl.europa.eu.

28 G. John Ikenberry, "Why American Power Endures: The U.S.-Led Order Isn't in Decline," Foreign Affairs 101, no. 6 (November to December 2022): 56 to 73; and Ikenberry, A World Safe for Democracy: Liberal Internationalism and the Crises of Global Order (Yale University Press, 2020).

29 On the analytical tension between inclusive multilateralism and values-based selective coalitions, see Ikenberry, A World Safe for Democracy; and Robert Kagan, The Jungle Grows Back: America and Our Imperiled World (Knopf, 2018).

30 Field research, UK Source 1, interview conducted 2026.

31 Field research, Norway Source 7, interview conducted 2026.

32 Field research synthesis on Canadian convening capacity, 2025 to 2026.

33 Admiral Rob Bauer, interview with Kasper Kildegaard, Børsen, 27 November 2025.

Chapter 12: The Idea Worth Defending

The idea of ‘The West’ is not an inheritance. It is a choice made repeatedly, under pressure, in the face of an adversary who understands that if the choice can be made to seem futile, or naïve, or simply exhausting, it will eventually stop being made at all.

Georgios Varouxakis, in his comprehensive intellectual history of the concept, traces “the West” not to the philosophical ideas of antiquity but to the 1840s, when the French philosopher Auguste Comte gave the idea its first coherent political form: a proposed supranational community defined not by blood or religion but by shared institutions, shared historical experience, and shared aspirations for what a society could be. Comte needed a word beyond what “Europe” could supply, because Europe by then included Russia, and Russia was not, in his conception, part of this project. The West was born as a political idea forged in deliberate distinction from an adversary to the east. It has never been anything else.[1]

Tony Judt's Postwar, the standard history of Europe after 1945, develops the same point through the institutional record rather than the intellectual history. The post-war European project was not the inheritance of a pre-existing civilisation but a deliberate political construction undertaken by states whose recent experience had taught them what the absence of that construction produced. The institutions that emerged, the European Coal and Steel Community, the Council of Europe, the European Convention on Human Rights, NATO itself, were built by people who understood, viscerally, that the West was a choice that had to be made institutionally because it had so recently been unmade. The two readings, Varouxakis on the intellectual genealogy and Judt on the institutional construction, converge on the same conclusion. The West is not a place. It is a choice, made repeatedly, by people who understand what its absence costs.[2]

The contest Varouxakis traces is now being fought through a different vocabulary. Cognitive warfare is the contemporary form of the contest he traces from Comte, conducted with tools the nineteenth century could not have imagined but pursuing the same strategic objective: the erosion of the institutional, civic, and meaning-making structures through which a society knows itself. Korobeynikov, Davydiuk, and Mokhor argue that cognitive warfare differs ontologically from previous forms of contestation

because it is more invisibile, which means the target experiences induced changes as endogenous evolution rather than as external attack, and because it targets the structures through which knowledge is constructed.[3] The question of what is worth defending is therefore the operational precondition for cognitive defence. If cognitive warfare is the contest of narratives that the threat assessments we believe it to be, this chapter asks what narrative is being contested, and why it is worth defending.

The Signs the West Missed

The signs were there. They were there in Kyiv's Independence Square during the Orange Revolution of 2004, when Ukrainians took to the streets holding anti-corruption signs and EU flags, choosing, in the most tangible way available to them, to belong to the Western project rather than the Russian one. As Anne Applebaum has argued for more than two decades, Putin understood those demonstrations not as a geopolitical provocation but as a personal and civilisational threat. If people could take to the streets in Kyiv, they might do so in Moscow too. The angry intervention of the Ukrainian public against a clumsy attempt to steal a presidential election in favour of a pro-Russian candidate profoundly unnerved the Kremlin. They labelled what had happened a "colour revolution," a phrase designed to delegitimise civic mobilisation by attributing it to foreign interference rather than genuine popular will.[4]

The Ukrainians wrote it again, in larger letters, during the Maidan uprising of 2013-2014. When then-Ukrainian President Viktor Yanukovych, under pressure from Russia, abandoned Ukraine's Association Agreement with the European Union, the population responded not with resignation but with occupation. The EU flags flying over the Maidan were a declaration of the Ukrainian people's desire to belong to an order defined by the rule of law and democratic accountability. The flags remain flying over the same square even though Ukraine is not a member of the European Union and does not yet have the legal right to call itself part of that project. The flags fly anyway, for what it represents.

Despite representing these values, the West was not able to recognise their expression clearly in Ukraine. The signal was unmistakeable and still they chose comfort, accommodation and process. Keeping the peace was the same as keeping the truth; a managed, harmonious order was worth more than an honest one. They chose

convenience because reality was going to cost too high a price. The Ukrainian people did not have a choice of whether to pay that price. The question this report asks is whether these countries now see reality for which it is, and are willing to pay the price required for freedom.

The West is More Than Democracy

Neither geography nor the act of simply holding elections are what define the West. Japan and South Korea, caught between an existential threat from North Korea, direct strategic competition with China, and the enduring gravitational pull of a security dependence on Washington, are liberal democracies with independent judiciaries, free press traditions, competitive elections, and rule of law frameworks. They are surrounded by adversarial or unpredictable powers that make the cost of any misstep existential rather than merely consequential. Both have provided material support to Ukraine. That choice was not made from interest alone. It was made from recognition: that what is at stake in Ukraine is the same principle that underwrites their own existence as free societies. Countries that make that recognition belong to this community regardless of where they sit on a map.

Australia and New Zealand complete this picture. Their membership in Five Eyes, AUKUS, and the AP4 partnership with NATO reflects a long-settled institutional recognition that the values at stake in the Euro-Atlantic contest are not geographically bounded. They face a distinct threat geometry. China is a proximate rather than a distant adversary, and the cost calculations of strategic alignment are correspondingly more complex. But the cognitive warfare techniques deployed against them, the information operations targeting diaspora communities, the platform architecture that adversaries exploit, and the erosion of the epistemic foundations on which democratic participation depends, are the same techniques deployed against every democracy in this report. Democratic resilience is not a European resource. It is a common-pool resource of all open societies, and its defence requires that the Euro-Atlantic and Indo-Pacific democratic communities treat each other as partners in a shared project rather than parallel but separate ones. The AP4 partnership with NATO is the institutional expression of that recognition and it should continue.

Canada’s Role in the West

Canada’s place in this community also goes beyond geography and voting. It is a matter of history, culture, and repeated deliberate choice. In 1914, Canada answered the call of empire and fought with distinction on the Western Front. By 1939, Canada was a sovereign country with autonomy over its foreign and defence policy. Prime Minister Mackenzie King waited seven days after Britain’s declaration of war before bringing Canada’s own before its Parliament, precisely to demonstrate its independence. A country that had no binding obligation to fight a war on another continent chose to do so from the very beginning, alongside allies whose cause it recognised as its own. Canada was among the founding members of NATO in 1949, one of the architects of the collective defence framework that has underwritten the security of the democratic world for seventy-five years. That history of choosing the West is a part of its collective DNA.

Canada’s natural home, in an era of great-power competition, is with Europe. As a free, liberal democracy it must grow closer to Europe, which has become the democratic centre of gravity during a time when the United States no longer reliably occupies that position. Despite whatever direction Canadian economic interests take it, Canada cannot escape the belief system that binds it to European democratic traditions.

This is the same recognition that underpinned the creation of NATO’s political dimension. In 1956, NATO Secretary General Lord Ismay tasked three foreign ministers, Lester B. Pearson of Canada, Gaetano Martino of Italy, and Halvard Lange of Norway, to examine what was then described as the flagging political and moral cohesion of the Alliance. Their report argued that NATO was also a community of values, and that its survival depended on its members treating one another as partners in a shared democratic project. The report's central conclusion was unambiguous: "an Atlantic Community which is divided politically cannot for long remain united economically and militarily." Pearson was the animating intellectual force behind that finding, and the Three Wise Men's articulation of it set the doctrinal frame within which the Alliance's political dimension was subsequently developed. The report further held that the Alliance's members were bound by "a sense of common destiny", and that the political and economic dimensions of cooperation were not supplementary to collective defence but constitutive of it. Collective defence, on this reading, is ultimately a community of shared values, and shared values are the binding

obligation that no treaty can manufacture and no tariff can dissolve.[5] When Norwegian Prime Minister Jonas Gahr Støre hosted Canadian Prime Minister Carney, alongside all five Nordic leaders in Oslo in January 2026, and Swedish Prime Minister Ulf Kristersson described Canada as “the most Nordic of non-Nordic countries”, this was recognition of a genuine kinship.[6] Approximately two-thirds of Canada’s population traces its heritage to Europe. Canada’s legal traditions derive from British common law and French civil law. Its parliamentary institutions are modelled on Westminster. Its founding conception of rights and governance emerged from a European tradition of human dignity and rule of law. The connection is demographic, institutional, and historical. Canada must now make it strategic.

Canada cannot compete alone with the weight of the United States, China, or Russia. Neither can the United Kingdom, Germany, France, or the Netherlands. But Europe can compete if it is willing to make the institutional and strategic choices that competition requires. This is where Veronica Anghel and Erik Jones of the European University Institute offer a clarifying frame. Their 2025 analysis of EU enlargement argues that the European Union has evolved from an exclusive club into a system of common-pool resources: goods that are at once rivalrous, because the capacity to defend them is finite, and non-excludable, because cognitive attacks on one democracy create vulnerabilities in all of them. The only way to preserve such resources is through governance structures that impose shared responsibility on all who have access. Widening and deepening, in their analysis, are part of the same process. Democratic resilience is exactly this kind of resource. It degrades under sustained attack unless collectively managed, and it cannot be defended by any single country acting alone.[7]

The Estonian experience provides the operational illustration of why this resource cannot be defended in isolation. When Russia launched a sustained cyber and information operation against Estonia in 2007, following the relocation of a Soviet-era war memorial in Tallinn, the attack was directed at a single democracy but the lessons were immediately recognised as collective. Estonia's response was not to defend its institutions alone but to build, deliberately, the architecture that became the NATO Cooperative Cyber Defence Centre of Excellence, established in Tallinn in 2008 and now the Alliance's principal institutional home for cyber and cognitive defence research. The Estonian institutional

response to a national attack became, by design, a common-pool resource for the democratic Alliance as a whole. Finland's post-2014 institutional reorganisation followed the same logic at the cognitive layer: the recognition that Russian information operations against Finnish democracy were not a Finnish problem to be solved domestically but the operational expression of a threat that every democratic society would face, and that the institutional response had to be built in a form that could be shared. The Finnish comprehensive security model and the Nordic-Baltic cooperation architecture that grew from it are the institutional record of that recognition. Democratic resilience is built by individual states. It is sustained only collectively.[8]

The Deliberate European Project

The EU's institutional complexity, often cited as a liability, is also a structural asset in the cognitive domain. Redundancy across 27-member states means that no single point of institutional failure disables the whole. The EU commands regulatory reach through the Digital Services Act and the AI Act, a convening capacity across member states and strategic partners, and an institutional knowledge base through the East StratCom Task Force and its network of excellence centres that no bilateral partnership can replicate. Coordinating capacity across languages, media environments, and legal traditions builds the kind of layered resilience that a sophisticated adversary finds most difficult to systematically attack.

Henry Kissinger is said to have asked "if I want to call Europe, who do I call?"[9] The question was meant to expose a weakness. It remains unanswered in any clean institutional sense, and the absence of a clear answer is itself a cognitive vulnerability: an alliance with no single authoritative voice is easier to fracture and confuse. But the question also points to the only institution that has the regulatory architecture, the economic weight, and the geographic span to serve as the anchor of a renewed democratic order. Brussels is a choice born of arithmetic. The argument of this manuscript is that the EU is the only institution currently capable of generating and sustaining the common-pool resource of democratic resilience at the scale that the current threat environment requires, for the countries that share the political identity to make that project meaningful.

The light of freedom that once burned brightest in Washington has dimmed. It cannot be relied upon to illuminate the path. The question now is whether Brussels, in partnership with Kyiv and the democratic capitals of the Euro-Atlantic community, is willing to carry the light forward.

Endnotes

1 Georgios Varouxakis, The West: The History of an Idea (Princeton University Press, 2025).

2 Tony Judt, Postwar: A History of Europe Since 1945 (Penguin Press, 2005)

3 Korobeynikov, Davydiuk, and Mokhor

4 Anne Applebaum, “The New Propaganda War,” *The Atlantic*, 4 June 2024.

5 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Security 4, no. 2 (2011): 49-60, & NATO Cooperative Cyber Defence Centre of Excellence institutional history at ccdcoe.org. & Finnish Government, *Security Strategy for Society*, 2017

6 Nordic-Canada Summit, Oslo, January 2026. Remark by Swedish Prime Minister Ulf Kristersson.

7 Veronica Anghel and Erik Jones, “Club to Commons: Enlargement, Reform and Sustainability in European Integration, Elements”, *Economics of European Integration* (Cambridge University Press, 2025), doi.org/10.1017/9781009499194.

8 Committee of Three on Non-Military Cooperation in NATO, Report by the Committee of Three on Non-Military Co-operation in NATO (Lester B. Pearson, Gaetano Martino, Halvard Lange), North Atlantic Council, 13 December 1956

9 Walter Isaacson, Kissinger: A Biography (Simon & Schuster, 1992), 204–205. The remark has been disputed by some historians as apocryphal but remains analytically useful.

Chapter 13: The Canada-Germany-EU Corridor

The Scaffolding Is Already There

The Canada-Germany-EU corridor is not a diplomatic aspiration. The institutional scaffolding already exists and includes: a Security and Defence Partnership, a Digital Partnership Council, a Canada-Germany Digital Alliance, CETA modernisation, and a European Parliament Recommendation on Enhanced EU-Canada Cooperation adopted in March 2026. In July 2026 the Prime Minister of Canada and the Chancellor of Germany announced the launch of negotiations towards a Canada-Germany Strategic Partnership Agreement, an explicit bilateral framework spanning security and defence, technology, artificial intelligence and space, supply chains and critical minerals, energy, and investment, which the two leaders intend to finalise before the end of 2026.[1] What does not exist is a cognitive warfare workstream. Anders Fogh Rasmussen, in an interview with *Politico*, named the architectural moment directly: European leadership of the democratic alliance is the strategic posture the moment requires.[2] An EEAS source captured the same condition from inside: the room is set up, everything is ready for a very good working environment, but it is as if we are inviting each other to go first.

The Institutional Scaffolding

The Canada-EU Security and Defence Partnership, signed in June 2025, covers cyber, hybrid threats, and emerging disruptive technologies, naming precisely the domains in which cognitive defence cooperation is most urgently needed. Its architecture was designed to accommodate new workstreams rather than requiring new instruments. The EU's High Representative confirmed in the EEAS Fourth FIMI Threat Report that countering foreign information manipulation and interference is now explicitly part of the EU's Security and Defence Partnerships with several countries.[3] The Canada-EU Digital Partnership Council, meeting for the first time in December 2025, addressed AI governance, platform accountability, and information environment integrity.[4] The Canada-Germany Digital Alliance, signed in December 2025 with a Joint Declaration of Intent on AI in February 2026, is the bilateral engine within the broader Canada-EU framework, expandable without requiring new political authorisation.

The Operational Gap

The gap is at the working level, and it is a choice rather than a structural constraint. The comparison with the United Kingdom makes the gap apparent. The EEAS counter-FIMI division meets with UK embassy staff at minimum monthly, uses UK embassy premises for confidential working sessions, has achieved near-methodological interoperability, and co-organises the FIMI Forum with the Foreign, Commonwealth and Development Office. None of this has happened with Canada. The EEAS source was direct: Canada has not yet reached Norway-level operational cooperation, let alone UK-level. Canada's trajectory is toward the UK level. This gap is a choice. Korobeynikov, Davydiuk, and Mokhor's framework names the broader threat environment: parasitic substructures, closed and functionally stable formations embedded within the multilayered architecture of pluralistic democracies, including foreign-controlled proxy networks operating as systems within the system.[5] Canada has a dedicated Rapid Response Mechanism, a substantial team within Global Affairs Canada, and political will at the strategic level. What is missing is an instruction from senior leadership to press ahead on operationalising the Security and Defence Partnership and begin regular structured engagement.

The instrument for that structured engagement is the Embassy of Canada to the European Union in Brussels. Canada can structure working-level engagement between the Embassy and the EEAS counter-FIMI policy and partnerships division on the UK model: monthly ideally, at minimum quarterly. The EEAS-UK working-level cadence is the operational benchmark the earlier comparison in this section names, and the Embassy of Canada is the institutional instrument available to match it. A regular Embassy-EEAS meeting cadence and a Global Affairs Canada secondment into the EEAS counter-FIMI unit, set out below, are distinct instruments. Both are necessary. The secondment, treated below, places a Canadian official inside the EU institutional unit and is the higher-bandwidth instrument by a substantial margin. The regular meeting cadence is the relationship-building and collaboration instrument that the secondment, however valuable, does not replace, since institutional relationships at the team level are built through sustained working-level contact between teams rather than through any single individual placement. The Embassy is the operational instrument the corridor needs in

Brussels. It does not require a new institutional creation. It requires adequate resource allocation.

The Bilateral Anchor

The Canada-Germany Digital Alliance is the best instrument to lead. It is bilateral, already operational, directly covers the relevant domains, and is expandable. Sophia Besch's concept of Germany as *Anlehnungsmacht*, a power to lean on, indispensable by virtue of size and economic weight but structurally preferring alignment over unilateral action, is precisely the partnership model the corridor requires.[6] Massie and Tallová's comparative analysis of Western military support to Ukraine ranks Germany alongside France in the category of states whose strategic pivots following February 2022 are reflected in actual contribution, with Germany more than quadrupling its relative military support between the first and second periods of the war.[7] Canada, by contrast, a typical token contributor in the first period. The Carney government's achievement of the NATO 2 per cent GDP target in 2025-26 marks a genuine inflection.[8] Germany has demonstrated sustained commitment; Canada is now making the investments that make future contribution credible.

The Canada-Germany Sovereign Technology Alliance, signed at the Munich Security Conference on 14 February 2026, gives the bilateral its operational anchor at the policy level. The Alliance accompanies a Joint Declaration of Intent on Artificial Intelligence between Innovation, Science and Economic Development Canada and the Federal Ministry for Economic Affairs and Energy, and builds directly on the Canada-Germany Digital Alliance announced at the G7 Industry, Digital and Technology Ministers' Meeting in Montreal on 8 December 2025.[9] Sovereign AI, sovereign compute, and the regulatory architectures that govern both are the declared scope. The June 2026 AI for All strategy operationalises this bilateral logic on the Canadian side: its sovereign-compute and build-partner-buy commitments are the domestic expression of the same Canada-Germany sovereign-technology cooperation the Alliance formalises. The democratic case for the Alliance is structural: two of the largest economies in the democratic world, neither home to a hyperscaler, committing to build the technology stack on which sovereign cognitive

defence depends, jointly and with explicit reference to the conditions that distinguish democratic governance from the closed systems being built elsewhere.

The Alliance changes what the corridor can carry. The corridor's bilateral anchor is no longer only a political commitment but a sovereign-technology platform on which the Canada-Germany-EU cognitive defence cooperation can operate. Cohere-Aleph Alpha at the firm level, treated in the next section, is one expression of the same logic. The Alliance is the policy frame within which that firm-level convergence makes strategic sense.

All In, the major Canadian AI conference convened annually in Montreal, has named Germany its Country of Honour for September 2026. The conference is the natural public moment to announce the cognitive defence layer of the Canada-Germany bilateral, paralleling the AI sovereignty cooperation already in train through the Sovereign Technology Alliance. A joint announcement at All In, made by Canadian and German principals, would give the corridor a public-event anchor and signal to allies, adversaries, and the democratic AI ecosystem that the policy-level Alliance and the firm-level convergence have an operational defence layer behind them. The suggestion is not a recommendation in the same sense as elsewhere in this report, but a sequencing observation: the public moment exists, and it should be seized.

The operational case for the corridor is strongest in Latvia. Canada has been the NATO framework nation in Latvia since 2017, leading the multinational battlegroup at Camp Adazi, with Canada-Latvia commitments to scaling that battlegroup to a brigade-size formation. Germany is deployed in Lithuania with parallel commitments. Germany and Latvia cooperate substantively on hybrid threats.

Germany is also identified within ACT field research as an exemplary case across the four cognitive-warfare-adjacent capability strands. Joint methodology development between the two on cognitive defence is the structural complement to the operational alignment that Latvia already demonstrates.

A novel operational recommendation from this research is the reciprocal secondment, developed at the Canada recommendations chapter as the operational mechanism through which Canada-EU cognitive defence cooperation should now proceed. The

precedent is the placement of two consecutive United States Department of State officials within the EEAS counter-FIMI policy and partnerships unit, working directly inside the EU institutional structure rather than from the United States mission to the European Union. The institutional learning that resulted has been substantial, and the model is replicable. The recommended Canadian instrument is the secondment of a Global Affairs Canada official into the same unit, working from inside the EEAS rather than from the Embassy of Canada to the European Union. The reciprocal direction, less developed in the literature but operationally symmetric, is for Canada to host a secondee from the EEAS or from an EU member state directly within the Rapid Response Mechanism or the Canadian Cognitive Defence Agency proposed at the Canada recommendations chapter, rather than seconding that official to fill a post at the EU mission in Ottawa. The two directions together convert what is currently a one-way institutional learning relationship into a genuine bilateral exchange, with the corridor as the architecture that makes the reciprocal direction operationally meaningful.

The Defence-Industrial Dimension

Helsing, one of Germany's leading AI defence companies, completed the first three tests in 2026 integrating its AI agent Centaur into the Gripen E platform, embedding German AI capability directly into Swedish airframes. Canada is in active procurement discussions with Saab on 72 Gripen E fighters and six GlobalEye surveillance aircraft, with domestic assembly and an AI and aerospace R&D centre in Montreal.[10]

In July 2026 Canada selected Germany’s ThyssenKrupp Marine Systems as preferred supplier for the Canadian Patrol Submarine Project, potentially up to twelve Type 212CD submarines, in what the government described as the largest defence procurement in Canadian history. The three governments framed the decision as the beginning of a long-term strategic partnership between Canada, Germany, and Norway, anchoring the corridor’s defence-industrial logic at the platform level as the Gripen and AI examples anchor it upstream.[11]

The Cohere-Aleph Alpha merger announced in April 2026, the firm-level expression of the Sovereign Technology Alliance’s policy frame, combines Canada's leading AI foundation-model company with one of Germany’s, and represents the corridor's

defence-industrial logic at the upstream layer: Canadian AI capacity married to European AI capacity to produce the sovereign democratic AI infrastructure. Presently, the United States and China collectively account for over seventy per cent of global AI investment, with the United States alone controlling roughly seventy-five per cent of high-end AI compute capacity.[12]

The corridor's defence-industrial cooperation is about pooling democratic AI research capacity so Canada, Germany, and EU partners can build cognitive defence tools without depending on platforms whose commercial incentives are misaligned with democratic values.

What the Corridor Enables

The corridor's value is that it creates a minilateral layer between the bilateral and the multilateral. This would be fast enough to be operational, trusted enough to share sensitive information, and politically coherent enough to present a common external face on threats NATO's collective defence architecture was not built to address. The corridor would allow complementarity. Germany leads where Canada lags, and Canada leads where Germany lags. Germany has seven decades of civic education infrastructure and is building its detection and attribution architecture. Canada has an excellent detection architecture and needs its public resilience institution.

The corridor also gives Canada its entry point into the wider architecture democracies with dedicated cognitive defence capacity are now beginning to build. A standing working-level exchange among states with dedicated counter-FIMI institutional architecture, anchored through the FIMI Information Sharing and Analysis Centre and convened by the European External Action Service, with the European Centre for Democratic Resilience launched in November 2025 as a core component of the European Democracy Shield serving as the wider EU coordination architecture for democratic resilience, is the natural collective container for the operational cooperation the corridor enables bilaterally. The candidate membership reflects existing capacity: France, Sweden, Germany, Italy, Poland, Latvia, Estonia, and Lithuania within the EU, with Canada, Norway, the United Kingdom, Ukraine, and Australia as close partners outside it. Such an exchange would do at the methodological and operational level what NATO's Strategic Communications

Centre of Excellence does at the doctrinal level, and what the FIMI ISAC is beginning to do at the threat-intelligence-sharing level. The corridor is the architecture through which Canada enters and helps build upon that exchange.

The European Union is the third anchor: only the EU can change the structural conditions of the information environment by enforcing the DSA's platform accountability obligations and the DMA's gatekeeper constraints with the market power to compel compliance, operationalising the Democracy Shield with the political weight to make it more than a signal, and governing the AI systems reshaping the epistemic conditions of democratic life.

The corridor would connect national resilience architecture to supranational regulatory power. That connection is what transforms a bilateral security arrangement into a democratic governance proposition. Through the Democratic Regulatory Partnership Framework, proposed in Chapter 29, the EU can extend that regulatory perimeter beyond its own borders, converting the corridor from a three-party arrangement into the first architecture of a global democratic governance framework for the information environment of the digital age. The Carney government's framing names the strategic posture required: working together to reinforce each other's respective strengths. The scaffolding is already there. The next step is to choose to use it.

Endnotes

1 Prime Minister of Canada, "Canada-Germany joint statement," Ankara, 7 July 2026.

2 Carolina Drüten, "Ex-NATO chief Rasmussen warns of 'disintegration' of alliance, calls for new European defense bloc", *Politico*, May 8, 2026. https://www.politico.com/news/2026/05/08/anders-fogh-rasmussen-interview-nato-00911431

3 European External Action Service, 4th EEAS Report on Foreign Information Manipulation and Interference Threats: Dismantling the FIMI House of Cards (Brussels: EEAS, March 2026), Foreword by High Representative Kaja Kallas, eeas.europa.eu.

4 Joint Statement of the First Meeting of the Canada-European Union Digital Partnership Council, Montréal, 8 December 2025, canada.ca; European Commission, Joint Statement of the First Meeting of the EU-Canada Digital Partnership Council, 8 December 2025, digital-strategy.ec.europa.eu.

5 Fedir Korobeynikov, Andrii Davydiuk, and Volodymyr Mokhor, "Ontological Foundations of Cognitive Warfare" (NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2026).

6 Sophia Besch, 'Germany's Reaction to Trump Is Another Paradigm Shift,' Carnegie Endowment for International Peace, April 2025, carnegieendowment.org.

7 Justin Massie and Barbora Tallová, 'Friends in Need, Friends Indeed? Explaining Variation in Military Support to Ukraine,' European Journal of International Security (2025), doi: 10.1017/eis.2025.13.

8 Government of Canada, Department of National Defence, 'Canada Achieves the 2% of Gross Domestic Product Defence Spending Benchmark,' 26 March 2026, canada.ca.

9 Innovation, Science and Economic Development Canada, 'Canada and Germany sign AI joint declaration and launch Sovereign Technology Alliance,' Government of Canada, 14 February 2026;

10 Daniel Leblanc, "Saab wants Canada to buy 72 Gripens and 6 GlobalEyes to fulfil promise of 12,600 jobs," CBC News, 14 January 2026; and "Saab dangles sovereign data centre in Montreal to undercut F-35 fighter contract," CBC News, 10 April 2026.

11 Murray Brewster, "Carney chooses German submarines as 'best platform and partnership' for Canada," CBC News, 6 July 2026.

12 On AI investment concentration, see Chatham House, How Middle Powers Can Weather US and Chinese AI Dominance (Royal Institute of International Affairs, February 2026), chathamhouse.org. On high-end compute capacity, see Alex Haag, "The State of AI Competition in Advanced Economies," FEDS Notes (Federal Reserve Board, 6 October 2025).

Part V: Recommendations

Chapter 14: Recommendations for Germany

Germany's greatest challenge is its institutional architecture and maintaining the operational tempo that the threat environment demands. The recommendations that follow are drawn directly from our analysis and from the field research conducted across German institutional, civil society, and security contexts. They are presented as a consolidated action set for the Federal Republic and Germany's European partners.

Recommendation 1: Close the Integrated Situational Awareness Gap

Germany lacks a Joint Intelligence Committee (JIC) equivalent . It does not have a clearing house that fuses Bundesnachrichtendienst (Federal Intelligence Service, BND) product, the Foreign Office view, and the Ministry of Defence picture into a single integrated assessment for the Chancellor and Federal Ministers of Foreign Affairs, the Interior (Bundesminister des Innern), and Defence. Intelligence and policy have been deliberately kept separate as a postwar inheritance with genuine democratic logic. The current structure routes intelligence upward to the Chancellor's Office through separate streams. No integrating mechanism produces a fused all-source picture that circulates across ministries. That separation is no longer tenable at the current threat level, nor in the current geopolitical environment. The National Security Council has the mandate to become this clearing house. It does not yet have the staffing. The NSC currently has less than 25 permanent staff. Germany recorded 321 sabotage incidents in the past year. The EEAS identifies it as the primary FIMI target among EU member states in Central Europe. This is not an ambient threat environment. One senior practitioner with direct knowledge of the institution assessed that effective operation at the scale of the threat requires between five hundred and one thousand. The structure exists in nascent form; the resourcing does not yet match the mandate set out in the November 2024 hybrid threat action plan, nor the scale the institution's own ambition implies. Closing that gap is the most direct single action available to the Merz government.

Building toward the JIC model requires a coordination function with political authority and analytical capacity sufficient to fuse the existing streams and present a single actionable

picture to all relevant principal actors. Germany has the correct starting point: a classified action plan already adopted, an inter-ministry task force architecture already in place, and a government with the mandate to expand both. The structural inadequacy of the National Security Council for cognitive domain coordination, identified by Stelzenmüller and confirmed in this report's field research, means the recommended dedicated cognitive domain coordination function must sit outside the NSC architecture rather than within it.[1] The NSC was designed for crisis coordination between senior ministers, not for the continuous, sub-crisis tempo at which cognitive domain threats operate. The sequencing is correct. The investment is the decision.

Recommendation 2: Establish a Russia-Vulnerability Mapping Programme

Russia systematically maps Western vulnerabilities and chokepoints as a prerequisite for its influence and sabotage operations. The 321 sabotage represent the output of an adversary that knows where Germany's critical nodes are. No Western democracy is currently doing the equivalent systematic mapping of Russian vulnerabilities: economic, social, informational, and political, as a prerequisite for a credible deterrence-by-punishment posture. This is the most analytically original recommendation to emerge from the German field research.

Germany is better positioned than most Allies to lead this work. It has institutional depth on Russia, a research community with genuine expertise, and the BND (Federal Intelligence Service) as a capable technical partner. The recommendation is to assign an explicit mandate within the NSC structure: systematic, ongoing mapping of Russian vulnerabilities as a standing analytical function. The output feeds the deterrence-by-punishment argument that Germany's intelligence community has already publicly adopted, and gives it the analytical foundation that a credible threat to impose costs requires.

Recommendation 3: Resource the VIGINUM-Style Agency

The ZEAM (Zentrum zur Abwehr von Einflussoperationen und Manipulation, Centre for Countering Influence Operations and Manipulation) coordination mechanism at the Federal Ministry of the Interior is the right institutional vehicle. The recommendation is to build it to the scale the threat requires, not to treat it only as a coordinator. The VIGINUM

model's core contribution is separating detection and attribution from strategic communications while connecting them operationally. Germany's historical inhibition on state information activities is not an obstacle. VIGINUM is not a propaganda agency. It is a detection, attribution, and exposure institution. The Goebbels constraint is not violated by building the capacity to identify what adversaries are doing and saying so publicly.

Public attribution of foreign interference, calibrated to the threshold criteria already developed in the Eckpunkte process, builds public resilience rather than public anxiety. The Estonia model is the precedent that makes the political case.[2] Germany should convene an annual Nordic-Baltic civil society exchange, bringing organisations from Estonia, Latvia, Lithuania, Finland, and Sweden to work with German counterparts on detection methodology and resilience practice. Germany’s civil society is ahead of its institutions. The goal is to close the gap between them.

Special attention should be given to cooperation with Lithuania as the country hosting German brigade which is under constant Russian hybrid attacks.

Recommendation 4: Reform the Bundeswehr's Cognitive Doctrine

The Cyber- und Informationsdomäne (CIR) branch is the correct institutional home for Germany's military cognitive warfare capability. The recommendation is to give CIR an explicit cognitive warfare mandate, beginning with curriculum reform. A mandatory basic cognitive warfare course at the officer school level for every officer. An additional course at the staff officer curriculum level. Specialised capability, including trained information planners and behavioural science expertise, assigned to special forces as the initial concentrated capability before broader distribution. The cultural understanding must precede the structural placement: trying to build institutional architecture before the conceptual framework exists internally produces bureaucratic orphans with no home to land in. Germany is not short of the analytical talent the reserve acquisition path can bring in. The sequencing is to build the culture first, then the structure. Finland built serious military cognitive capacity within a liberal democratic framework by integrating civilian expertise rather than militarising it, which is precisely the combination Germany’s constitutional culture can accept. The Bundeswehr source was direct: becoming more like Finland resonates in Germany in ways that other reference models do not.

Establish a structured pathway for reserve participation that connects civilian talent to the military cognitive doctrine function. The reserve acquisition path is an underused asset (Germany's reserve system allows direct commissioning of civilian specialists at officer rank, without full military training). Germany can bring relevant human talent into the system relatively quickly. Computational social scientists, communications professionals, behavioural economists, and digital analysts are currently operating almost entirely separately from official policy in the defence start-up ecosystem. Helsing is the proof of concept.[3] German AI capability developed primarily for Ukraine, operating at the frontier of what military cognitive tools can do. It would be beneficial to formalise the relationship between government and this ecosystem.

Recommendation 5: Expand the Canada-Germany Digital Alliance into the Cognitive Domain

The Digital Alliance, formalised through the Joint Statement of December 2025 and the Joint Declaration of Intent on AI of February 2026, is the right bilateral instrument. It addresses the upstream problem that the German Council on Foreign Relations (DGAP) technology sovereignty memo identified precisely: tech dependence as strategic submission. Germany and France are named as committed sovereignty partners in that analysis; the Canada-Germany Digital Alliance extends this logic bilaterally and grounds it in a shared democratic governance framework rather than pure industrial competition. Germany is Country of Honour at ALL IN 2026. Germany helped Canada gain entry to EU's SAFE programme and is pushing for Canada's inclusion in E3 discussions, more actively than either the United Kingdom or France. These are recent, specific actions demonstrating German investment in the bilateral relationship at the operational level. The Alliance should be expanded explicitly into cognitive defence with five elements: bilateral memoranda of understanding on intelligence sharing for cognitive threats; joint research programmes on detection, attribution, and resilience measurement; personnel exchanges between relevant agencies including structured secondments; shared exercises and tabletop scenarios for cognitive threat scenarios; and joint methodology development building the interoperability the EEAS-UK relationship has demonstrated is achievable.

Recommendation 6: Build the Coalition of the Willing on Democratic Cognitive Defence

Germany's most operationally effective coordination format is the Weimar Triangle. The recommendation is to institutionalise this model as the template for a wider coalition of the willing on democratic cognitive defence. Germany should lead, not merely participate in, this coalition.

Germany's leading position in the EEAS StratCom architecture, and its role in the new hybrid sanctions regime on Russia explicitly including FIMI entities, confirms political will at the institutional level. The EEAS assessment that Germany is among the four most-targeted countries in EEAS monitoring creates the conditions for Germany to argue, within EU and NATO forums, that the resourcing of cognitive defence response is proportionally inadequate to the threat.

Germany should make that argument explicitly, connecting it to the NATO 1.5 per cent commitment and the EU Multiannual Financial Framework negotiation.

Germany should also work with France bilaterally to build momentum within Europe on this agenda, and engage Ukraine substantively, whose practitioners are leaders in cognitive defence with unparalleled experience operating under conditions of active cognitive warfare.

Recommendation 7: Defend and Modernise the Politische Bildung Infrastructure

Germany already has the most developed Layer 1 social-infrastructure architecture of any similar democracy. The Bundeszentrale für politische Bildung (BZpB), founded in 1952 as part of post-1945 democratic reconstruction, has spent seven decades publicly funding civic education and democratic literacy as a standing government obligation. The Landeszentralen operate at the *Länder* level. The federally funded political foundations attached to the major parties operate transnationally with established office networks across more than a hundred countries. The infrastructure is the foundation that cognitive defence requires and that no other comparator democracy has. The recommendation is to defend and modernise what exists. The Bundeszentrale was the institutional defence Germany built against the collapse of shared civic and epistemic space that the country had lived through under National Socialism, and the post-1945 democratic reconstruction

named that defence as a permanent institutional task rather than as a transitional measure.

Defending the infrastructure means recognising that the BZpB's core function, building the epistemic and civic foundations of democratic life, is now also a security function. The institution's mandate should be expanded explicitly to include cognitive defence, with corresponding resourcing.

The mandate expansion is an acknowledgement that the BZpB's work and the security of German democracy are no longer separable. The political contestation now visible around the European Centre for Democratic Resilience demonstrates that cognitive-defence institutions face an adverse domestic political environment. The BZpB's existing legitimacy across the political spectrum, including its seven decades of cross-party support, is precisely the political asset that protects the institution against the political contestation newer cognitive-defence institutions face.

Modernising the infrastructure means equipping the BZpB to operate within the cognitive warfare environment. First, it must integrate emotional regulation and digital literacy explicitly into its curricular framework, drawing on the Klassens Tid model from the Nordic countries and the Finnish *politiikkakasvatus* tradition. Second, formalise the connection between the BZpB and the Federal Ministry of the Interior's ZEAM detection and attribution work, so that the BZpB's public-facing educational function and the state's detection function operate as complementary layers of the same institutional response rather than as parallel tracks. Third, position the BZpB as the convening institution for an EU-wide network of comparable Layer 1 institutions, leveraging federally funded foundations' existing transnational networks to build the European political-education infrastructure that the Niinistö Report has formally recommended at the EU level.[4] Defending and modernising the German foundation is the precondition for that corridor working at scale.

A Coherent Institutional Package

These recommendations span the framework's full architectural arc. The package is the architecture through which Germany operationalises its strategic-autonomy moment. The political will exists. The civil service, the defence-industrial base, and the public have already adapted. What remains is the political-cultural reflex of treating these foundations

as security assets, building the institutional architecture that connects them to the operational layers above, and exercising the strategic agency that the moment requires. The corridor architecture proposed in Chapter 13 is the partnership through which Germany operationalises the moment with Canada and the EU. The recommendations in this chapter are the institutional foundation that makes the corridor possible.

Endnotes

1 Constanze Stelzenmüller, 'Germany's National Security Council Isn't Up to the Task,' *Financial Times*, 28 August 2025.

2 Henrik Praks, *Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics, the Case of Estonia*, International Centre for Defence and Security, Tallinn, 2025, icds.ee.

3 helsing.ai institutional documentation; reporting in *Handelsblatt* and *Frankfurter Allgemeine Zeitung*, 2024-2026.

4 Sauli Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, report by the Special Adviser to the President of the European Commission, European Commission, October 2024

Chapter 15: Recommendations for Canada

Previously, we set out the diagnosis for Canada. The country arrives at this juncture with historical memory but without institutional knowledge, with capacity but without coordination. Andrew Coyne's characterisation of Canada as 'uniquely unprepared for the dire national-security crisis we are now in' captures the present state.[1]

The recommendations that follow answer that diagnosis. The federal government has already begun the architectural shift this chapter promotes, through its March 2026 announcement on continuous Rapid Response Mechanism Canada detection, the *Strong and Free Elections Act*, and the Cabinet Directive on the Coordinated Response to Threats to Elections.[2] The Defence Industrial Strategy commits C$6.6 billion over five years to the defence-industrial base building.[3] Canada met its NATO two percent target in 2026 and has committed to 3.5 per cent of GDP on core defence and a further 1.5 per cent on defence-and-security-related investments by 2035.[4]

The fiscal architecture for cognitive defence as a defence-and-security-related investment now exists in a way it did not eighteen months ago.

The Canadian context: diagnostic and methodological foundations

The following recommendations rest on a diagnostic and methodological foundation established earlier in this report. Three diagnostic findings, one methodological commitment, and one conceptual foundation recur across multiple recommendations and are therefore set out here once, rather than re-developed within each recommendation.

The first concerns Canada's foreign intelligence architecture. Canada is the only G7 country without a dedicated foreign intelligence agency. The structural absence is the most acute single capability deficit identified in the field research, and it is the precondition for almost everything else this chapter recommends.[5] No Canadian agency performs the foundational function of clandestine human intelligence collection abroad. Canada cannot independently assess the origins, objectives, or operational methods of foreign cognitive operations targeting its population, and depends on allies, primarily the United States, to tell it what is happening. In the operating environment Chapter 9 documented, that dependency is a sovereignty problem.

The second diagnostic finding concerns Canada's regulatory exposure on data sovereignty and platform accountability. Canada's federal data sovereignty score on the Upper Harbour Provincial Data Sovereignty Exposure Index of March 2026 sits at the bottom of the comparative table; only Quebec, with Law 25, has a sovereignty framework comparable to international standards.[6] Canada’s main privacy protection law, PIPEDA, has not been materially updated since 2001. Maximum penalties stand at $100,000 with no private right of action and no order-making authority for the Office of the Privacy Commissioner. No Canadian jurisdiction explicitly addresses CLOUD Act exposure in binding law. The CUSMA review of July 2026 is the binding near-term horizon: any data-sovereignty legislation Canada passes must account for the digital provisions of CUSMA, which the *Financial Times* described in 2018 as a 'big winner' for Silicon Valley.[7] The Digital Services Tax rescission of June 2025 is the warning: digital sovereignty instruments not entrenched in legislation are tradeable.

The third diagnostic finding concerns the upstream infrastructure question that Canadian regulatory discourse has barely engaged. Heidi Tworek, with Taylor Owen and Nanjala Nyabola, has set out a four-domain framework for assessing platform governance and digital sovereignty: content, data, competition, and infrastructure. Canadian regulatory discourse has concentrated on the first, made limited progress on the second through provincial leadership in Quebec, neglected the third, and barely engaged the fourth. Infrastructure ownership and control sits upstream of the others. Content moderation reaches only the platforms that operate in Canadian markets; competition policy binds only on the actors a Canadian regulator can compel; data-sovereignty obligations bind only as effectively as the underlying infrastructure permits. The Canadian empirical position is structurally worse than the regulatory discourse acknowledges. Microsoft and Google together hold approximately 93 per cent of the Canadian office software market.[8] Approximately 60 per cent of the Canadian cloud market runs on US hyperscalers subject to the *Clarifying Lawful Overseas Use of Data Act* of 2018, which authorises American authorities to compel disclosure of data held by US-jurisdiction companies regardless of where the data physically resides.[9]

The Microsoft Canada $7.5 billion AI infrastructure pledge of December 2025, even with its sovereignty messaging, does not change the underlying jurisdictional exposure that the Microsoft executive admission to the French Senate in June 2025 made structurally explicit. The Government of Canada's own 2024 Digital Sovereignty White Paper acknowledged the principle: as long as a cloud service provider operating in Canada is subject to the laws of a foreign country, Canada does not have full sovereignty over its data.

These three diagnostic findings sit underneath the operational, intelligence, technical, regulatory, and infrastructure recommendations that follow as the empirical case for action. Each of these layers (operational, intelligence, technical, regulatory, infrastructure, coordination, the human-relational substrate of cognitive defence anchored in emotional regulation, social trust, and the conditions of resilient societies that the manuscript names Layer 1, and the institutional layer) reinforces the others, and each works against the conditions adversarial cognitive operations exploit: isolation, low trust, weak associational density, hollowed public space, housing precarity, civic disengagement, and the loss of dialogue across difference. The recommendations respond to these conditions as much as to the threats themselves.

Read alongside the framework chapters, the recommendations that follow are also organised to deny adversaries cognitive advantage across the three dimensions NATO Allied Command Transformation has named: narrative advantage, psychological advantage, and decision advantage. Recommendations 1 through 5 concern primarily narrative and decision advantage, building the institutional architecture through which Canada detects, attributes, and responds to adversarial operations across the continuum of competition. Recommendation 6 strengthens whole-of-government coordination as the spine on which the rest depends. Recommendations 7 and 8 concern primarily psychological advantage, building the population-level conditions of cognitive resilience that adversaries cannot fracture and the human-relational substrate without which the layers above sit on sand. Recommendation 9 secures the international partnership architecture through which Canadian cognitive defence operates beyond Canada’s own borders. The collective object of these recommendations is Canadian cognitive

sovereignty: the sovereign capacity of Canadians to form genuine political preferences free from coercion, and the institutional architecture that makes that capacity continuous, public-facing, and durable.

Recommendation 1: Complete Rapid Response Mechanism Canada

The Rapid Response Mechanism is among the most credible open-source monitoring operations in the democratic world. Canada built it at the 2018 Charlevoix Summit before any equivalent national agency existed in any G7 country; France's VIGINUM, now the Alliance's reference standard, was modelled on the RRM and established three years later in 2021.[10] Canada is the originator of the architecture VIGINUM operationalised more fully. The recommendation is not to import a foreign model but to complete Canada's own.

The March 2026 commitment to continuous detection, with $31.5 million over five years, moves the RRM to year-round operation. The remaining gap is mandate and tempo. VIGINUM holds the authority to engage directly in the information environment, not only to monitor it. The RRM's expanded form should include attribution authority, public communication mandate, and operational tempo equivalent to VIGINUM's. Russia spends three to four billion dollars annually on disinformation operations, Canada spends twenty to thirty million addressing them.[11] This commitment does not close that gap.

The Canadian model improves on VIGINUM along a further dimension. Dave McMahon has proposed a federated public-private architecture in which Canadian sovereign intelligence companies feed operational intelligence and analytical capacity into the federal mandate.[12] The expanded RRM holds the legal authorities, the classified equities, and the federal mandate that the private sector cannot. The federation solves the talent, agility, and tooling problem the federal government cannot. VIGINUM has the federal mandate but no equivalent private-sector federation.

Recommendation 2: Establish a dedicated foreign intelligence service

The foreign intelligence gap set out previously is the most acute single capability deficit Canada faces. The recommendation is not to establish a HUMINT service. Instead, Canada must establish a dedicated foreign intelligence service whose primary collection

modality is digital, with a human analytical core, working with the private sector to fill capability gaps.

AI-enhanced signals collection can collect at scale and attribute at speed. What it cannot do is interpret. Understanding why a particular narrative is resonant in a specific cultural context, what historical grievances it activates, what religious or ethnic identity it exploits, requires human expertise. Canada is operating against adversaries whose societies, languages, histories, and internal political dynamics are not understood by most Canadian analysts. The specialists in psychology, culture, language, and history are the analytical core. In peacetime they produce the threat picture that feeds the RRM operational mandate and the CCDA's public-engagement work. In a conflict scenario they are the foundation of whatever active defence capacity the government decides to authorise. CSIS's mandate should be clarified concurrently as exclusively domestic, ending the mission creep that has muddied institutional accountability for years. The foreign intelligence service is classified and operationally clandestine; the Canadian Cognitive Defence Agency proposed at Recommendation 8 is open-source-only and public-facing. They are complementary, not competing. The classified service feeds the open-source agency's threat picture; the open-source agency speaks where the classified service cannot.

Recommendation 3: Modernise the Communications Security Establishment

The Communications Security Establishment (CSE) is the upstream technical fusion centre that feeds the RRM operational mandate and the foreign intelligence service. Its modernisation is the technical precondition. Three components are required.

First, AI-enhanced signals intelligence at the scale the contemporary cognitive threat environment requires. This includes: network-level pattern detection, temporal analysis, content pattern analysis at scale, cross-platform correlation, link and domain analysis, statistical anomaly detection, and higher-level attribution signals at the global and domestic infrastructure layers; coordinated behaviour detection, account behaviour profiling, and pattern of life analysis at the platforms layer.[12] The capacity required to operate AI-enhanced SIGINT at this scale is now substantively in place. The Cohere-Aleph Alpha merger, with a combined valuation of $20 billion, gives Canada a sovereign

AI inference platform of the scale and depth Canada has not previously possessed.[13] Through the Defence Industrial Strategy the CSE could secure sovereign inference capacity at the scale the threat environment requires.

Second, sovereign space-based intelligence, surveillance, and reconnaissance. Telesat is the Canadian platform capable; the Defence Industrial Strategy's identification of digital technologies and cyber as priorities establishes the procurement architecture.[14]

Third, amended legal authorities for semantic-layer operations. The current CSE Act of 2019 authorises foreign signals intelligence and active and defensive cyber operations within statutory limits. The contemporary cognitive threat environment requires explicit legal authorities for operations at the semantic layer, with appropriate oversight from the National Security and Intelligence Review Agency and the Intelligence Commissioner, and with the National Security and Intelligence Committee of Parliamentarians as the political-level oversight mechanism.

Recommendation 4: Build the regulatory architecture for data sovereignty and platform accountability

The regulatory exposure on data sovereignty and platform accountability is the Government of Canada’s impetus to enact the regulatory architecture before the window closes.

Three operational recommendations follow. First, pass the *Consumer Privacy Protection Act*, including explicit cross-border data-flow controls and CLOUD Act provisions, statutory penalties at international scale, order-making authority for the Office of the Privacy Commissioner, and a private right of action.

Second, extend Canada’s no deepfake-in-elections precedent to year-round cognitive defence: the prohibition on deepfakes targeting electoral actors should sit alongside platform accountability legislation that mandates ownership-and-control disclosure for federal contracts, classification at the point of procurement distinguishing Canadian-owned from foreign-parented vendors with full extraterritorial legal exposure, and weighting of that classification alongside price in bid evaluation.

Third, enact platform regulation as the floor, not the ceiling, of platform accountability, building on the framework currently before Parliament as Bill C-34 (the *Safe Social Media Act*), with platform design obligations and algorithmic transparency requirements as the durable foundation Canadian platform accountability has so far lacked. International comparators are converging fast: France announced in January 2026 that 2.5 million civil servants will stop using Microsoft Teams and Zoom by 2027. The German state of Schleswig-Holstein is migrating 44,000 employee accounts to open-source. The Austrian military has dropped Microsoft Office for LibreOffice. And the Dutch parliament is tendering for a national cloud after a 67 per cent foreign-provider audit.[15] Canada lags behind many peer countries. Canadian platform legislation should additionally be brought into substantive alignment with the European Union's Digital Services Act and Digital Markets Act, creating a transatlantic digital commons with shared rules and standards. Market-size realism is the operational reason: Canada is too small a jurisdiction to pass divergent platform legislation that platforms can simply exit, as the Online News Act demonstrated when Meta pulled news rather than comply. DSA and DMA harmonisation is therefore not merely desirable but practically necessary for Canadian platform legislation to be enforceable.

The dominant Canadian regulatory frame addresses content moderation and platform liability for harmful material. The contemporary cognitive threat environment requires the frame to extend further, to platform architecture and the monetisation models that produce the conditions in which cognitive operations succeed. Renée Black, founder of Good Bot and previously founding Executive Director of PeaceGeeks, identifies the inflection point: the 2018 algorithmic shift to engagement-based ranking, which forced even routine government communication to adopt more sensational and divisive language to register in user feeds, restructured the information environment Canadians now inhabit.[16]

The empirical foundation for proportionate regulation is now sharply documented at the Canadian level. The Media Ecosystem Observatory's study of 14 million social media posts found that approximately 100 accounts produce 68 per cent of conspiratorial posts in the Canadian online ecosystem and capture 90 per cent of associated views.[44] Reuters' November 2025 investigation of internal Meta documents found that the company

projected approximately ten per cent of its 2024 global revenue, roughly $16 billion, from advertising for scams and banned goods.[17] Canadian regulation that does not reach the advertising marketplace and the platform-design choices that monetise harm only addresses symptoms rather than structure.

Platform accountability legislation should characterise foreign information operations through demonstrable behavioural patterns, identify coordinated infrastructure, and tactical identification, without making contested claims about content.

A fourth operational recommendation follows: use the existing Canadian sanctions architecture to disrupt the revenue generation of Russian and Chinese state media operating in Canada. The operational precedent is Estonia's 2018-19 closure of Sputnik's Tallinn office.[18] The architecture for the equivalent Canadian move exists. The political will to use it has not yet been mobilised.

Recommendation 5: Build digital sovereignty infrastructure alongside regulatory architecture

Canadian platform accountability legislation should treat infrastructure as a foundational layer alongside regulation. There should be explicit ownership-and-control classification of cloud, compute, and platform infrastructure used for federal workloads, and with procurement weighting that favours Canadian-jurisdiction infrastructure.

Regulation of dominant foreign-owned platforms does not change the underlying market structure that made Canadian information environment dependence possible. Decentralised social media have now reached the scale where a parallel investment track is operationally credible. Bluesky, built on the open AT Protocol, reached approximately 43.5 million users by April 2026.[19]

The recommendation: pair the platform accountability legislation with a Canadian decentralised-infrastructure investment track. The Canadian Internet Registration Authority's existing community investment programme is the institutional starting point. A sovereign-tech venture instrument modelled on the Venture Capital Catalyst Initiative, with a mandate scoped to Canadian-anchored decentralised social, communications, and AI infrastructure, would build the alternative ecosystem at the pace the threat environment

requires. Such a dual track is the structural complement that makes the regulatory architecture sustainable.

Recommendation 6: Increase cognitive defence coordination architecture across levels of government

The provinces and territories deliver education, healthcare, local government, and many of the civil society functions that constitute the lower foundation of the six-layer model. The federal government must convene, resource, and coordinate. The federal-provincial-territorial mechanism reactivated under the Carney government is the delivery vehicle.

First, these governments must establish a dedicated FIMI and cognitive security agenda item within the federal-provincial-territorial process at the Council of the Federation level, and create a standing FPT Security and Democratic Resilience working group meeting at minimum annually. Premiers and territorial leaders cannot act on threats they cannot see. There is evidence of US support for provincial secessionist movements, exploitation of Indigenous reconciliation processes, and targeting of regional cleavages to achieve the dismemberment rather than annexation of Canada.[20] Provincial governments need to be provided the resources to better understand and confront these threats.

Second, Indigenous governments are architectural partners. Indigenous data sovereignty work, including the FNIGC OCAP principles and Animikii's leadership on Indigenous-led data governance, should inform the architectural design of the federal cognitive defence response. The Sturgeon Lake Cree First Nation case stands separately as the only worked example to date of a successful Canadian institutional response operating from the treaty framework.

Third, citizen engagement architecture. Peter MacLeod, a leading Canadian practitioner of citizen engagement design and author of Democracy’s Second Act: Why Politics Needs the Public, proposes mandatory civic-engagement components for Grade 12 students and newcomers to Canada, delivered provincially through education and immigration settlement programmes.[21] Toronto, Montreal, and Vancouver are primary adversary targets for both diaspora community manipulation and critical infrastructure operations. The municipal dimension currently has no formal role in the national security architecture;

this recommendation names the gap as a structural design problem requiring a future mechanism.

The political-level coordination gap has two clean solutions at the federal level. The Minister of Canadian Identity and Culture, whose portfolio holds broadcasting policy, cultural industries, and the federal response to online harms and disinformation, should be added to the Cabinet Committee on National Security. The current arrangement, in which the regulatory minister whose portfolio holds the cognitive defence policy architecture is not in the security room, is a structural design problem with a one-line solution. NATO's own consolidation of information capabilities into a single division (J10) five years ago is the operational precedent for political-level integration of the cognitive warfare file: the institutional logic that drove NATO's decision is the same institutional logic that drives this recommendation.

Mandatory annual public threat reporting completes the coordination architecture. Canadian intelligence legislation should require designated intelligence-receiving institutions to produce coordinated annual public threat assessments, modelled on Articles 8 and 26 of the Lithuanian Law on Intelligence, which require the State Security Department and the Defence Intelligence and Security Service to jointly publish a National Threat Assessment and a Report on Activities each year. Estonia operates a similar architecture under the Security Authorities Act, with three intelligence services publishing public threat assessments. Norway anchors the practice in its *totalforsvar* doctrine, with three independent intelligence services publishing annual public threat assessments. Finland combines a 2019 Civilian Intelligence Act with the Finnish Security and Intelligence Service’s annual public yearbook, published by institutional convention since 1994. The principle these jurisdictions share is that public trust in intelligence institutions depends on the public being told what those institutions know about the threats facing the country. Canadian legislation should name this requirement explicitly, with the Government of Canada’s Privy Council Office, the Communications Security Establishment, the proposed foreign intelligence service, and the Canadian Cognitive Defence Agency identified as institutions subject to the public-reporting mandate.[22]

A separate coordination gap operates at the working level. Canadian point of contact for cognitive defence cooperation is currently unclear from the European side.[23] Global Affairs Canada is the operational lead for external cognitive defence coordination. The Privy Council Office is the domestic coordination point for the federal cognitive defence architecture. The split mirrors the division of labour between policy lead and operational delivery that already structures Canadian foreign policy on every other major file. Articulating it explicitly removes the friction the EU practitioner field research synthesis identifies.

Recommendation 7: Treat emotional self-regulation as Layer 1 cognitive defence infrastructure

The human capacity to recognise emotional manipulation as it happens is what this recommendation operationalises.

Acute emotional arousal, whether triggered by fear, outrage, or moral disgust, takes the prefrontal cortex offline. The author's interviews with experts on the subject describe the result: under perceived threat the brain instinctively protects executive function by suspending it, and access to logic, reasoning, empathy, and forward thinking degrades.[24] The objective is not to make Canadians believe a particular narrative. It is to erode the information space sufficiently that Canadians stop believing in anything, including the integrity of the democratic process itself.

The Canadian population is arriving at this contest vulnerable. Recent data from Abacus Data show that more than eight in ten Canadians have to stay on guard financially because another hit could come at any time, 45 percent say everyday spending decisions are more mentally draining than they were a year ago, and that 44 percent believe life in Canada is becoming increasingly unpredictable.[25] The financial precarity these surveys document has its largest single substrate in housing: the housing-affordability crisis is the most operationally significant of the precarity conditions adversarial cognitive operations exploit, because it is sustained, geographically distributed, and shapes the daily life cognition of working-age Canadians. Adversaries operating in this environment do not need to do much to push Canadian cognitive function below the threshold required for resilient democratic engagement. Cognitive resilience at population scale, the outcome

this recommendation is designed to produce, depends on the emotional and material conditions in which Canadians live as much as on any institutional capability built above them.

We recommend three operational changes. First, the federal-provincial-territorial mechanism should treat social infrastructure as a standing agenda item alongside the cognitive security agenda, with delivery sectors named explicitly: educators, who spend more waking hours with Canadian children than primary caregivers do across the working week; police services, whose officers serve disproportionately the populations who are themselves dysregulated by trauma, addiction, and structural disadvantage, and currently receive no training in trauma-informed practice or in their own emotional self-regulation under operational conditions; and the foster system, which absorbs children carrying intergenerational trauma into placements with carers who themselves are typically under-resourced, under-trained, and under-supported. The argument is that the substrate of cognitive defence runs through the adult sectors that regulate children and the dysregulated, not primarily through curriculum changes for the children themselves. Layer 1 investment in these three adult-facing sectors is the highest-leverage cognitive defence spending available. What this investment buys is cognitive resilience at population scale: the capacity of Canadians, individually and collectively, to recognise adversarial manipulation, regulate the emotional reactivity it is designed to provoke, and sustain democratic participation under continuous cognitive pressure.

Second, there should be open-source-only methodology extending to publicly accessible educational programmes for educators, front-line responders, and the wider population on the recognition of foreign cognitive operations as they target emotional response. The Canadian Cognitive Defence Agency proposed in Recommendation 8 should work with provinces and territories to develop this programming with the three delivery sectors named above (educators, police, foster carers) explicitly in scope.

Third, the federal government should commit to Layer 1 delivery as an investment under the 1.5 per cent defence-and-security-related envelope on the same fiscal footing as the institutional architecture above. Layer 1 social infrastructure is the foundation on which the hard architecture functions. Investments in social infrastructure are not values driven

nor ‘soft’ policy. It is an investment in foundational democratic resilience upon which our democratic way of life relies.

The provinces and territories deliver. The federal architecture makes delivery possible.

Recommendation 8: Establish a Canadian Cognitive Defence Agency

The report’s most original recommendation is that Canada establish a Canadian Cognitive Defence Agency that would create a synthesising institution which holds the open-source mandate that the secretive components of the architecture cannot, and gives Canadian cognitive defence a single named accountable body for citizens, civil society, journalists, and allies to engage with directly.

The Hogue Commission found that information manipulation poses the single biggest threat to Canadian democracy and recommended the establishment of a new agency to monitor open-source information.[26] The Canadian Cognitive Defence Agency is the answer to that deferral.

The CCDA is the institution Canada's architecture most lacks. The RRM watches, attributes, and briefs upward to the government and to G7 partners. The CCDA would speak, educate, and engage outward to civil society, educators, journalists, diaspora communities, and the general public. Modelled on the Swedish Psychological Defence Agency but adapted for Canadian realities, the CCDA would operate entirely on open-source material, publish its analytical product publicly, and engage civil society. France's VIGINUM operates at sixty-plus dedicated personnel, Italy is reportedly assembling a Ministry of Defence-anchored hybrid threats unit at one hundred-plus, the German VIGINUM-equivalent is under construction within the Federal Interior Ministry, and Poland's NASK continues to expand.[27] The CCDA should be staffed at one hundred to one hundred and fifty personnel at full operating capability, drawing on the Italian and German benchmarks rather than VIGINUM as the lower bound, given Canada's larger population and more contested information environment.

The CCDA's open-source-only scope would be a design principle. It is the source of the agency's political viability and the reason civil society and private-sector partners can engage with it without compromising sources, methods, or commercial relationships.

Statutory limits on what the CCDA collects, holds, and produces are what would make it credible to the Canadian public, defensible against political instrumentalisation, and durable across changes of government. The explicit goal is to ensure public trust in cognitive defence institutions continues and ideally increases over time, with public trust treated as the central operational metric of the agency's success.

The CCDA should be established at arm's length from the Privy Council Office, with a dotted-line institutional relationship modelled on the Communications Security Establishment's relationship to the Minister of National Defence. This separation from the government of the day is part of the trust foundation principle: the agency speaks publicly in its own institutional voice, not as a political organ. It should be funded from the 1.5 per cent defence-and-security-related envelope. Its core functions, drawing on McMahon's framework, sit at the Human (receiver) layer of the cognitive defence architecture.[28] Classified inputs from CSE and CSIS feed the threat picture that informs CCDA analysis without the CCDA itself generating classified product.

The Quebec experience with the *Centre d'optimisation, de développement et d'excellence numérique* is the cautionary parallel the CCDA's design must absorb. The CODE proposal, structured as a 51-49 public-private partnership with CGI, drew an Unité permanente anticorruption red flag on cronyism and contract length; the SAAQclic precedent, projected at $1.1 billion by 2027 with 329 per cent over budget on one component, is the operational warning of what Canadian digital sovereignty implementation produces when public-private architecture is built without governance scaffolding.[29] The CCDA must be designed explicitly against this risk: open procurement, statutory ownership-and-control disclosure for federal contracts, and arm's-length governance with civil-society partnership obligations modelled on the relationship between Public Safety Canada's Community Resilience Fund and ISD Canada, whose April 2026 *Online Domestic Extremism Data Briefing* demonstrates the analytical work civil society already delivers that the federal government does not internally produce.[30] The local journalism cluster sits within the CCDA's convening mandate; the empirical case and the operational interventions for the Free Press are set out in Recommendation 10.

Recommendation 9: Build Canada's European cognitive defence partnerships

The Canada-Germany-EU corridor is the strategic frame within which Canadian cooperation with European partners operationalises, and is set out separately in the Corridor chapter. The wider European partnership architecture extends further, and Prime Minister Carney has spent his first year in office building it. At the eighth European Political Community Summit in Yerevan in May 2026, the first EPC summit a non-European leader has ever attended, the Prime Minister identified seven domains of strategic autonomy in which Canada and Europe should now build sovereign capabilities together, and concluded that "the international order will be rebuilt, but it will be rebuilt out of Europe."[31] Cognitive sovereignty is the missing eighth domain. It should be named. The recommendation is to build the partnerships set out below as the operational architecture for that domain.

France. France is Canada's deepest single European bilateral relationship on cognitive defence, and the relationship's institutional foundations are now in place. Prime Minister Carney's first official trip abroad was to Paris on 17 March 2025, where the leaders launched a new bilateral partnership on intelligence and security focused on cybersecurity, foreign interference, sabotage, and threats associated with advanced technologies.[32] The methodological lineage between Rapid Response Mechanism Canada and VIGINUM is well established: VIGINUM was modelled on the RRM, and France's weekly public electoral threat bulletins around its 2026 municipal elections were developed from discussions with the Office of the Privacy Commissioner of Canada about lessons from Canadian general elections. The recommendation is to formalise the bilateral cognitive defence cooperation through a structured working-level cadence between the expanded RRM and VIGINUM, with joint methodology development on attribution standards, public communication formats, and the three-tactic active counter-FIMI model that France has operationalised through its Ministry of Foreign Affairs SWAT Unit. France has approached Canada to learn from the Canadian model, and Canadian counterparts have approached France to learn from the SWAT Unit; the relationship is genuinely two-way and should be institutionalised on that basis. The Canada-France Declaration on Artificial Intelligence, signed in 2018 and developed through the Global Partnership on AI and the Paris AI Action Summit of February 2025, is the second

institutional anchor of the bilateral. Cognitive defence cooperation should be built on that foundation, with the AI track developed alongside the counter-FIMI track and brought into triangulation with the Canada-Germany Sovereign Technology Alliance, signed at the 2026 Munich Security Conference. The strategic horizon is a Canada-France-Germany cooperation toward a global commons approach to artificial intelligence: democratic, sovereign, and accountable, as the alternative to the closed-system AI architectures the United States and the People's Republic of China are each building.

The European Union. The Canada-EU institutional relationship has moved from rhetorical alignment to operational architecture across the past year. The New EU-Canada Strategic Partnership of the Future and the Security and Defence Partnership were announced in June 2025. In February 2026, Canada became the first non-European country to join the EU's Security Action for Europe (SAFE) initiative.[33] The Canadian secondment to the EEAS counter-FIMI policy and partnerships division is the operational mechanism through which Canada-EU cognitive defence cooperation should now develop. The European Centre for Democratic Resilience, announced as a core component of the European Democracy Shield in November 2025, is the EU-level coordination hub through which the FIMI Information Sharing and Analysis Centre architecture and the wider counter-FIMI cooperation now run, and Canadian engagement with the Centre as a partner-tier participant should follow the model already established through the Canadian secondment to the EEAS counter-FIMI division. Two further actions follow. First, Canada should join the EU FIMI Toolbox working group as an associate participant, the lowest-cost mechanism for Canadian alignment with EU methodological standards. Second, Canada should accept the European External Action Service's standing offer to participate in joint attribution exercises on adversary networks operating across both jurisdictions, with the Doppelganger and Portal Kombat networks as immediate operational subjects. Two additional operational engagements complement these. First, Canada should join the Hybrid Centre of Excellence's hybrid threats model in practice project, originated at the Sydney Countering Foreign Interference Summit, with its focus on documented deterrence successes across the thirteen hybrid threat domains as the substantive cooperation vehicle that operationalises Canada-EU policy dialogue into shared methodology. Second, Canada should join Team Europe Plus coordination

on the ground through the network of Canadian diplomatic missions, including coordinated briefings to local journalists in third countries, joint training delivery, joint situational awareness reporting, and joint statements at country level.

Ukraine. Ukraine is the partnership in which Canadian cognitive defence cooperation has the deepest operational case. Prime Minister Carney met with President Zelenskyy in Halifax in December 2025, conducted a surprise visit to Kyiv in August 2025, met with President Zelenskyy again on the margins of the Yerevan EPC, and announced a C$270 million contribution to the NATO Prioritised Ukraine Requirements List from Yerevan.[34] Canada is a core member of the Coalition of the Willing and has renewed Operation UNIFIER through 2029. The cognitive defence dimension of the Canada-Ukraine partnership is currently underdeveloped relative to the broader bilateral. Three operational steps follow. First, Canada should work with the UK and France to formalise cognitive defence cooperation as a named workstream within the Coalition of the Willing architecture, with Ukrainian StratCom counterparts as the primary operational partners. Second, Canadian engagement with the Ukraine Communications Group, currently the only operational coordination success in the EU FIMI ecosystem operating without United States participation, should be deepened from observer to substantive contributor. Third, Canadian doctrinal development on cognitive warfare should incorporate Ukrainian battlefield experience as a foundational empirical input rather than a peripheral case study. Fourth, and structurally most important, Canada should engage Ukraine specifically on the integration of digital infrastructure into whole-of-society defence. The Ukrainian Ministry of Digital Transformation, the Diia application's wartime functions including the eVorog reporting system, the volunteer-led OSINT and detection networks, and the Centre for Countering Disinformation under the National Security and Defense Council together constitute a digital-substrate model for cognitive defence that no Nordic-Baltic comparator has yet matched in operational maturity or population-level integration. The Ukrainian innovation is that digital infrastructure is constitutive of total defence rather than adjacent to it. Canada's digital sovereignty exposure is the inverse problem: the substrate has not been built. The Ukraine engagement on this dimension should run through the Canadian Digital Sovereignty Roadmap recommended in Recommendation 5, with Ukrainian counterparts as the primary methodological reference for what an

integrated digital-cognitive defence substrate looks like under operational conditions. The April 2026 report of the Standing Senate Committee on National Security, Defence and Veterans Affairs explicitly recommended deeper Canada-Ukraine cognitive defence cooperation along these lines, providing parliamentary endorsement of the substantive direction proposed here.

The Nordic Five: paired learning, not one-way knowledge transfer. The Nordic Five, Denmark, Sweden, Norway, Finland, and Iceland, are the cohort from which Canada has the most to learn on the conditions of resilient societies, and to which Canada has the most to offer on multicultural integration and Indigenous reconciliation. The Oslo Canada-Nordic summit in March 2026 was the political moment that authorised this partnership: the first Canadian Prime Ministerial visit to Norway since 1980, with all five Nordic Prime Ministers convening with Prime Minister Carney, who described "working with this group" as "at the centre of Canada's strategic interests."[35] The recommendation is paired learning, not one-way knowledge transfer. The Nordic countries lead the OECD on every interpersonal trust measure and have built the institutional infrastructure that produces those outcomes; Canada is currently grappling with the conditions adversarial cognitive operations exploit. At the same time, the Nordic countries are actively grappling with the integration of newer populations and with reconciliation processes that Canada has more institutional experience navigating, even where Canadian outcomes remain incomplete. The relationship is genuinely two-way.

Five named cooperation focus areas, one per Nordic country. Denmark is the leader within the cluster on housing-as-Layer-1-infrastructure. With Denmark, Canada should actively work to draw lessons from Danish housing and social-infrastructure models, and to understand the foundational philosophy that underpins them. The almene boliger non-profit social housing model constitutes approximately twenty per cent of the Danish housing stock, with resident-elected boards and explicit community-orientation provisions in legislation. Bofællesskaber, the cohousing tradition originated in Denmark and now codified in Danish planning law, is the architectural complement. Canada is making historic investments in housing through the federal housing strategy. These investments must have a community orientation or they risk degrading collective resilience rather than

building it. The Danish architectural and legislative models are the proven precedent that builds resilience as a byproduct of housing investment. Klassens tid, the curriculum-embedded empathy and emotional regulation programme, is the second strand of the Danish contribution. Denmark's active study of the Canadian Rangers as a model for Greenland-Nunavut territorial defence cooperation, including involvement of Indigenous communities, is the reciprocal Canadian contribution.[36] With Sweden, Canada should build on the Strategic Partnership signed during the Swedish royal state visit to Ottawa in November 2025, which named societal resilience, civil preparedness, and the Swedish total defence concept as enhanced strategic dialogue subjects. The Swedish Psychological Defence Agency (MPF) is the closest existing institutional analogue to the Canadian Cognitive Defence Agency proposed in this chapter. Canada should work with Sweden to draw on the MPF model in establishing the CCDA, including advisory engagement during the agency's design and standing-up phase, before deepening to a sustained Canada-Sweden working relationship between the CCDA and MPF, including secondment exchanges and joint training delivery. With Norway, Canada should build on the strategic cooperation announced during the March 2026 Carney visit, including cooperation on counter-FIMI methodology development through the Norwegian Defence Research Establishment (FFI). Norway's March 2026 Strategy for Strengthening Resilience to Disinformation (2025–2030), led by the Ministry of Culture and Equality, anchors a distributed institutional architecture rather than a dedicated agency model, structurally more analogous to Canada's federal-provincial-territorial coordination challenge than to Sweden's MPF model. Norway is among NATO's leaders in cognitive defence research, anchored by FFI, which makes it a particularly valuable partner for Canada in joint methodology development. FFI's research programme is where independent confirmations of the emotional regulation finding from a Norwegian research vantage strengthen the Canadian Layer 1 case. Canada should draw on the Finnish philosophy of whole-of-society security, as the Senate Standing Committee on National Security and Defence disinformation report recommended. The Carney-Stubb joint statement of April 2026 and its "values-based realism" framing provide the political authorisation for sustained engagement. The Hybrid Centre of Excellence in Helsinki is the institutional anchor; an MOU for Canadian participation in HybridCoE projects,

including the hybrid threats model in practice project, formalises the cooperation. The Finnish elite defence courses model, in which CEOs attend four-week courses at personal economic cost because the social contract supports it, is a Canadian capacity gap that Finnish cooperation can directly address. With Iceland, Canada should engage on Arctic information environment integrity as a cognitive defence priority, anchoring cooperation in the strategic communications dimension of public-information campaigns around submarine cable disruption and Arctic infrastructure threats. Iceland's positioning at the GIUK gap and its institutional posture on civil resilience under Arctic threat conditions are directly relevant to Canada's own Arctic cognitive defence posture.

Poland. Poland is Canada's deepest European, and increasingly close, partnership and the country Prime Minister Carney has named repeatedly as the model on defence rebuilding. The Canada-Poland Strategic Partnership was renewed during Prime Minister Carney's August 2025 visit to Warsaw, with annual bilateral consultations between government officials and a High-Level Steering Group on Bilateral Cooperation as the institutional architecture.[37] Canada will be the Lead Nation of the 2026 International Defence Industry Exhibition in Kielce, Poland, in September 2026. The cognitive defence dimension of the Canada-Poland partnership runs through NASK (the Państwowy Instytut Badawczy), the Polish counter-disinformation institute that functions as the Polish VIGINUM-equivalent and with which Canadian connections are already established. The recommendation is to formalise NASK as a named partner institution alongside VIGINUM and the German Federal Interior Ministry VIGINUM-equivalent in a structured monthly working-level cadence with VIGINUM and the German VIGINUM-equivalent, extending the existing trilateral architecture into a quadrilateral working group. The German VIGINUM-equivalent, the Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM), established within the Federal Ministry of the Interior in June 2024 with a €7.8 million initial budget allocation and led by Hanna Katharina Müller, is the German institutional anchor for this cooperation. The Weimar Triangle's near-weekly Signal exchanges at analyst-to-political-director level is the model for how this kind of cooperation produces operational impact through habit formation rather than through new political declarations.

The Baltic Three plus One: signal seriousness, learn the threat. Canadian Baltic engagement is one of the oldest continuities in Canadian foreign policy, predating NATO itself. From 1940 onwards, every Canadian government, Liberal and Progressive Conservative alike, refused to recognise the Soviet annexation of Estonia, Latvia, and Lithuania as legitimate. Prime Minister John Diefenbaker's 1960 to 1962 campaign at the United Nations General Assembly named Soviet rule over Eastern Europe and the Baltics as colonialism the international community should condemn alongside the colonial powers it was already condemning. Canada received and resettled Estonian, Latvian, and Lithuanian refugees fleeing Soviet occupation across decades, building three of the largest Baltic diaspora communities outside the homelands themselves. In 1991, Canada was the first major Western country to recognise the restored independence of the Baltic states, helping to formalise their international legitimacy and to cement the end of the Soviet Union. Operation Reassurance from 2014, the Canada-led NATO Multinational Brigade in Latvia, the Baltic 3+1 working group at foreign minister level, and Prime Minister Carney's participation in the Joint Expeditionary Force leaders' virtual meeting on 26 March 2026 are the operational continuation of a Canadian commitment to Baltic sovereignty that has been continuous for eighty-five years. The recommendation is to deepen the bilateral tracks alongside the multilateral architecture, with three operational components that follow.

First, Canada should signal long-term commitment to Baltic security by converting Operation Reassurance from a rotational mission to a permanent base footing in Latvia. Field research, especially out of the Nordic-Baltic capitals, converged on the same finding: Baltic engagement requires flesh and blood, not trade or subsidies, and Canada's Latvia-led NATO Multinational Brigade is the single most credible signal of seriousness Canada has sent to Baltic partners. Permanence answers the doubt Baltic publics carry about Alliance commitment. The cognitive defence dimension of this is direct: a permanent Canadian base says Canada is not going anywhere, and that signal is itself cognitive defence infrastructure for Baltic populations under sustained Russian pressure. Permanence also signals to Europe Canada's commitment to European security architecture and our intention to be a substantive participant in it going forward. Second, Canada should learn from Baltic counter-FIMI capability, particularly Estonia's digital

government infrastructure and the operational precedent of Estonia's 2018 to 2019 closure of Sputnik's Tallinn office using EU sanctions on Kiselyov, the only documented case of a democracy operationalising legal closure of a Russian state media presence on its territory. Estonia's digital government also provides the operational model for the kind of citizen-state digital infrastructure that makes platform-accountability work tractable; the e-Estonia model is genuinely transferable in part. Lithuania, as the Lithuanian National Crisis Management Centre demonstrated through its OECD disinformation hub training programme to twenty countries last year, is the methodology-transfer leader in the cohort, and Canada has an active StratCom working relationship with the Lithuanian Ministry of Foreign Affairs that field research confirmed is productive and underused.

The United Kingdom and the Joint Expeditionary Force. Canada should seek to join the Joint Expeditionary Force as a full member. The Joint Expeditionary Force is the British-led ten-country rapid response coalition that integrates the Wider North as a single strategic theatre encompassing Arctic, Greenland-Iceland-United Kingdom (GIUK) gap, North Atlantic, and Baltic Sea. Prime Minister Carney participated in the March 2026 JEF leaders' virtual meeting and General Carignan met JEF counterparts in London in early April 2026; the directional commitment exists.[38] Canada was invited to join JEF in 2013 and declined; thirteen years later, the strategic optics and operational realities are different. JEF accession formalises the Wider North architecture under which the Latvia base, the Baltic 3+1 working group at foreign minister level, and the broader Nordic-Baltic cooperation cohere. Capability development through the Defence Industrial Strategy is the bridging measure that makes the membership credible operationally, not a reason to defer the political commitment. The UK Foreign Affairs Committee's March 2026 report Disinformation Diplomacy recommended the establishment of a UK National Counter Disinformation Centre on a statutory footing, modelled on Sweden's Psychological Defence Agency, Ukraine's Center for Countering Disinformation, and France's VIGINUM. The doctrinal convergence with the Canadian Cognitive Defence Agency proposed in Recommendation 8 is direct, and the institutional debate now under way in Westminster offers Canada the opportunity to shape that conversation as a JEF member with a parallel architecture in build, rather than to join the conversation later as a follower.

Frontline EPC democracies: Moldova and Armenia. Frontline democracies, operating under sustained adversarial cognitive operations at greater operational intensity than peer democracies face, are the operational target population for the Canadian doctrinal contribution to Information Peacekeeping. Moldova and Armenia are the two named anchors. The Yerevan European Political Community summit's invitation, and Prime Minister Carney's bilateral with Prime Minister Pashinyan as the first listed bilateral on the summit margins, is the political signal that frontline EPC democracies are inside Canada's strategic frame, not outside it. Canada opened its embassy in Yerevan in October 2023, providing the institutional foundation for deepened bilateral cooperation. With Armenia, the recommendation is to build on the Yerevan bilateral with cognitive defence capacity-building cooperation as a Canadian contribution to Armenian democratic resilience, including methodology transfer through CCDA technical assistance once the agency is established.

With Moldova, the existing G7 Rapid Response Mechanism joint monitoring of the October 2025 parliamentary elections is the operational foundation; the recommendation is to formalise the RRM-Moldova relationship as the Canadian flagship case for the Information Peacekeeping doctrine in operational application, with the Swedish Psychological Defence Agency's information campaign training deck, currently in use in Moldova in Romanian translation, as the model of cooperation Canada should join through CCDA programming. The broader cohort of frontline EPC participating states, without exhaustive listing, should be understood as a category of cooperation rather than a one-off, with Moldova and Armenia as the operational anchors and the cohort framing authorising future cooperation as the political-rhetorical work begun at Yerevan develops.

Recommendation 10: Create a doctrine of Free Press and Information Peacekeeping

Free Press at home and Information Peacekeeping abroad are two halves of one Canadian doctrinal commitment to the conditions under which truth-based deliberation is possible. The recommendation is to operationalise both halves as a single coherent doctrine, with the domestic substrate authorising the international articulation, and the international articulation giving the domestic substrate strategic ambition.

The domestic foundation: Free Press as cognitive defence infrastructure. Canada's free press is the substrate that authorises the doctrinal contribution. Without a sustained, locally-rooted Canadian information ecosystem that can model what truth-based information operations look like, the Information Peacekeeping doctrine has no operational credibility. The empirical case for action is now sharply documented. The *Lost Estate*, the February 2025 Public Policy Forum analysis, found 526 outlet closures across 347 communities since 2008, with about half of the closures concentrated in communities of 20,000 people or fewer; 402 new outlets opened across the same period, of which 274 survive.[39] These are not journalism deserts. They are information vacuums adversaries fill. Civil society has documented the wound; this report names the predator. The Centre for Media, Technology and Democracy's AI News Audit of March 2026 adds a second dimension. Testing four major AI models against 2,267 real Canadian news stories drawn from the models' training data, the audit found that AI models provided no source attribution 82 per cent of the time, and that when given web access the same models substituted for original reporting in 54 to 81 per cent of cases.[40] Canada's Layer 2 problem is not only that local journalism is disappearing through closure. Where journalism is still produced, AI systems are distributing it without attribution in ways that degrade the economic foundation of the outlets producing it. The source of trusted information is being hollowed out through substitution as well as through closure.

Five operational interventions follow. First, the federal Local Journalism Initiative should be reconceived as a Report-for-Canada-style multi-year programme with matched philanthropy and an arm's-length board, lifting it out of the year-to-year programme cycle and giving it the institutional architecture sustained civic journalism requires. Second, federal legislation should mandate a 120-day sales notice period before the closure or non-local sale of any local news outlet, allowing community alternatives to organise. Third, federal and provincial governments should commit a defined percentage of advertising spend to locally-owned independent media, taking the Government of Ontario's July 2024 25 per cent commitment as the working precedent.[41] The Sygutek class action against Google and Meta, filed for C$8 billion across multiple jurisdictions, is the litigation complement to the legislative recommendations. Fourth, Canada's international information presence requires reinvestment: Radio Canada International,

drawing on McMahon's framework, should be rebuilt as a multilingual evidence-based journalism platform with fact-checking partnerships and a CBC reform mandate that ends advertising dependence, modelled on the BBC World Service. Fifth, all five interventions should be funded under the 1.5 per cent defence-and-security-related envelope, alongside the architectural recommendations above. Investment in the Free Press is investment in democratic defence infrastructure, not cultural policy or social policy that competes with security for resources.

The international articulation: Information Peacekeeping as the Canadian doctrinal contribution. Canada has the doctrinal capacity to articulate Information Peacekeeping as a coherent doctrinal contribution to like-minded democracies and to frontline EPC partners. The Information Peacekeeping concept was introduced by Robert Garigue at the Canadian Department of National Defence in 1993 and developed in the contemporary cyber-age context by Dave McMahon; what this recommendation articulates as the Canadian doctrinal contribution is the pairing of Information Peacekeeping abroad with Free Press at home as two halves of a single doctrinal commitment, developed below.[42] Lester B. Pearson's contribution was a doctrine the world needed and that only a middle power positioned between great powers and committed to multilateral institutions could plausibly articulate. Information Peacekeeping is the same kind of contribution. It is a doctrine for democracies that need to defend their information environments without ceding the political legitimacy that distinguishes them from the regimes attacking those environments. Three operational components define it. First, open-source-only methodology, with classified intelligence kept separate, so that the doctrine is publicly defensible and exportable. The Rapid Response Mechanism is the natural Canadian institutional home for the personnel pipeline because RRM analysts hold the classified clearance required to read upstream intelligence and translate it into open-source-defensible products. Second, principled institutional separation: cognitive defence capability built inside military command, without clear legal limits on domestic application, has in multiple democracies seen its mandate expand to fill the operational space available, with public backlash and erosion of trust as the cost. The structural remedy is institutional separation, not better instructions. Third, credibility as a strategic asset: truth-based information operations are not only ethically correct, they are

strategically superior, because nations that engage in disinformation degrade their own ability to communicate truthfully when it matters most. The Ukraine contrast is the empirical case: Ukraine does not lie online because it needs to be trusted, and its adversary provides real war crimes daily.

The doctrinal articulation should be operationalised through three named institutional channels. First, the Canadian Cognitive Defence Agency proposed in Recommendation 8, as the public-facing institutional home for the doctrine. Second, the partnerships set out in Recommendation 9, with Moldova as the operational flagship and Armenia as the second anchor. Third, like-minded democracy forums beyond the Alliance, including the Media Freedom Coalition, the Summit for Democracy follow-on architecture, and the OECD's information integrity work. Canadian doctrine that is not articulated to like-minded democracies and Alliance partners does not travel; the doctrine that travels shapes the international cognitive defence architecture being built now.

Free Press at home and Information Peacekeeping abroad are not two recommendations. They are the two operational halves of the same Canadian commitment to the conditions of truth-based democratic deliberation, at home and beyond.

A coherent architectural package

These ten recommendations span the framework's full architectural arc. Recommendation 1 completes the operational layer through continuous Rapid Response Mechanism Canada detection, attribution authority, and the operational tempo VIGINUM has established as the Alliance reference standard. Recommendation 2 closes the foreign intelligence gap that Chapter 9 identified as Canada's most acute single capability deficit and the precondition for almost everything else this chapter recommends. Recommendation 3 modernises the Communications Security Establishment as the upstream technical fusion centre that feeds the operational mandate above it. Recommendation 4 builds the regulatory architecture for data sovereignty and platform accountability before the CUSMA review window closes. Recommendation 5 builds the digital sovereignty infrastructure on which the regulatory architecture depends. Recommendation 6 establishes the cognitive defence coordination architecture across federal, provincial, territorial, Indigenous, and municipal levels of government, and across

the political and working levels of the federal architecture itself. Recommendation 7 treats emotional self-regulation and the Layer 1 social infrastructure on which it rests as cognitive defence infrastructure on the same fiscal footing as the institutional architecture above. Recommendation 8 establishes the Canadian Cognitive Defence Agency as the public-facing institutional home for the architecture and the synthesising institution Canada's cognitive defence most lacks. Recommendation 9 builds the European cognitive defence partnerships through which Canadian cognitive defence operates beyond Canada's own borders. Recommendation 10 pairs Free Press at home with Information Peacekeeping abroad as the doctrinal contribution the rest of the architecture is built to carry.

The fiscal architecture exists. The 1.5 per cent defence-and-security-related envelope of the NATO 3.5-plus-1.5 commitment is the funding instrument under which the institutional architecture, the Layer 1 investment, and the Free Press interventions can all be resourced as the defence-and-security-related investment they are. The political authorisation exists in the March 26, 2026 announcement on continuous Rapid Response Mechanism detection, the *Strong and Free Elections Act*, the Cabinet Directive on the Coordinated Response to Threats to Elections, and the Defence Industrial Strategy. The partnership architecture exists in the seven domains of strategic autonomy Prime Minister Carney named at the European Political Community Summit in Yerevan on 4 May 2026, to which cognitive sovereignty should be added as the missing eighth. What remains is the institutional decision to use these instruments at the scale the threat environment requires.

The corridor architecture proposed in Chapter 13 is the partnership through which Canada operationalises this moment with Germany and the European Union. The recommendations in this chapter are the institutional foundation that makes the corridor possible.

Closing

The Canadian doctrinal contribution articulated in Recommendation 10, Free Press at home and Information Peacekeeping abroad as two halves of one commitment to the conditions of truth-based deliberation, is the export the Pearson lineage authorises

Canada to articulate to like-minded democracies and beyond. The partnership architecture in which that contribution travels is the one Prime Minister Carney has spent his first year in office building: France, the European Union, Ukraine, the Nordic Five, Poland, the Baltic Three plus One, the United Kingdom through the Joint Expeditionary Force, and the frontline EPC democracies of Moldova and Armenia.

Canada is the furthest behind among the developed democracies studied for this report. The gap is operational, not conceptual. Because Canada has yet to establish coordinated cognitive defence architecture, it has the rare advantage of learning from its partners and integrating the best of what each country has to offer while replicating none of them in full. The window is narrow. The moment is ripe for the taking.

Endnotes

1 Andrew Coyne, “Canada is uniquely unprepared for the dire national-security crisis we are now in”, *Globe and Mail,* February 6, 2026

2 Government of Canada, 'Government of Canada introduces measures to further protect Canada's electoral processes and strengthen democracy,' news release, 26 March 2026.

3 Government of Canada, *Security, Sovereignty and Prosperity: Canada's Defence Industrial Strategy*, launched by Prime Minister Mark Carney, Montreal, 17 February 2026.

4 Prime Minister of Canada, 'Prime Minister Carney announces Canada has achieved the NATO 2% defence spending target,' news release, 26 March 2026

5 See comparative literature on G7 intelligence architectures

6 Joshua van Es, *Provincial Data Sovereignty Exposure Index*, Upper Harbour Research, March 2026.

7 Shawn Donnan and James Politi, 'Silicon Valley Is Big Winner from Trump's New Trade Deal,' *Financial Times*, 2 October 2018; United States CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), Pub. L. 115-141, 2018.

8 Heidi Tworek and Alicia Wanless, 'How to Confront Canada's Digital Dependence,' CIGI, July 2025

9 Build Canada, 'A Blueprint for Canada's Digital Sovereignty,' 19 February 2026

10 Prime Minister of Canada, 'Prime Minister Carney announces Canada has achieved the NATO 2% defence spending target,' news release, 26 March 2026

11 Standing Senate Committee on National Security, Defence and Veterans Affairs, *Russia's Disinformation: Understanding the Challenge, Strengthening Canada's Response*, Senate of Canada, April 2026, Recommendation 6

12 Dave McMahon, ‘Cognitive War and Information Peacekeeping,’ Sapper Labs Group, 10 December 2021

13 'Cohere acquires, merges with Germany-based startup to create a transatlantic AI powerhouse,' *TechCrunch*, 24 April 2026

14 Government of Canada, *Security, Sovereignty and Prosperity: Canada's Defence Industrial Strategy*, 17 February 2026, Build-Partner-Buy framework and ten sovereign capabilities.

15 On France's Microsoft Teams and Zoom announcement, January 2026 reporting on French government plans for 2.5 million civil servants. On Schleswig-Holstein's open-source migration of 44,000 employee accounts, see government of Schleswig-Holstein press releases. On Austria's military shift to LibreOffice, see Austrian Federal Ministry of Defence releases. On the Dutch parliament's national cloud tender, see Dutch parliamentary documentation following the 67 per cent foreign-provider audit.

16 Field research synthesis with Renée Black, founder of Good Bot and previously founding Executive Director of PeaceGeeks, drawing on Good Bot's published work on platform accountability and her work with the Council on Technology and Social Cohesion.

17 Pranav Dixit and Jeff Horwitz, 'How Meta is making billions off scam ads,' *Reuters*, 6 November 2025, citing internal Meta documents from the company's finance, safety, engineering, and lobbying teams covering 2021 to 2025.

18 Estonian government press releases of 27 December 2019 and Estonian internal security service annual reports

19 Lauren Goode, 'Bluesky hits 40 million users, introduces dislikes beta,' *TechCrunch*, 31 October 2025

20 Andrew Coyne, 'MAGA's plan for Canada: not annexation, but dismemberment,' *The Globe and Mail*, 27 March 2026.

21 Jaxson Khan and Sean Mullin, *Sovereign by Design: Strategic Options for Canadian AI Sovereignty*, Munk School of Global Affairs and Public Policy, University of Toronto, March 2026.

22 Republic of Lithuania, Law on Intelligence, Articles 8 and 26, mandating annual public threat assessments by the State Security Department (VSD) and the Defence Intelligence and Security Service (AOTD)

23 Field research synthesis from senior practitioner analysis at the EEAS Strategic Communications and Foreign Information Manipulation and Interference Division

24 Field research synthesis from a senior Canadian clinical practitioner with extensive front-line trauma work in policing, education, and child welfare

25 David Coletto, *Canadians Are Living on Financial Alert as Tariff Turbulence Fuels the Precarity Mindset*, Abacus Data, 20 February 2026

26 Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, *Final Report* (Hogue Commission), January 2025.

27 Italian Defence Minister Guido Crosetto, presentation to the Italian Supreme Defence Council convened by President Sergio Mattarella, 17 November 2025.

28 Dave McMahon, ‘Cognitive War and Information Peacekeeping,’ Sapper Labs Group, 10 December 2021.

29 Martin Patriquin, *The Logic*, April 2026

30 Institute for Strategic Dialogue Canada, *Online Domestic Extremism Data Briefing, June to November 2025*, published 20 April 2026,

31 Prime Minister of Canada, “Prime Minister Carney strengthens trade and security partnerships with European nations,” news release, Yerevan, 4 May 2026

32 Prime Minister of Canada, “Prime Minister Carney to strengthen ties with France and the United Kingdom and reaffirm Canada’s sovereignty,” news release, 15 March 2025

33 New EU-Canada Strategic Partnership of the Future and the Canada-EU Security and Defence Partnership, announced 23 June 2025

34 Prime Minister of Canada, “Prime Minister Carney announces new contribution to support Ukraine’s defence,” news release, Yerevan, 4 May 2026

35 Prime Minister of Canada and Government of Norway, joint communiqué from the Canada-Nordic Summit, Oslo, 15 March 2026

36 Field research synthesis with a Royal Danish Defence College source, identifying the Canadian Rangers as a model under active study by Denmark and Greenland for what is tentatively termed Green Valley Rangers, with a specific report on lessons learned from the Canadian model in preparation at time of interview.

37 Prime Minister of Canada, “Joint statement on enhancing the Canada-Poland strategic partnership,” Warsaw, 25 August 2025

38 Prime Minister of Canada, “Prime Minister Carney participates in the virtual meeting of the Joint Expeditionary Force,” readout, 26 March 2026

39 Andrew Phillips, Edward Greenspon, and Alison Uncles, *The Lost Estate: How to Put the Local Back in Local News*, Public Policy Forum, Rideau Hall Foundation, and Michener Awards Foundation, 12 February 2025, https://ppforum.ca/publications/local-news-canada/.

40 Taylor Owen and Aengus Bridgman, *AI News Audit: AI, Canadian Journalism, and Paths for Policy Action*, Centre for Media, Technology and Democracy, McGill University, March 2026.

41 Government of Ontario, ministerial directive on local media advertising spend, July 2024.

42 Dave McMahon, ‘Cognitive War and Information Peacekeeping,’ Sapper Labs Group, 10 December 2021

Chapter 16: Recommendations for the European Union

The recommendations that follow in this chapter are drawn directly from our previous analysis, from the field research conducted across EU and NATO institutional contexts. They are presented as a consolidated action set for EU institutions and member states

The strategic context for these recommendations is a moment of unusual opportunity. Stewart Patrick's analysis of the middle power moment argues that when great power leadership recedes, minilateral coalitions among capable democracies become the most productive vehicle for advancing collective goods. Toygur and von Ondarza frame EU-Canada relations explicitly as a strategic response to US unreliability, with the language of like-minded middle powers building democratic resilience together. The EU, in this reading, is not merely a regulatory body but the anchor institution of the democratic middle power coalition.[1] The recommendations that follow are arguments for using the instruments already built, at the scale the moment demands.

Recommendation 1: Resource the Regulatory Architecture

The Digital Services Act and Digital Markets Act are not self-executing. Enforcement requires national digital services coordinator capacity that most member states do not have. Fund national digital services coordinator capacity as a strategic EU investment. The TikTok non-compliance decision on addictiveness is the precedent to extend. Where platform business models produce anti-democratic outcomes, fines are insufficient.

The European Fact-Checking Standards Network's Great Retreat white paper, documenting the withdrawal of Google, YouTube, and LinkedIn from the Code of Conduct on Disinformation following the 2024 US election, closes the debate on voluntary self-regulation.[2] The Code was structurally vulnerable because shared goodwill cannot be mandated, and geopolitical shifts will always affect voluntary engagement. The EU must embed civil society formally in the enforcement process, contracting public-interest technologists for specific projects rather than consulting them. Private enforcement is structurally underfunded. Make private enforcement as accessible as possible through structural funding support.

Press freedom protection is the regulatory arc's third leg. The European Media Freedom Act, in force since August 2025, addresses the kind of state media consolidation

documented in Hungary, where government-aligned ownership was used to convert independent outlets into vehicles of political propaganda. The instrument exists. The implementation capacity at member-state level is uneven. Resourcing media-pluralism monitoring, source-protection enforcement, and cross-border editorial-independence cooperation is the missing operational layer beneath the EMFA's regulatory framework.

Recommendation 2: Operationalise the FIMI Deterrence Playbook

The FIMI Deterrence Playbook, published March 2026, is the strongest argumentative foundation for EU cognitive-defence ambition. The Playbook positions the EU's response architecture as implementation rather than as new architecture. The instruments already exist, and the recommendation is to use them at the scale the threat environment requires. Resource the Playbook at operational scale. The architectural separation of regulation and disruption into two distinct pillars, currently under active EEAS consideration, should be supported. Having them in one pillar is intellectually muddled because the DSA serves regulatory accountability purposes that have little to do with disruption operations.

The sword framing requires the operational capabilities a sword implies. Apply deterrence-by-punishment practices across the Playbook by ensuring fast and clear attribution, imposing predictable and visible costs through sanctions, responding rapidly and across domains, and acting consistently and collectively to build credibility and raise the cost of hostile information operations. The hybrid sanctions regime including FIMI entities is the precedent to extend.

Recommendation 3: Sharpen the FIMI Toolbox

The Estonia Sputnik closure model is the most precise available example of creative use of existing legal tools. Estonia used existing EU sanctions on Dmitri Kiselev from 2014 to close the Sputnik office by arguing that paying wages and rent created revenue for a sanctioned entity, with no broadcast ban, no content-based decision, and no successful legal challenge. The EU should actively circulate this model to member states as a template for action within existing law. At the EU level, the structural improvement requiring no new legislation is to build a formal channel connecting FIMI exposure work to law-enforcement and sanctions-compliance mechanisms. Some FIMI operations are

powered by illicit funding, money laundering, and sanctions circumvention, and those financial trails are already within scope of existing enforcement powers.

A formal entry-ban architecture for individuals materially involved in cognitive operations against EU member states would close the gap between attribution and personal consequence. The architecture exists in principle through existing Schengen instruments. The application to FIMI is what has not yet been built. The data layer underneath the regulatory and counter-FIMI architectures is also inadequately protected. If data protection rules are not properly enforced, interoperability remedies and competition interventions are built on sand.

Recommendation 4: Close the Domestic Gap

FIMI was developed as an external threat concept. The EU has no clear institutional owner for the domestic information environment. The European Centre for Democratic Resilience should become that owner, with genuine political weight to coordinate across Directorates-General. Its mandate should be consolidation: bringing existing programmes under a single accountability structure rather than layering new bodies on top of them. If the European Centre for Democratic Resilience were to “own” the domestic information environment, it should act as a central operational hub by providing real-time monitoring and early warning, coordinating responses across the EU and Member States, supporting attribution, guiding strategic communication, working with platforms, and strengthening national capacities and societal resilience.

The Centre’s value is coordination. Diaspora communities remain outside the primary EU attention on FIMI. The Sweden Muslim community gap illustrates the rupture point adversaries exploit when diaspora communities are left unprotected. The Centre's founding mandate should include diaspora-targeted FIMI explicitly. This matters equally for Canada-EU coordination given Canada's significant diaspora communities.

The European Centre for Democratic Resilience should anchor a coordinated civil society funding mechanism operating on three distinct tracks, each with its own legal basis. The first track funds EU member state civil society actors directly. The second funds civil society actors in non-EU countries under existing EU external action instruments, making organisations like those operating in Ukraine, the Baltic states, and partner democracies

eligible without requiring their governments to be formal participants. The third enables structured cooperation with like-minded partners including Canada, the UK, and Norway through equivalence frameworks and co-financing arrangements, allowing non-EU governments to contribute to and benefit from the mechanism without it operating as a NATO funding substitute. This three-track architecture is a legal necessity.

The US withdrawal has eliminated approximately $268 million in annual counter-disinformation and press freedom funding globally. The cost of replacement, distributed across EU member states and like-minded partners through co-financing arrangements, is fiscally manageable. The harder problem is institutional: avoiding duplication with existing EU instruments, preventing politicisation of funding decisions, and designing decision cycles fast enough to match the operational tempo of the threat.

The Centre should be explicit about what this mechanism is and is not. It is an EU external action instrument with partner participation, not a NATO funding substitute. And it is a response to a documented operational gap, not a new institutional layer.

Recommendation 5: Build the External Coalition

The EU's regulatory power in the cognitive domain derives from market size. Platforms comply with the DSA and DMA because of the cost of losing access to 450 million consumers. That logic becomes more powerful, and the EU's anchoring role more credible, if the regulatory perimeter is deliberately extended to partner democracies. Canada, the United Kingdom, Norway, and other like-minded democracies that implement DSA-equivalent platform-accountability rules, DMA-equivalent gatekeeper obligations, AI Act-equivalent transparency requirements, and Democracy Shield-equivalent counter-FIMI architecture should be treated as part of the EU's regulatory jurisdiction for enforcement purposes. The EEA model, the GDPR adequacy framework, and the UK data adequacy arrangement all establish the precedent.

The realistic pathway is structured regulatory cooperation rather than full adoption. Pair this with a joint research-funding commitment, co-funding a programme through a designated Canadian institution targeting the detection, attribution, and resilience-measurement gaps both sides have identified.

This chapter recommends that Canada place a secondee in the EEAS counter-FIMI policy and partnerships division, following the precedent of two consecutive US transatlantic fellows in the same unit. The EU should actively welcome and facilitate this by designating a named point of contact within the division, confirming the institutional framework for the placement, and treating the secondee as a substantive analytical partner rather than as an observer.

Recommendation 6: Build the Layer 1 Foundation

The European Union has not yet built the social-infrastructure foundation that effective cognitive defence requires. The European Union's role in the Layer 1 foundation is not to build social infrastructure directly, which is a member-state competence, but to resource and coordinate the member-state institutions that build it, and to set the standards against which that work is measured. Naming the Layer 1 foundation explicitly as a defence against the conditions cognitive operations exploit is the framing the moment requires. Sauli Niinistö's report on EU comprehensive security, commissioned by the European Commission and published in October 2024, formally recommended the Finnish comprehensive security model as a European template.[3] Niinistö's central finding is that resilience cannot be assembled in crisis. It must be built deliberately, in peacetime, across the full span of social, civic, and institutional infrastructure. The Finnish model, anchored in *kokonaisturvallisuus* (comprehensive security) and operationalised through standing whole-of-society arrangements, is the institutional reference. The EU has received the recommendation. It has not yet built the infrastructure.

The institutional model the European Union already partly contains is Germany's BZpB, the only institution in any democracy specifically designed around the lived experience of what state propaganda can do to a population. The BZpB should be positioned as the institutional model for an EU-wide network of comparable Layer 1 institutions, leveraging other federally funded political foundations' existing transnational networks, and building the European political-education infrastructure that the Niinistö Report has formally recommended.[4]

The Layer 1 ask is operationalised through three concrete components. First, establish the Democracy Shield's emotional regulation and digital literacy infrastructure as a

standing programme rather than as a project portfolio. Second, embed civic education investment as part of the Democratic Regulatory Partnership Framework so that partner democracies adopting EU-equivalent regulatory standards also build complementary Layer 1 architecture. Third, establish member-state political-education infrastructure as a Democracy Shield component, with funding flowing through the Centre for Democratic Resilience. The BZpB is the model. The EU funding architecture is the mechanism through which the model becomes European infrastructure.

A Coherent Architectural Package

These recommendations span the framework's full architectural arc. The instruments exist. The political authorisation exists in the form of the FIMI Deterrence Playbook, the Democracy Shield, the Niinistö Report, and the Security and Defence Partnerships. What remains is the operational scale at which the EU is willing to use the instruments.

The corridor architecture proposed in Chapter 13 is the partnership through which the EU operationalises this moment with Canada and Germany. The recommendations in this chapter are the institutional foundation that makes the corridor possible. The EU has the regulatory power, the convening authority, the institutional reach, and the strategic logic. What it has lacked is the political will to use them at the scale the threat environment requires.

Endnotes

1 Stewart Patrick, 'The Middle Power Moment: A Strategy for the Coming Multipolar World', Carnegie Endowment for International Peace, 2025, carnegieendowment.org.

2 European Fact-Checking Standards Network, *The Great Retreat*, policy white paper, EFCSN, 3 March 2026, efcsn.com

3 Sauli Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, report by the Special Adviser to the President of the European Commission, European Commission, October 2024 (

4 See Chapter 14, Recommendation 7

Chapter 17: Recommendations for Democratic Cooperation

The 1956 Pearson report argued that NATO existed to create the conditions under which democratic governance could sustain itself. Collective defence, in his formulation, was ultimately the defence of a community of shared values, and the binding obligation among members was the obligation to treat an attack on one as an attack on all.[1] NATO's motto 'Stronger Together' remains true today. The charter tenets stand. In today's day and age, democracies cannot survive unless they take the threat of cognitive warfare seriously and actively instead of passively. The pillars of democracy rest on the ground that cognitive warfare is currently destroying.

The cognitive defence architecture this report has set out is built on the recognition that democratic resilience is what Veronica Anghel and Erik Jones have called a common-pool resource: a good that is rivalrous because the capacity to defend it is finite, and non-excludable because cognitive attacks on one democracy create vulnerabilities in all of them.[2] The only way to preserve such a resource is through governance structures that impose shared responsibility on all who have access. The recommendations in this chapter set out the architecture through which democracies can act on that responsibility together.

Six recommendations follow. They are not a coalition design proposal. The coalition the recommendations address is the community of shared values that the charter tenets already name and that the manuscript has set out in full: any liberal democracy that shares the political identity NATO was founded to defend, and the willingness to act on it. These recommendations do not cover every actor and every dimension that this work requires. They are the institutional foundation on which broader cooperation can build, and they identify the architecture that already exists and is closest to operational use. What follows are recommendations for the broad-based democratic cooperation against cognitive warfare that this report has set out to advance.

Recommendation 1: Operationalise the FIMI ISAC and the European Centre for Democratic Resilience as the architecture of collective democratic cognitive defence

The institutional architecture this work requires already exists at EU level. The European External Action Service Information Integrity and Countering FIMI Division is the convening authority.[3] The FIMI Information Sharing and Analysis Centre, announced by High Representative Borrell on 7 February 2023 and now operational, is the working-level mechanism through which member-state agencies, partner-democracy agencies, and civil society organisations share evidence, methodology, and attribution.[4] The European Centre for Democratic Resilience, announced in November 2025 as a core component of the European Democracy Shield, is the coordination hub through which the FIMI ISAC architecture and the wider counter-FIMI cooperation now run.[5]

The recommendation is that this architecture become the architecture of collective democratic cognitive defence. The EEAS Information Integrity and Countering FIMI Division should be the convening authority. The FIMI ISAC should be the working-level operating system. The European Centre for Democratic Resilience should be the coordination hub. Canada, the United Kingdom, Norway, Ukraine, along with the Indo-Pacific partner democracies of Australia, Japan, South Korea, and New Zealand, should participate on the substantive terms already piloted bilaterally, with further partner democracies welcomed on demonstrated alignment with the architecture's working principles. The Canadian secondment to the EEAS counter-FIMI policy and partnerships division, recommended in Chapter 15 and proposed by the EU as a substantive analytical placement rather than an observer arrangement, is the working precedent for what full partner participation looks like operationally.[6]

Three operational components follow. First, partner democracies should adopt the FIMI Toolbox as the shared methodological framework for attribution, exposure, and cost imposition.[7] The Toolbox is the most fully developed counter-FIMI methodology in any democracy, and the working assumption should be that members align to it rather than build parallel methodologies. Second, a standing working-level cadence should be established at the FIMI ISAC convening, anchored on the Threat Analysis Cycle and the

Response Cycle that the ISAC has already developed, with quarterly ministerial-level reporting through the convening authority to keep political authorisation continuous rather than episodic.[8] Third, joint attribution and exposure table-top exercises on adversary networks operating across multiple jurisdictions, with the Doppelganger and Portal Kombat networks as the immediate operational subjects, should be the first collective product. The Information Manipulation Sets framework developed by EU DisinfoLab's working group in January 2026, which proposes a structured method for collective attribution across overlapping operational ecosystems, is the methodological substrate this work can build on.[9] Joint attribution carries more deterrent weight than any single state's attribution carries on its own.

Recommendation 2: Extend the EU regulatory perimeter to like-minded partner democracies

Chapter 16's External Coalition recommendation sets out the Democratic Regulatory Partnership Framework as the mechanism through which the EU extends its regulatory perimeter to like-minded partner democracies on platform accountability, AI transparency, and counter-FIMI architecture.[10] The recommendation here is that this framework be the regulatory foundation of collective democratic cognitive defence. Partner democracies that implement Digital Services Act-equivalent platform-accountability rules, Digital Markets Act-equivalent gatekeeper obligations, AI Act-equivalent transparency requirements, and Democracy Shield-equivalent counter-FIMI architecture should be treated as part of the collective regulatory jurisdiction for enforcement purposes. The EEA model, the General Data Protection Regulation adequacy framework, and the UK data adequacy arrangement together establish the legal precedent for extending EU regulatory perimeter beyond EU borders, though each operates on a narrower regulatory scope than the Framework would require.

The strategic logic is the logic we presented previously. Platform compliance with EU regulation reflects the cost of losing access to 450 million consumers. That logic becomes more powerful, and the regulatory anchor more credible, when the perimeter expands to encompass partner-democracy markets. A perimeter that has aligned its platform-accountability rules across the EU, the UK, Canada, Norway, the Indo-Pacific partner democracies, and Ukraine reaches an addressable population at which platforms have

no economically viable option other than compliance. The Digital Services Tax episode of June 2025, when Canada rescinded its digital sovereignty instrument under US pressure within ninety days of enactment because the instrument was not embedded in collective architecture, is the negative case that demonstrates the recommendation. Sovereignty instruments not embedded in collective architecture are tradeable. Sovereignty instruments embedded in collective architecture are not.

Recommendation 3: Adopt whole-of-society security frameworks that name the cognitive domain

Each democracy should commit to a total defence or whole-of-society security framework that explicitly names the cognitive domain among its constitutive elements. The Finnish concept of *kokonaisturvallisuus* (comprehensive security), the Swedish and Norwegian total defence models (*totalförsvar* and *totalforsvar*), the Estonian, Latvian, and Lithuanian comprehensive defence frameworks, the Ukrainian wartime version forged under live cognitive warfare, and the framing of European comprehensive security set out in the Niinistö Report of October 2024 are among the institutional references the manuscript has developed.[11] Each is a national model that has developed in its own constitutional and political context. The common thread is that resilience cannot be assembled in crisis. It must be built deliberately in peacetime, across the full span of social, civic, and institutional infrastructure, with the cognitive domain treated as constitutive of the security architecture rather than as a sectoral specialism adjacent to it.

The substantive case rests on the report's central finding that cognitive defence is multilayered, and that no operational, intelligence, or regulatory layer can substitute for the foundational layer of civic and epistemic infrastructure on which democratic deliberation depends.[12] An architecture that builds its operational and regulatory layers without naming and resourcing this foundation has built the upper floors of a building whose foundations are still being laid. Germany's Bundeszentrale für politische Bildung, developed in the chapter on Germany's recommendations, is the most developed example of standing civic-education infrastructure in any comparator democracy and has spent seven decades publicly funding civic education and democratic literacy as a standing government obligation.[13] Denmark's 180-year foundation-layer architecture, comprising the folk high school heritage, the associational tradition, the Klassens Tid

practice within the *Folkeskole*, the *almene boliger* housing system, the *bofællesskab* cohousing tradition, and the *Cities for People* public-space architecture, is the most comprehensive Layer 1 social-infrastructure foundation in this research set.[14] Each democracy should build the equivalent in its own institutional context. The recommendation here is not that democracies adopt a single institutional template but that each names the cognitive domain and the Layer 1 social-infrastructure foundation as two distinct elements of its whole-of-society security framework, and resources both accordingly.

Three operational principles follow. First, each democracy should publish, review, and resource its whole-of-society security framework on a defined cadence that treats the framework as a standing institutional obligation rather than as an episodic political product. Second, the cognitive domain should be named within these frameworks alongside the conventional, cyber, economic, and hybrid domains, rather than folded into one of them. Third, the social-infrastructure foundation that cognitive defence requires should be funded as a security investment rather than as a discretionary civic expenditure, with the standing institutional architecture each democracy chooses reflecting its own constitutional, political, and cultural context.

Recommendation 4: Treat defence-industrial cooperation as cognitive sovereignty

The dependency logic this report has developed across the energy, telecommunications, rare-earths, and financial systems domains applies equally to defence procurement. Authoritarian states weaponise economic and energy dependency as a coercion vector. A democracy that sources its military hardware exclusively or predominantly from a single great power, or from partners outside its core alliance architecture, has created a dependency that adversaries can exploit and that undermines the political will to act independently in crisis. Defence-industrial diversification is not merely an economic or industrial policy question. It is a cognitive sovereignty question, because the dependency a state carries on its procurement architecture is the dependency adversaries will leverage to fracture democratic cohesion under pressure.

The operational consequence is that defence-industrial cooperation among democracies should be treated as cognitive defence infrastructure, with the same analytical seriousness given to the operational and regulatory layers. The European Security Action

for Europe instrument, which Canada became the first non-European member of in February 2026, is the working architecture for this dimension.[15] SAFE is currently configured for capability development. The recommendation is that its scope extend explicitly to the cognitive defence dimension of defence-industrial cooperation, including the dual-use AI-integrated defence-system architecture that is now the leading edge of the European defence-industrial base. The Saab Gripen E platform's integration of Helsing's Centaur AI agent, which completed its first three test flights in 2026 and embeds German AI capability directly into Swedish airframes, is the operational demonstration: European defence procurement carrying advanced AI and cognitive-warfare capability into the platform rather than alongside it.[16] Defence procurement aligned with this architecture builds collective cognitive defence capacity as a byproduct. Defence procurement not aligned with this architecture builds dependencies democracies cannot afford.

Recommendation 5: Sustain the American democratic ecosystem as a collective commitment

The current American administration is not the American democratic ecosystem. American civil society organisations, researchers, and practitioners working on cognitive defence, democratic resilience, and information environment integrity remain among the most capable actors in the field. They are active participants in the NATO cognitive warfare architecture, in the FIMI ISAC defender community, and in the bilateral working-level relationships that political disruption at the federal level has not severed. The Atlantic Council's Digital Forensic Research Lab, the German Marshall Fund's Alliance for Securing Democracy, the Carnegie Endowment's Information Environment Project, the University of Washington's Center for an Informed Public, the Institute for Strategic Dialogue's US programme, and the Stanford Internet Observatory's successor architectures are among the working-level institutions through which American counter-FIMI capacity continues to operate, in many cases under significant federal-government pressure.

The collective response to American political unreliability at the federal level should include active investment in the American democratic ecosystem at every other level. That includes sustained working-level relationships between allied agencies and

American civil society organisations. It includes member-state funding for American research consortia where federal funding has been withdrawn or politicised. It includes the principled refusal to treat American withdrawal from the institutions the United States built as the position of the American people. The long game is not to replace the United States in the liberal order. It is to hold the space, with the American democratic ecosystem inside the working architecture, until American democratic politics reconstitutes itself.

The operational principle is that collective cognitive defence cooperation should continue to include American counterparts where they are willing and able to participate, on a working-level basis, regardless of federal-government posture. The institutional posture toward the United States should distinguish between the administration and the ecosystem. The administration is one actor whose posture has shifted. The ecosystem is the broader and more durable American commitment to democratic governance that the charter tenets exist to defend.

Recommendation 6: Treat Ukraine as the operational anchor

Ukraine is the most operationally experienced democracy in cognitive defence in the present international system. The Ukrainian Centre for Countering Disinformation under the National Security and Defence Council, the Ministry of Digital Transformation's Diia application with its wartime functions including the eVorog reporting system, the volunteer-led open-source intelligence and detection networks, and the institutional architecture coordinating Ukraine's information operations under conditions of intense active cognitive warfare together constitute a national cognitive defence ecosystem that no comparator democracy has yet matched in operational maturity or population-level integration. The Ukraine Communications Group, currently the only operational coalition coordination format on a specific cognitive defence portfolio that has demonstrated working-level coordination among democracies without United States participation, is the proof of concept for what working-level allied coordination produces.[17]

The recommendation is that Ukraine be treated as the operational anchor of collective democratic cognitive defence, not as an observer, not as a recipient of capacity building, and not as a peripheral participant. Two operational components follow. First, Ukraine should be a founding partner in the FIMI ISAC and the European Centre for Democratic Resilience on equal terms with EU member states and partner democracies. The

institutional precedent for Ukraine on equal footing with member states already exists in the NATO-Ukraine Council established at the Vilnius Summit in July 2023, and in Ukraine's operational participation at the March 2026 EEAS FIMI Conference at senior operational level. The recommendation here is that the FIMI ISAC and the European Centre for Democratic Resilience extend the same institutional recognition. Second, the doctrinal architecture of collective cognitive defence should incorporate Ukrainian operational experience as a foundational empirical input rather than as a peripheral case study or as wartime contingency. The institutional pathways each democracy takes will reflect its own constitutional, political, and cultural context. What the coalition should commit to is the recognition that Ukraine's innovations are foundational evidence for the cognitive defence field.

The Ukrainian position is structurally different from any other partner-democracy position. Ukraine is the democracy that has been most directly tested by the cognitive warfare democracies exist to defend against, and the democracy whose practitioners have the deepest operational experience in successful response. Treating Ukraine as the operational anchor is the institutional acknowledgement of that empirical reality.

A coherent architectural package

These six recommendations span the architecture democracies acting together require for collective cognitive defence. Recommendation 1 operationalises the institutional system through the EEAS, the FIMI ISAC, and the European Centre for Democratic Resilience. Recommendation 2 builds the regulatory foundation. Recommendation 3 commits each democracy to a whole-of-society security framework that names the cognitive domain. Recommendation 4 extends cognitive sovereignty to the defence-industrial domain. Recommendation 5 sustains the American democratic ecosystem as a collective commitment in the face of federal-government withdrawal. Recommendation 6 anchors the architecture on Ukrainian operational experience.

The instruments exist. The institutional architecture exists. The political authorisation exists in the form of the FIMI Deterrence Playbook, the Democracy Shield, the Niinistö Report, and the Security and Defence Partnerships. What does not yet exist, in the configuration this contest requires, is the collective decision among democracies to use

them at the scale the threat environment demands. The recommendations above are the institutional content of that decision.

Prime Minister Carney has named the strategic condition: democracies must be masters in their own home. Nowhere is more our own home than our own hearts and minds. Cognitive defence is the defence of that home, and democracies can only hold it together.[18]

Endnotes

1. The 1956 Pearson report on the non-military cooperation of the North Atlantic Alliance, produced by Lester B. Pearson of Canada, Gaetano Martino of Italy, and Halvard Lange of Norway as NATO's Three Wise Men.

2. Veronica Anghel and Erik Jones, *From Club to Commons: Enlargement, Reform and Sustainability in European Integration*, Elements in Economics of European Integration (Cambridge University Press, 2025), doi.org/10.1017/9781009499194.

3. European External Action Service, Information Integrity and Countering FIMI Division, institutional documentation at eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en..

4. Josep Borrell, High Representative/Vice-President of the European Union, announcement of the FIMI Information Sharing and Analysis Centre at the EEAS Conference on Foreign Information Manipulation and Interference, 7 February 2023.

5. See Chapter 16, Recommendation 5.

6. See Chapter 15 Recommendation 9 (the EU section) and Chapter 16 Recommendation 5.

7. European External Action Service, FIMI Toolbox, institutional documentation at eeas.europa.eu. The Toolbox includes short-, medium-, and long-term measures from prevention to reaction, organised around the Threat Analysis Cycle and the Response Cycle.

8. EEAS, *First EEAS Report on Foreign Information Manipulation and Interference Threats*, 2023, and *Second EEAS Report on Foreign Information Manipulation and Interference Threats*, January 2024

9. EU DisinfoLab, *Building a Common Operational Picture of FIMI: The Information Manipulation Sets Framework*, working group report, January 2026, disinfo.eu.

10. See Chapter 16 Recommendation 5.

11. Sauli Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, report by the Special Adviser to the President of the European Commission, European Commission, October 2024.

12. See Chapter 5 (the six-layer cognitive defence framework) and Chapter 15 Recommendation 7

13. See Chapter 14 (Germany) Recommendation 7; see also Chapter 16 Recommendation 6

14. See Chapter 22, Denmark.

15. See Chapter 15 Recommendation 9 (the EU section) and Chapter 13.

16. Canadian Defence Review, November 2025; Saab CEO Micael Johansson, investor call, Breaking Defense, 5 February 2026

17. Field research synthesis at the EEAS Hybrid Threats and Cyber Division; see Chapter 15 Recommendation 9 (the Ukraine section).

18. Prime Minister Mark Carney, post-swearing-in press conference, Rideau Hall, Ottawa, 14 March 2025.

Conclusion

Cognitive warfare does not announce itself. It does not arrive with a declaration, a border crossing, or an event that triggers the institutional response mechanisms that democratic societies have built over eighty years of collective security. Rather, it metastasizes through the accumulation of small degradations. It happens when a population trusts its institutions a little less. Or when the shared information environment feels a little more unreliable. Or when the political class finds consensus a little harder to reach, and then harder still. It calls in to question longstanding allied relationships. None of these conditions, taken alone, crosses a threshold. Taken together, over time, they constitute a strategic defeat without a battle.

This report has argued that the defeat is not inevitable. The fifteen countries and within EU and NATO institutions have demonstrated, each in their own way and at different stages of development, that cognitive defence is buildable. Finland built it through eight decades of investment in social cohesion and critical thinking, beginning before the threat had a name. Estonia built it through the experience of occupation and the deliberate choice to make that experience the foundation of a security culture rather than only a wound. Lithuania built it through institutional innovation, a calibrated narrative response architecture that other democracies are now studying and adapting. Ukraine is building it, at existential cost, in real time, and demonstrating that a population with coherent identity and genuine political will can resist an adversary with vastly superior kinetic resources. The framework is not theoretical. It has been built. The question is whether Canada, Germany, and their democratic allies will build it in time.

The finding across all fifteen countries is consistent. No democracy has all six layers of cognitive defence functioning at full capacity. The Nordic and Baltic democracies come closest, and they share a common explanation: they treated the social infrastructure beneath the operational layers, the emotional regulation, the civic identity, the institutional trust, not as a precondition they could assume but as an investment they had to make, deliberately and continuously, over decades.

The Layer 1 investments that make Finland and Estonia genuinely resilient were not security investments in the sense that any defence ministry would have recognised them. They were education investments, cultural investments, welfare state investments. Their security function was not the intention. It was the windfall. That distinction matters enormously for the policy argument, because it means the timeline for building genuine cognitive resilience is not immediate but generational, and the decisions that matter most are not the ones taken in response to the next threat but the ones taken before the threat becomes visible.

The adversary understands this. Russia's cognitive operations against European democracies are not primarily designed to win arguments. They are designed to exhaust, to fracture, to make the maintenance of shared reality feel costlier than its abandonment. China's operations are designed to build dependency and shape the information environment through which democracies will eventually make decisions about China. Both operate continuously, at low cost, with deniability, and with a time horizon that democratic electoral cycles are structurally ill-equipped to match. The defence must be built with that asymmetry in mind: not as a response to the last operation, or even the current one, but as a durable architecture capable of absorbing sustained pressure across a timeline measured in decades, not news cycles.

The six-layer framework the author advances in this manuscript is a response to that requirement. It begins where no existing operational framework begins: with the individual citizen's capacity for emotional self-regulation, social connection, and identity coherence, because that is where the adversary begins. It ends with legislative architecture, doctrinal frameworks, and sovereign response capacity. But it insists that the upper layers cannot function if the lower layers have been eroded, and that the social infrastructure beneath all six is not a soft complement to the hard security investment but its enabling condition. A democracy that has allowed its social infrastructure to degrade, that has underfunded its civil society, hollowed its local journalism, allowed its care economy to collapse, and left its populations economically precarious and culturally unmoored, has already done a significant portion of its adversary's work for it. The most important cognitive defence investments are not security investments. They are democracy investments.

Canada and Germany are the report's primary addressees, and the gap between them is narrowing faster than many observers expected. Germany has moved from strategic restraint to strategic engagement at a pace that the Zeitenwende speech alone could not have predicted: €500 billion in infrastructure and defence investment, new legislative authorities for cyber and hybrid operations, a National Security Council activated and a VIGINUM-style attribution agency under construction. The kinetic and institutional pivot is genuine. What has not yet followed is the cognitive architecture: no dedicated civilian agency with a public mandate, no whole-of-society cognitive defence doctrine, no institutional equivalent of the MPF that has made Sweden the most credible cognitive defence model in the Alliance. Germany has the institutional depth, the civil society tradition, and the research community to build it. What it has lacked, until now, is the political will to name the cognitive domain as a primary security domain requiring dedicated institutional investment. The Merz government's legislative pivot suggests that will is forming. This report is an argument for accelerating it.

Canada's gap is different in character, if not in depth. Canada has no ruins from cognitive warfare. It has no equivalent of Germany's 321 documented sabotage incidents, no visible infrastructure attack that crystallises the threat for a public and a political class that have not yet been asked to pay a visible cost. The primary security challenges of this decade leave no ruins and produce no body count, which is precisely why they are difficult to resource and easy to defer. Brian McQuinn captured the resulting institutional posture precisely in May 2026: Canada is “sleepwalking into” the cognitive contest it is already in. The sleepwalking framing is the Canadian-vernacular companion to the UK Foreign Affairs Committee’s sitting ducks characterisation and to Marija Golubeva’s awake-but-groggy diagnosis: the awareness is present, the institutional response is not. Canada's Rapid Response Mechanism watches the information space with skill and international credibility. Canada's civil society counter-disinformation community, underfunded and fragile, punches above its weight. Canada's intelligence community understands the threat and has documented it with precision in the Hogue Commission and the NSICOP reporting. What is absent is the institutional architecture that converts that understanding into continuous, public-facing, whole-of-society response. The author’s headline institutional recommendation is a Canadian Cognitive Defence Agency: a civilian body

with a public mandate, modelled on the Swedish Psychological Defence Agency but adapted for Canadian conditions including federalism, linguistic complexity, and demographic diversity. The agency would sit outside the intelligence architecture so that it can engage civil society, educators, and diaspora communities without the constraints that intelligence equities impose, and the design principles, civilian, arms-length, open-source-only methodology, and institutionally separated from the intelligence community, are the author's own, developed from field research into the Swedish, Estonian, Lithuanian, and Finnish institutional models. It is not expensive. It is not technically complex. It requires only the political decision to treat cognitive sovereignty as a governance priority rather than a security afterthought.

The Canada-Germany-EU corridor is the vehicle through which both countries build it together, and build it faster than either could alone. The institutional scaffolding exists: the Canada-EU Security and Defence Partnership, the Canada-Germany Digital Alliance, the CETA digital architecture. What does not yet exist is the deliberate decision to use these frameworks for the specific purpose of cognitive defence cooperation: shared detection methodology, interoperable attribution architecture, joint civil society funding, and the kind of regular practitioner exchange that has made the Nordic-Baltic cooperation so operationally effective. The corridor is not a substitute for NATO, for NORAD, or for the bilateral relationships that Canada and Germany maintain with their respective allies. It is the architecture that NATO was never designed to provide: proactive, values-based, continuous, and organised around demonstrated commitment to democratic governance rather than historical alliance membership alone.

The Idea Worth Defending, which this report names in Chapter 12, is not a rhetorical flourish. It is the load-bearing argument for why this architecture is worth building. The Nordic and Baltic democracies have built their cognitive resilience not because they faced a sophisticated threat assessment, but because their populations understood, through living memory and continuous civic cultivation, what the alternative looked like. Estonia's cognitive defence culture is inseparable from the Estonian experience of Soviet occupation. Finland's resilience is inseparable from Finnish cultural memory of the Winter War. The connection between historical identity and present security investment is not sentimental. It is structural. Canada and Germany do not have the same proximity to

existential threat. They have something else: a long, deliberate record of choosing the Western project, defending it at cost, and building the institutions through which that choice becomes durable. That record is not nostalgia. It is a strategic resource. It is the argument for why the cognitive architecture built in the window that remains open will hold.

This report does not end with certainty. The outcome of the period of rupture during which it was written is genuinely undetermined. The decisions made now are load-bearing in a way that ordinary policy decisions are not, and the architecture that democratic allies build, or fail to build, in the years ahead will shape the conditions of democratic life for the decades that follow. The adversaries who understand this are already acting on it. Russia is investing more heavily in the cognitive domain precisely as its conventional capabilities are degraded by the war in Ukraine. China is building the information infrastructure of the next decade while democracies debate the regulation of the last one. What the democracies that have built genuine cognitive resilience have demonstrated is not that the threat can be eliminated. It is that it can be managed, absorbed, and turned back, by populations that know who they are, trust the institutions that serve them, and have been given the tools to recognise and resist what is being done to them.

Democracy and the ideas that make up ‘the West’ are a choice. The policy conversation this report enters is already underway. Konrad-Adenauer-Stiftung Canada hosted a cognitive warfare panel at the Munich Security Conference in February 2026 using language that maps directly onto this framework. The strongest independent validation of this report’s central institutional design conclusion arrived from the UK House of Commons Foreign Affairs Committee, which published its inquiry Disinformation Diplomacy: How Malign Actors Are Seeking to Undermine Democracy in March 2026 following fourteen months of evidence sessions. The Committee reached the same conclusion through a different evidentiary path: that open liberal democracies are sitting ducks against adversary disinformation operations, and that the institutional remedy is a statutory, public-facing agency modelled on Sweden’s Psychological Defence Agency and France’s VIGINUM, the same institutional anchors this report advances for Canada and Germany. That convergence, between an independent parliamentary inquiry and this research programme, working in different countries with different methodologies and

arriving at the same architecture, is the strongest available signal that the analysis is correct and the moment for action has arrived. The democracies that built genuine cognitive resilience did so because they decided, before the cost became undeniable, that the conditions of democratic life were worth defending deliberately. That decision is available now. The window for making it will not stay open for long.

ANNEXES

Annex A: Note on Further Research

This report does not comprehensively address several areas requiring further work. Each represents a meaningful research gap that future work in this field should prioritise:

- Private sector dimensions beyond platforms, including debunking companies, telecommunications infrastructure, cybersecurity firms, consulting, and public relations industries, and their role in both propagating and defending against cognitive threats.
- Engagements of other international organizations and alliances beyond the EU and NATO, like the UN, OECD, OSCE, Council of Europe, etc.
- Measurement methodology for cognitive defence effectiveness, including the development of validated input, process, and outcome metrics that allow peer-comparison across allied and like-minded democracies.
- Generational dynamics in cognitive vulnerability and resilience, addressed briefly in this report but warranting deeper longitudinal analysis, particularly given differential platform use and trust profiles across age cohorts.
- AI-enabled manipulation and detection, an area evolving faster than any policy cycle can track. This report captures the state of the threat as of early 2026 and recommends ongoing institutional attention.
- International legal framework development for cognitive attacks, including questions of attribution, proportionality, and lawful response under international law.
- Economic and financial dimensions of cognitive warfare, including financial flows enabling influence operations, the effectiveness of sanctions in disrupting adversary cognitive warfare infrastructure, and the economic costs of successful cognitive attacks on democratic governance.
- Military operational doctrine for cognitive defence, specifically strategic communications, psychological operations, and information warfare doctrine across allied military establishments, and the relationship between military and civilian cognitive defence architectures.
- Democratic AI governance and the Global South. If democratic allies want to win the long-term competition against authoritarian technology governance models, they must engage the countries that will determine whose norms and infrastructure govern the next generation of AI deployment. This report does not address that competition in adequate depth.

Annex B: Key Concepts and Terms

The following glossary defines the governing concepts and key terms used throughout this report. It is organised in three sections: governing concepts that form the analytical and normative foundation of the report's argument; core operational and structural concepts used in the framework and case analyses; and institutional and practitioner vocabulary, documenting the terms used by allied institutions and their relationship to this report's governing framework. Where institutional usage differs from the definitions adopted here, those differences are noted.

Definitional Approach: Maximalist versus Minimalist

A foundational choice in any analysis of cognitive warfare is the scope of the definition adopted.

Minimalist definition: Cognitive warfare as specific military or intelligence activities with defined actors, identifiable operations, and discrete targets. This framing favours operational precision but risks excluding the structural and platform-mediated dimensions of the threat.

Maximalist definition: Cognitive warfare encompasses the full spectrum of activities affecting societal cognition, including structural factors, platform dynamics, social architecture, and adversary operations. This framing provides broader policy orientation.

This report adopts maximalist framing. The broader lens provides more useful policy orientation for democracies whose vulnerability is structural as well as operational.

Governing Concepts

The following concepts form the analytical and normative foundation of this report's argument.

Cognitive sovereignty: The sovereign capacity of democratic citizens to form genuine political preferences, free from coercion or systematic manipulation of the information environment, and the collective conditions that enable it. Cognitive sovereignty is the precondition for legitimate democratic governance. It is the ultimate object of cognitive defence and the value that adversary cognitive warfare operations are designed to erode.

This report uses “cognitive sovereignty” as the most politically salient and institutionally accessible framing of what is at stake.

Cognitive warfare: Activities conducted in synchronisation with other instruments of power to affect attitudes and behaviour of target populations by influencing, protecting, or disrupting individual and group cognition to gain an advantage. This report adopts the NATO ACT formulation. Cognitive warfare operates in both war and peace; this is the feature that most distinguishes it from earlier conceptions of information operations and that creates the most significant gap in existing democratic defence architectures.

Epistemic warfare: Operations whose primary objective is not to persuade audiences toward a specific false belief but to degrade the conditions under which belief formation is possible. The goal is not to make people believe false things, but to make them unable to confidently believe true things. Distinguished from disinformation operations by objective: epistemic warfare targets the cognitive process, not the cognitive output.

Information peacekeeping: A doctrine of truth-based information operations as cognitive defence infrastructure. The concept was developed by Robert Garigue at the Canadian Department of National Defence in the mid-1990s, in connection with semantic warfare and the broader conceptual framework for information warfare he presented in his 1995 paper, and developed in the contemporary cyber-age context by Dave McMahon (Sapper Labs Group, 2021), who attributes the originating concept to Garigue. This report adopts and extends Information Peacekeeping as the international half of a Canadian doctrinal commitment in which Free Press at home and Information Peacekeeping abroad operate as two operational halves of the same commitment to the conditions of truth-based democratic deliberation. Three operational components define the doctrine as developed in Recommendation 10: open-source-only methodology with classified intelligence kept separate, so that the doctrine is publicly defensible and exportable; principled institutional separation of cognitive defence capability from military command, so that mandate creep does not erode democratic trust; and credibility as a strategic asset, on the principle that truth-based information operations are not only ethically correct but strategically superior, because nations that engage in disinformation degrade their own ability to communicate truthfully when it matters most. The pairing of Information

Peacekeeping abroad with Free Press at home as two halves of one Canadian doctrinal commitment is the analytical contribution of this report.

Ontological warfare: The most advanced form of epistemic attack: targeting not what people believe, but what is permitted to be believable. Controlling the substrate of possibility. When adversaries succeed at the ontological level, certain thoughts become difficult to think, not merely unpopular to express. Distinguishes itself from epistemic warfare by attacking the conditions of thought rather than the conditions of belief.

Passive citizen problem: An original field-research contribution of this report, named in interviews with Lithuanian practitioners in 2026. The passive citizen problem describes the structural side effect of highly effective institutional cognitive defence architecture: when institutions reliably monitor, attribute, and respond to adversary cognitive operations, citizens may delegate their own cognitive vigilance to those institutions rather than maintaining it individually. The trust is real and deserved, but if it substitutes for rather than supplements individual capacity, it creates a new vulnerability. A population trained to defer to institutional cognitive defence has no individual reserve if those institutions are captured, overwhelmed at scale, or absent during rapid escalation. The implication for the architecture this report recommends is structural: institutional and individual capacity must be built in parallel rather than sequentially. The phenomenon is documented in Lithuania, where the most operationally precise calibrated narrative response system in the research set has produced exactly the dependency risk Lithuanian practitioners themselves identify.

Core Concepts

Active defence: Measures that impose costs on adversaries through exposure, attribution, sanctions, legal prosecutions, diplomatic consequences, and regulatory action. Distinct from passive resilience (absorbing attack) and from offensive operations (initiating attack). Active defence operates within democratic legal constraints while creating meaningful deterrence (deterrence-by-punishment) through consequences. This report advocates for a graduated active defence posture as the missing middle layer of democratic cognitive defence.

All-platforms architecture: The Russian operational architecture in which every transmission channel available is used as an instrument of cognitive warfare, including not only media but also conferences, international frameworks, diplomatic channels, foreign media partnerships, journalist training programmes, religious institutions, and individuals operating across all of these. The implication for democratic response is structural: a defence architecture focused only on social-media disinformation will miss most of the operation, because the operation is not primarily conducted through social media. The all-platforms architecture is also the doctrinal foundation for the Information Peacekeeping recommendation developed in Recommendation 10: democratic media presence, cultural diplomacy, and sustained international broadcasting are not soft-power adjacencies but cognitive defence infrastructure operating on the same architecture adversaries already use. The most operationally significant religious-institution vector identified in the report is the Russian Orthodox Church Moscow Patriarchate, developed in full in Chapter 18.

Cognitive intrusion: The deliberate manipulation of individual and collective mental processes to promote political violence or undermine democratic governance. A narrower operational term than cognitive warfare, typically used in legal and regulatory contexts where precision of definition is required for enforcement. The legal specificity matters: cognitive intrusion frames the harm as an act done to individuals and communities, which is a precondition for regulatory accountability and criminal prosecution. This report uses cognitive intrusion where the analysis concerns specific, identifiable acts rather than systemic conditions.

Cognitive resilience: The capacity of individuals, communities, societies, governments, and organisations to withstand, adapt to, and recover from cognitive attacks while maintaining the capacity for genuine political preference formation. Distinct from passive immunity: resilient populations can recognise manipulation, reject it, and maintain social cohesion under sustained pressure.

Collective defence: Alliance model where an attack on one member is treated as an attack on all, established under Article 5 of the North Atlantic Treaty. Reactive by design: it requires consensus that an attack has occurred and that a collective response is

warranted. This is NATO's founding security architecture. Cognitive warfare systematically complicates collective defence because adversary operations are specifically designed to generate ambiguity, suppress attribution consensus, and keep attacks below the threshold at which Article 5 obligations activate. NATO has long recognised that hybrid attacks, including cognitive operations of sufficient severity, can trigger Article 5. The design challenge for democratic cognitive defence is to build mechanisms that can function before the consensus threshold is reached.

Collective security: Proactive cooperation among states to maintain a shared security environment, based on shared interest in preserving the conditions of security rather than requiring consensus that a specific attack has occurred. This distinguishes collective security from collective defence: collective security is continuous and preventive, while collective defence is reactive and episodic. The distinction matters for cognitive defence architecture, which must operate continuously across peacetime, crisis, and conflict rather than activating only once an attack is confirmed. Hybrid threats and cognitive operations below the Article 5 threshold may trigger Article 4 consultations among Allies, providing a mechanism for collective awareness and coordination without requiring the attribution certainty that Article 5 demands.

Comprehensive security (kokonaisturvallisuus): Finland's contemporary evolution of the total defence concept. Where total defence (kokonaismaanpuolustus) integrated military and civil sectors against external military threats, comprehensive security extends the framework across all hazards and all circumstances, including natural disasters, pandemics, hybrid threats, and armed conflict. Vital functions of society are secured through collaboration between authorities, the business community, organisations, and citizens at all levels of society. The Finnish Security Strategy for Society, most recently updated in January 2025, assigns strategic tasks to every branch of government, the private sector, civil society, and individuals. Individuals are treated as key security actors, not merely beneficiaries of state protection. Finland's comprehensive security model is among the most institutionally developed whole-of-society resilience architectures among allied democracies and is increasingly referenced as a template by NATO partners.

Digital autocracy: An autocratic regime that has institutionalised digital authoritarian tools as a constitutive element of its governing model, rather than deploying them episodically in response to crisis. China represents the consolidating example: surveillance infrastructure, social credit systems, AI-enabled population management, and comprehensive information environment control are structural features of governance, not emergency instruments. Digital autocracy differs from digitally-enabled autocracy in integration and intent: the digital architecture is not a tool the regime uses but the medium through which the regime governs. The exportability of digital autocracy infrastructure, including surveillance systems, platform architecture, and AI governance models, means that democratic societies face not only direct cognitive warfare from digital autocracies but a longer-term competition over whose model of the information environment becomes the global default.

Digitally-enabled autocracy: An autocratic regime that effectively deploys digital tools for control, surveillance, and external influence operations without having built the comprehensive integrated digital authoritarian architecture that characterises digital autocracy. Russia is the primary example: troll farms, state media, hack-and-leak operations, and social media manipulation are instrumentally deployed in pursuit of specific political objectives, but they do not constitute a systemic governing architecture of the kind China has constructed. The distinction matters for threat assessment: digitally-enabled autocracy is more flexible and harder to attribute, while digital autocracy produces more structural and durable effects on the populations it governs. Both pose distinct cognitive warfare threats to democratic societies.

Fantasy-industrial complex: A self-organising and loosely coordinated system whose objective is no longer to make individuals believe specific false claims but to distract, generate distrust, and activate anti-democratic norms and authoritarian behaviours. Named by the European Commission Joint Research Centre in its April 2026 report Fractured Reality: How Democracy Can Win the Global Struggle Over the Information Space (Scharfbillig, Lewandowsky et al.), the fantasy-industrial complex framing names what this report treats as the contemporary evolution of Russian cognitive warfare doctrine into a system that no longer requires adversary intent to operate. As the JRC

report notes, blaming individuals for being misinformed is a misdiagnosis: the attention economy structurally privileges negative, emotional, and conflictual content not because of adversary design but because engagement maximisation is the platform business model. The adversary does not need to build the architecture; it already exists. The fantasy-industrial complex is operationally distinct from disinformation because the harm it produces is environmental rather than propositional: even truthful content can sustain the system if its framing produces the distraction, distrust, and anti-democratic activation the system optimises for.

Frame-not-fact mechanism: A structural feature of contemporary Russian cognitive operations in which the adversary does not assert false propositions but produces multiple partial-true versions of the same event, none completely true, none entirely false, and lets the resulting confusion both fragment public understanding and sustain consumption of adversary content. The mechanism is named explicitly in this report's Latvia field research and developed analytically in Chapter 3 as a structural feature of the contemporary Russian operational repertoire. Frame-not-fact is operationally distinct from disinformation as conventionally understood: debunking addresses fact but not frame, and audience research in Latvia documents fatigue with the debunking format precisely because it cannot reach the frame layer. The mechanism overlaps with the firehose of falsehood model formally characterised by RAND in 2016 (see firehose of falsehood) but is analytically distinct: where firehose-of-falsehood operations are characterised by volume and inconsistency, the frame-not-fact mechanism is characterised by the construction of partial-truth narrative architectures within which audiences must choose among competing frames rather than between truth and falsehood. The October 2024 Latvia drone case and the March 2026 Stoltenberg-memoir reframe document the mechanism at operational scale.

Grey-zone warfare: Coercive activities conducted below the threshold of formally declared armed conflict, designed to achieve strategic objectives while avoiding the legal and political consequences that overt military action would trigger. The grey zone is the primary operational space of cognitive warfare: it is defined by deniability, ambiguity, and the deliberate exploitation of the threshold at which democratic collective defence and

legal response mechanisms activate. Democratic institutions were largely designed for the binary of peace and war; the grey zone is the space adversaries have engineered to operate in between. The asymmetry is structural: authoritarian actors can sustain grey-zone campaigns indefinitely, while democratic governments face pressure to either escalate to a declared response or absorb the attack without cost imposition.

Hybrid threats (EU): The EU's 2016 Joint Framework defines hybrid threats as the mixture of coercive and subversive activity, combining conventional and unconventional methods spanning diplomatic, military, economic, and technological domains, used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. The EU deliberately keeps the definition flexible to respond to the evolving nature of hybrid threats, which may include information manipulation, cyberattacks, economic coercion, covert political manoeuvring, and threats of military force. The EU's primary operational response framework is the hybrid toolbox, established in 2022 under the Strategic Compass.

The two formulations are substantively compatible and refer to the same threat landscape. The EU definition is broader in scope, explicitly encompassing non-military instruments and emphasising the below-threshold character of hybrid activity. NATO's definition places greater emphasis on the destabilisation objective and the societal cognitive dimension. The EU definition was developed for regulatory and policy coherence across member states; NATO's for military planning and collective defence. This report uses both in their respective institutional contexts.

Hybrid threats (NATO): NATO defines hybrid threats as combining military and non-military as well as covert and overt means, including disinformation, cyberattacks, economic pressure, deployment of irregular armed groups, and use of regular forces, with the aim of blurring the lines between war and peace and sowing doubt in the minds of target populations to destabilise and undermine societies. Since 2016, NATO has publicly stated that hybrid actions against one or more Allies could lead to invocation of Article 5 of the North Atlantic Treaty. Hybrid threats may also trigger Article 4 consultations among Allies.

Kill-chain methodology (information operations application): The application of the standard military-doctrinal framework for the sequenced application of kinetic force against a target to adversary information operations infrastructure rather than to discrete adversary narratives. Developed by Ukrainian practitioners working at the receiving end of Russian operations since 2014, the doctrine treats adversary information operations as having identifiable infrastructure with mappable nodes: production capacity, amplification networks, embedded media properties, financial flows, institutional partnerships, religious-institution channels, journalist training programmes, and cultural-diplomacy vehicles. The argument is that targeting the infrastructure produces durable defensive gains, while targeting the narratives produces individual rebuttals that the infrastructure replaces faster than the rebuttals can accumulate. The doctrine is the operational expression of the analytical recognition that Russian operations cannot be defeated through Western-style counter-messaging because the messaging itself is not the operation. The Ukrainian doctrine is developed at length in Chapter 18, and its implication for allied democratic defence architecture is structural: democracies must build the institutional capacity to identify, target, and disrupt adversary operations infrastructure inside their own legal and institutional frameworks.

Psychological defence: Defensive measures protecting societal cognition from manipulation and attack, with emphasis on the population's capacity to maintain free opinion formation under adversarial pressure. The primary institutional term in Swedish and French contexts, with somewhat different operational emphasis in each. Sweden's Myndigheten för psykologiskt försvar (MPF), established in 2022, uses it to encompass the full institutional architecture for defending the population's epistemic autonomy, including media literacy, pre-bunking, and rapid response to coordinated influence operations. The Swedish model treats psychological defence as a standing peacetime function rather than a crisis-only mechanism. This report treats psychological defence as a subset of the broader cognitive defence architecture, alongside institutional resilience and active defence.

Reflexive control: The unifying Russian military doctrine under which the techniques of cognitive warfare are organised, defined as the practice of conveying specially prepared

information to an opponent in order to incline that opponent to make, voluntarily, the decision the initiator wants made. Developed in the 1960s by the Soviet mathematician Vladimir Lefebvre, codified inside Soviet military doctrine through the 1970s and 1980s, and the subject of continuous theoretical and operational development inside Russian military thought for over half a century. The objective of reflexive control is not persuasion. It is paralysis: overloading adversary decision-making with contradictory information, constructing false strategic images that the adversary acts on, and making the adversary take self-defeating decisions while believing those decisions reflect the adversary's own strategic interest. The information confrontation doctrine, the 4Ds, vranye, the information-overload technique, the firehose of falsehood, the all-platforms architecture, and the historical-warfare method are each operational instantiations of reflexive control. The doctrine explains why Western counter-disinformation frameworks built on the assumption that Russia is attempting to persuade audiences of specific propositions miss the point at the foundational level: Russia is optimising for adversary decision-making paralysis, not belief change. The defensive task changes accordingly: metrics, detection architecture, and response posture must be calibrated against the paralysis objective rather than against persuasion metrics.

Total defence (totalförsvar): The integration of military and civil capabilities into a unified whole-of-society security framework, premised on the principle that modern threats cannot be met by military means alone. The concept originated in the Nordic states during the Cold War and has been substantially revived and revised across allied democracies since 2014. Country-specific implementations vary: Norway (totalforsvar) centres on mutual civil-military support across the full crisis spectrum, with resilience, cross-sectoral situational awareness, and civil-military cooperation as foundational principles. Sweden (totalförsvaret) covers all society-wide activities required to prepare the country for war, comprising military and civil defence, with the whole of society responsible for defending Sweden's security, freedom, and independence; Sweden's 2025–2030 Defence Resolution represents the most substantial reinforcement since the Cold War. Finland has evolved its model toward comprehensive security (see below). Estonia organises national defence comprehensively across six pillars: military defence, civilian support for military defence, international action, domestic and internal security,

maintenance of continuous state and societal operation, and psychological defence. Latvia (Visaptveroša valsts aizsarčība) is structured around seven pillars: military capabilities, public-private cooperation, public education, civil defence, strategic communication, economic resilience, and psychological resilience. Lithuania enshrines total and unconditional defence in its founding policy documents, built on three pillars: national defence capabilities, NATO deterrence, and the whole-of-society approach. Ukraine has developed a de facto total defence system, accelerated by Russian aggression in 2014 and formalised through the 2021 Law on the Fundamentals of National Resistance; unlike classical total defence models, Ukraine's approach combines government and society as equal partners in a bottom-up and top-down architecture simultaneously.

Whole-of-society security: A defence model premised on the recognition that the attack surface of modern threats, including cognitive warfare, is societal rather than purely military. Mobilises all sectors of society, including government institutions, civil society organisations, educational systems, media, the private sector, and individual citizens, in a coordinated and mutually reinforcing security posture. The whole-of-society model differs from whole-of-government approaches in that it extends accountability and active participation to non-state actors and citizens, not only to state institutions. This report identifies whole-of-society architecture as the appropriate governance model for cognitive defence, and documents the Nordic and Baltic implementations as the most developed operational examples among allied democracies.

Key Manipulation Techniques

The following terms describe specific operational techniques documented in this report's field research and open-source analysis.

Environment-Shaping Techniques

4Ds (dismiss, distort, distract, dismay): The operational logic of Russian information operations as originally articulated by Ben Nimmo (former NATO press officer, later Atlantic Council Digital Forensic Research Lab) in his May 2015 piece "Anatomy of an Info-War," and subsequently adopted into NATO StratCom and UK information operations

doctrine. The four operations describe the techniques by which adversary cognitive operations exhaust the capacity for coherent response rather than win an argument: dismissal of inconvenient evidence, distortion of context and framing, distraction from the central issue, and dismay through emotional and reputational pressure. The 4Ds operationalise the firehose of falsehood model (see firehose of falsehood) at the level of individual operations and sit, with that model, as instantiations of the broader reflexive control doctrine that unifies Russian cognitive operations theory (see reflexive control).

Firehose of falsehood: The Russian propaganda model formally characterised by RAND researchers Christopher Paul and Miriam Matthews in 2016 (RAND Corporation Perspectives PE-198-OSD), identifying four defining characteristics of Russian information operations: high volume, multichannel distribution, no commitment to objective reality, and no commitment to consistency. The model depends on exhaustion rather than persuasion: the objective is not to win an argument but to flood the information environment with sufficient contradictory content that audiences exhaust their verification capacity and cease attempting to reach attribution consensus. Though published in 2016, the model has become more operationally consequential with each passing year as AI and social media have expanded the volume, reduced the cost, and accelerated the pace of saturation operations. The firehose of falsehood is one operational instantiation of the broader reflexive control doctrine and is related to but analytically distinct from the frame-not-fact mechanism: the firehose model emphasises volume and inconsistency, while frame-not-fact emphasises the construction of partial-truth narrative architectures.

Information alibi: Pre-emptive narratives planted before an anticipated event to provide ready-made justification or alternative explanation, seeding the information environment before the primary account can establish itself. The information alibi functions by preventing attribution consensus: once multiple competing explanatory frameworks are in circulation, audiences must choose among them rather than accepting the factual account as self-evident. The technique has been documented extensively in Russian operations, including the pre-seeding of narratives around the MH17 downing and the poisoning of Sergei Skripal. An information alibi is distinct from reactive denial in that it

requires advance operational planning and anticipates the need for plausible deniability before the event occurs.

Information overload: Flooding the information environment with contradictory explanations, competing narratives, and high volumes of content to prevent attribution consensus and exhaust verification capacity. A technique of epistemic warfare: the goal is not to persuade but to overwhelm. Documented by field research interviewees as a distinct operation type alongside persuasion and manipulation. A well-documented example is the 2014 downing of MH17, in which dozens of Russian-originated narratives flooded the information space to obscure attribution.

Mundanisation: Routine, repetitive coverage that normalises horror, suffering, or wrongdoing by presenting it as unremarkable. A technique of epistemic attrition: through sustained exposure to atrocity or injustice framed as ordinary, populations lose the moral clarity and emotional urgency required to demand institutional response. Mundanisation does not persuade audiences that atrocities are acceptable; it exhausts the capacity for outrage that motivates political action. Documented in the coverage of the war in Ukraine, where sustained high-volume reporting on civilian casualties progressively reduced audience engagement and political pressure in Western countries. The technique operates through volume and repetition rather than through false content, making it resistant to standard debunking approaches.

Vranye: A Russian strategic-culture term, italicised in this report, defined as a ritualistic performance of untruth whose objective is not persuasion but saturation, flooding the information environment with contradictory claims until reliable belief feels impossible. Vranye is closely related to but analytically distinct from disinformation: where disinformation targets belief in specific false claims, vranye targets the epistemic conditions under which any confident belief is possible. The Russian vranye tradition combines both epistemic and ontological dimensions: high-volume contradictory claims in the present operate as epistemic attack, while sustained Russian historical revisionism, including the systematic rewriting of Soviet-era narratives and the contemporary insistence that Ukrainian statehood is itself historically illegitimate, operates as ontological attack on what is permitted to be thought about the boundaries of nations and the

legitimacy of independent post-Soviet societies. Vranye is one operational instantiation of the broader reflexive control doctrine (see reflexive control).

Distribution and Laundering Techniques

External source effect: A psychological and informational phenomenon in which content is perceived as more credible when it appears to originate from an external or foreign source, compared to identical content from a domestic origin. Exploited in influence operations through a feedback loop in which domestically-produced disinformation is seeded through foreign outlets, platforms, or intermediaries and then recirculated back into the target country as apparently independent external validation. The effect compounds information laundering: the foreign circulation launders the content's origin while the external source effect launders its credibility. Documented as a deliberate operational technique in Russian influence operations targeting European and North American audiences.

Information laundering: The process by which foreign-originated narratives are placed in domestic media ecosystems through intermediary and proxy channels, typically local outlets, political actors, or social media accounts, to obscure their origin and increase credibility. Documented as a primary Russian and Chinese operational technique.

LLM grooming and the Pravda network: An infrastructure-level rather than content-level threat in which adversaries deliberately flood the internet with false information to corrupt the outputs of large language models when citizens use those models to verify claims. The term "LLM grooming" is attributed to the American Sunlight Project. The Pravda network, a coordinated system of more than 150 pro-Kremlin websites originating with the Crimea-based IT company TigerWeb and designed to contaminate AI training data with disinformation, is the documented operational case. A March 2025 DFRLab / CheckFirst report (Amaury Lesplingart and Valentin Châtelet, "Russia-linked Pravda network cited on Wikipedia, LLMs, and X") documented the Pravda network's insertion of over 1,900 hyperlinks across 44 Wikipedia language versions. A parallel March 2025 NewsGuard study testing ten leading generative AI models found that those models reproduced Pravda network content approximately 33 per cent of the time in response to prompts on relevant topics. The NORDIS Hub network (European Digital Media

Observatory) corroborated the finding in Nordic languages, documenting that ChatGPT, Google Gemini, and Microsoft Copilot sometimes rely on Pravda network domains when answering questions in Finnish, Swedish, Danish and Norwegian, occasionally reproducing less common false claims and citing these sources without flagging their pro-Kremlin provenance. The adversary is no longer only injecting false content into the information environment; it is corrupting the verification infrastructure citizens rely on to navigate it. LLM grooming represents the AI-era operationalisation of information laundering at the infrastructure layer rather than at the content layer.

Media capture: An operational model in which a state actor occupies the information space with volume and credibility, crowding out independent reporting in markets where local journalism is weak, rather than primarily fabricating content. Distinguished from content manipulation by the structural target: media capture displaces the conditions under which independent journalism survives, rather than inserting false claims into an otherwise functioning ecosystem. The Reporters Without Borders Propaganda Monitor Season 2 (launched March 2026) documents China Global Television Network's reach across television, radio and online platforms in over 160 countries, with its radio service operating in 65 languages, the most expansive language service of any radio broadcaster worldwide. CGTN-affiliated outlets operate in diaspora media ecosystems including Canada's Chinese-language diaspora media without the regulatory constraints that apply to domestic broadcasters. The implication for democratic cognitive defence is that media-capture operations require sustained investment in independent local journalism as a structural counter-measure rather than narrative-by-narrative rebuttal.

Psychological Persistence Mechanisms

AI-generated vox-pop content: A category of synthetic media in which entirely AI-generated footage, including faces, settings, audio, and apparent spontaneity, is produced in the man-on-the-street interview format from the Latin vox populi. The format carries ambient credibility because of its association with journalistic practice: audiences assume vox-pop content represents genuine public opinion. Field research with Ukraine's Centre for Countering Disinformation identified a campaign that deployed entirely AI-generated vox-pop content; the giveaway, on close forensic examination, was that the

eyes were clearly AI-generated, but the production quality was otherwise high. As generation quality continues to improve, easy identifiers will disappear. AI-generated vox-pop content sits outside the deepfakes-of-individuals taxonomy and represents a new threat category in cognitive warfare's AI dimension, distinct from synthetic media targeting specific named individuals.

Dormant-narrative reactivation: A mechanism by which adversaries do not always need to create new operations but instead identify dormant narratives, often developed or tested in earlier operational cycles, and wait for the domestic and technological conditions that will make those narratives resonate. Documented in field research with the Swedish Psychological Defence Agency, which confirmed that the same narrative targeting Swedish social services as hostile to Muslim families had circulated in the Swedish information environment more than a decade before the 2021 to 2022 campaign that exploded into international attention and a terrorist attack in Brussels. The narrative did not gain traction in its earlier iterations; what changed was not a new adversary operation but a combination of domestic activist organisation and platform amplification that created the conditions for a pre-existing narrative to detonate. The policy implication is significant: a threat detection architecture that focuses only on new narratives will systematically miss dormant-narrative reactivation operations, and detection capacity must include the historical mapping of dormant adversary narratives alongside live monitoring of current ones.

Historical warfare: The selective deployment of historical narratives meant to undermine the founding legitimacy of target societies. A core method in the Russian operational repertoire alongside hack-and-leak operations, troll farms, state media amplification, and proxy amplification. The mechanism by which historical warfare operates in pre-existing cultural memory has been documented at length by Jade McGlynn (Senior Lecturer in War Studies, King's College London) in Memory Makers: The Politics of the Past in Putin's Russia (London: Bloomsbury, 2023) and Russia's War (Cambridge: Polity, 2023), both of which trace the deliberate construction of historical narrative as an instrument of state power inside Russia and as a vehicle for influence abroad. Operational examples documented in the report include the Forest Brothers

framing, used without differentiation across all three Baltic states to support rehabilitation-of-Nazism narratives; the Bronze Soldier monument removal in Tallinn in 2007; and the reactivation of Soviet war memorials in Norwegian Finnmark as vectors for memory politics directed at local and national audiences. Historical warfare is one operational instantiation of the broader reflexive control doctrine (see reflexive control).

Liar's dividend: The phenomenon by which the existence of synthetic media, including AI-generated audio, video, and images, degrades the credibility of authentic content. Coined by legal scholars Bobby Chesney and Danielle Citron in the context of deepfakes. The mechanism is asymmetric: the liar's dividend does not require audiences to believe that specific synthetic content is real, only that the question of authenticity becomes sufficiently difficult to answer that authentic evidence loses its evidentiary weight. In cognitive warfare contexts, adversaries exploit the liar's dividend to neutralise inconvenient authentic documentation, deny attribution, and sustain parallel reality claims. Distinct from disinformation in mechanism: the liar's dividend degrades the epistemic environment rather than inserting false content into it.

Memory politics: The instrumentalisation of historical memory, monument symbolism, and commemorative ritual as vectors for contemporary cognitive operations. Memory politics is the operational complement to historical warfare (see historical warfare): where historical warfare targets the founding legitimacy of target societies through narrative, memory politics deploys the physical, symbolic, and ritual infrastructure of memory, including monuments, commemoration practices, and public-history institutions, as live operational vectors. Documented operational examples in this report include the 2007 removal of the Bronze Soldier monument from central Tallinn, Russian-language information operations exploiting the resulting public reaction; the Forest Brothers framing used to recast Baltic anti-Soviet partisans as Nazi collaborators; and the reactivation of Soviet war memorials in Norwegian Finnmark by the Russian Consulate General in Kirkenes as vectors directed at local and national audiences. Memory politics is also the conceptual frame within which the Volume II Estonia, Latvia, and Lithuania chapters develop the operational signature of contemporary Russian cognitive operations against the Baltic states.

Operation INFEKTION: A KGB active-measures campaign of the 1980s that falsely attributed the HIV epidemic to United States biological warfare. Named in this report as the direct template for modern health disinformation, including the COVID-era disinformation operations documented in the CSIS reporting cited in Chapter 3. The persistence of the INFEKTION template across more than four decades is one of the empirical foundations for this report's argument about the multigenerational character of Russian cognitive operations: narratives developed in earlier operational cycles remain available for selective reactivation in contemporary conditions, and detection architectures focused only on novel narratives will systematically miss reactivations of templates with long operational histories.

Prebunking: Proactive inoculation against anticipated adversary narratives, exposing target audiences to weakened forms of manipulative techniques before full-scale operations deploy them. Distinct from debunking, which reactively corrects content already in circulation: prebunking intervenes before the narrative is seeded, reducing its effectiveness when it does appear. The inoculation logic draws on psychological research showing that prior exposure to manipulation techniques increases resistance to subsequent manipulation, even when the specific content differs. Field research evidence from Finland, Sweden, and the Netherlands identifies prebunking as consistently more effective than debunking, in part because debunking risks amplifying low-reach content and because the sleeper effect means corrections fade faster than the original content. Prebunking has been implemented at scale through online games (Go Viral, Bad News) and government communications programs.

Institutional and Practitioner Vocabulary

The following terms are used by allied institutions and practitioners. Their relationship to this report's governing framework is noted where usage differs or where institutional terms carry specific connotations.

Active measures: The Soviet-era doctrinal term for systematic state-organised influence operations including forgeries, agents of influence, front organisations, and disinformation campaigns. Institutionalised inside the KGB's Active Measures directorate, with Operation INFEKTION (see Operation INFEKTION) the most-cited operational case. The

active-measures lineage is the historical continuity inside which contemporary Russian cognitive operations operate: the techniques, the targets, and the operational logic are recognisable as evolutions of the Soviet-era doctrine, with the principal change being the technical means (cyber, AI, platform amplification) rather than the underlying operational concept. This report uses “active measures” in its specifically historical sense, to mark the Soviet-era doctrinal lineage, rather than as a contemporary operational descriptor.

Calibrated narrative response: A Lithuanian institutional innovation in which adversary narratives are assessed on a scale of operational reach and an appropriate response is selected at the matching scale, rather than every adversary narrative receiving the same response. The system features eleven Lithuanian institutions sharing a common methodology, rating narrative on a scale from ‘no response’, for low-reach content where debunking would amplify it, through to responses from academic contacts, ministry experts, senior officials, and head-of-state intervention at the highest reach. The doctrinal principle is that not every piece of disinformation warrants an institutional response, and responding to low-reach content does the adversary’s amplification work for it. Calibrated narrative response is the most operationally precise architecture in the research set for matching response capacity to operational reach, and is named alongside Lithuania’s institutional reliability as one of two structural sources of the passive citizen risk identified in Lithuania (see passive citizen problem).

Cognitive degeneration: The gradual erosion of a population's capacity for shared reality formation as a cumulative outcome of sustained cognitive warfare, rather than the effect of any single discrete operation. Used in NATO informal and analytical discourse to describe the long-term trajectory of societies subjected to persistent influence operations: not a single moment of deception but a progressive degradation of the epistemic conditions under which democratic deliberation is possible. Cognitive degeneration manifests as declining institutional trust, the fragmentation of shared factual baselines, and the growing inability of populations to distinguish credible from non-credible sources. It is the systemic outcome that epistemic warfare and ontological warfare target. The concept is significant because it implies that successful cognitive

defence cannot be measured only by the defeat of individual operations but must also track the long-run health of the information ecosystem.

Cognitive security: The defensive posture oriented toward protecting cognitive processes and epistemic conditions from manipulation and attack. Roughly equivalent to cognitive defence as used in this report, with a framing distinction: cognitive security positions the function as a standing security capability comparable to cybersecurity or physical security, rather than framing it primarily as a response to a named adversary. Used in Norwegian interagency and policy contexts and increasingly across allied institutions. The cognitive security framing has institutional advantages: it is easier to budget and staff as a permanent function, and it avoids the political sensitivities of explicitly naming adversary operations in democratic contexts. Its limitation is that it may understate the intentional adversarial dimension of the threat, which carries implications for deterrence and cost imposition strategies.

Cognitive superiority / cognitive advantage: NATO ACO's preferred framing for the objective of operations within the cognitive domain. Structured as a three-part framework: understand (intelligence and analysis), protect (defensive resilience), and project (influence and narrative). This report uses the same tripartite logic but frames it as protection, detection, and response to emphasise the defensive orientation appropriate for democratic contexts.

Digital sovereignty: The capacity of a state to exercise meaningful authority over its digital infrastructure, data flows, platforms, and information architecture. Distinguished from traditional territorial sovereignty in that digital sovereignty is not inherently bounded by national borders: foreign-owned platforms, cloud infrastructure, and algorithmic systems can shape a society’s information environment without being subject to domestic governance. Democratic digital sovereignty requires not only data localisation and cybersecurity capability but the capacity to regulate the underlying architecture, including platforms, algorithms, and data flows, through which information circulates and through which cognitive effects are achieved. Most allied democracies currently govern the outputs of their information systems, such as disinformation and harmful content, rather

than the systems themselves. The EU's Digital Services Act represents the most advanced allied attempt to regulate the architecture rather than the outputs.

FIMI (Foreign Information Manipulation and Interference): The European Union's primary operational term for this threat domain, designed for regulatory acceptability under the Digital Services Act and related frameworks. Actor-focused (foreign) and effect-focused (manipulation and interference). Used by the EU institutions, including the EEAS. This report's governing concept of cognitive warfare is broader than FIMI, encompassing domestic and structural dimensions that FIMI's definition excludes by design.

Hostile influence / Malign influence: Terms used by the NATO StratCom COE and across allied institutions to describe influence operations attributed to a specific hostile actor. Actor-focused rather than effect-focused: where FIMI describes a category of activity by its character (foreign, manipulative, interfering), hostile or malign influence describes it by the intent and identity of the actor conducting it. Used interchangeably in most institutional contexts, with "malign" preferred in US government usage and "hostile" more common in European and NATO settings. The actor-focused framing is operationally useful when attribution is established or presumed, as it supports specific deterrence and cost imposition responses. Its limitation is that it depends on attribution, which adversaries deliberately complicate. This report uses the effect-focused framing of cognitive warfare as analytically more precise for the structural dimensions of the threat.

Information confrontation: The Russian doctrinal term for the treatment of cognitive operations as permanent rather than exclusively wartime activity, developed by the Russian military and intelligence community. Distinguished from the Western information warfare framing by its temporal scope: information confrontation is a continuous condition of strategic competition, not an instrument activated in the conduct of declared armed conflict. Core methods within the information confrontation doctrine include hack-and-leak operations, troll farms, state media amplification through outlets like RT and Sputnik, proxy amplification through domestic sympathisers and elite cultivation, and historical warfare (see historical warfare). The information confrontation framing is one operational instantiation of the broader reflexive control doctrine that unifies Russian cognitive operations theory (see reflexive control), and explains why episodic Western counter-

disinformation architectures structurally mismatch the threat: the operations they are responding to are continuous, while the response postures activate only at moments of acute political pressure.

Information ecosystem: The totality of actors, platforms, channels, norms, and incentive structures through which information is produced, distributed, amplified, and consumed within a society. Encompasses legacy media, social media platforms, search engines, messaging applications, influencer networks, and the algorithmic systems that govern content visibility and reach. The health of a democratic information ecosystem is determined not only by the accuracy of content circulating within it, but by the structural conditions shaping what populations see, what they trust, and what they are capable of evaluating. A degraded information ecosystem, characterised by platform fragmentation, algorithmic amplification of emotionally polarising content, declining institutional trust, and the erosion of shared information baselines, constitutes a structural vulnerability to cognitive warfare independent of any specific adversary operation.

Information influence: Finnish operational and legal term for the weaponisation of information to achieve political effects, explicitly broader than disinformation. Information influence encompasses true content deployed manipulatively, selectively accurate content, emotionally amplified content, and outright fabrication: the unifying element is intent to manipulate rather than factual falsity. Finland's use of this framing reflects a sophisticated understanding of the threat landscape documented throughout this report: adversaries do not need to lie to manipulate, and a defence framework limited to correcting false content will miss the majority of the threat. The term has begun to influence EU regulatory thinking, where the FIMI framework similarly moves beyond a false/true binary to focus on manipulation and interference as the operative harms.

Information warfare: The use of information and communications capabilities to gain advantage over an adversary by influencing, disrupting, corrupting, or denying their access to information, while protecting one’s own. NATO defines information warfare as an operation conducted in order to gain an information advantage over the opponent. Information warfare is the broader strategic concept; its constituent tools include psychological operations, electronic warfare, cyberspace operations, deception, and

operational security. Distinct from cognitive warfare in objective: information warfare targets the control and flow of information, while cognitive warfare targets the mental processes through which individuals interpret and act on information. In practice the two are deeply intertwined, with information warfare serving as a primary delivery mechanism for cognitive effects.

Narrative competition / narrative advantage: Terms used across multiple allied institutions, particularly in the StratCom tradition, to characterise the information environment as a sustained competition for dominant framing of events, actors, and values, rather than a series of discrete crises requiring episodic response. Narrative competition positions the information contest as structural and continuous: adversaries are always working to establish their preferred frames before events occur, and democratic institutions must maintain counter-narrative capacity at all times rather than only during crises. The framing is analytically useful for planning and resourcing. Its democratic tension is real: a state actively competing for narrative advantage risks instrumentalising public communication in ways that blur the line between legitimate public information and strategic influence operations. This report documents this tension as a recurring theme in field research across allied institutions.

Psychological warfare (PSYOPS): NATO defines psychological operations as planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives. Psychological warfare is the broader strategic concept of which PSYOPS is the institutionalised military expression. It encompasses the deliberate use of communication, imagery, symbolic action, and narrative to affect the emotional states, beliefs, and will of target populations, including adversary military forces, civilian populations, and third-party audiences. Distinct from cognitive warfare in scope and era: psychological warfare is an older, more operationally bounded concept focused on influence campaigns; cognitive warfare encompasses structural and technological manipulation of the conditions of thought itself, including through platform architecture, algorithmic amplification, and identity targeting. PSYOPS operates within democratic legal constraints and requires approval of target audiences

through the North Atlantic Council; cognitive warfare by adversaries operates with no such constraints.

Sammensatte trusler (composite threats): Norwegian term, literally "composite threats," used in Norwegian national security doctrine and institutions as the preferred equivalent of the English-language "hybrid threats." The terminological preference reflects a substantive distinction: where "hybrid" emphasises the blending of military and non-military means, "composite" emphasises the deliberate combination of multiple simultaneous pressure vectors across domains, including military, economic, informational, and political. Norway's institutional preference for this framing reflects a broader Nordic tendency toward precision in threat categorisation, and a concern that "hybrid" has become so broadly applied as to lose analytical utility. Sammensatte trusler maps closely to what this report describes as the multi-domain character of cognitive warfare campaigns.

Societal security: Finnish working term for the whole-of-society security model, encompassing physical, economic, psychological, and informational dimensions of national resilience under a single strategic frame. Broader than cognitive defence in scope: societal security addresses the full spectrum of threats to the functioning of society, from natural disasters and pandemics to hybrid campaigns and armed conflict. The Finnish model operationalises societal security through the Security Strategy for Society, which assigns specific preparedness tasks to every ministry, the private sector, civil society, and individuals. This whole-of-society assignment of responsibility, rather than the concentration of security functions in defence and intelligence agencies alone, is the feature this report identifies as most transferable to allied democracies currently building cognitive defence capacity. Finland's societal security model is increasingly studied by NATO partners as a template for resilience architecture.

StratCom (Strategic Communications): NATO, EU, and government usage for the coordinated use of communications activities by states or organisations to advance policy objectives, maintain public support, and counter adversary narratives. StratCom integrates public affairs, public diplomacy, military information support operations, and information operations into a coherent whole, premised on the idea that communication

is not an add-on to policy but a core instrument of statecraft. The NATO StratCom Centre of Excellence in Riga is the primary allied institution for research, doctrine development, and training in this domain. On the EU side, the East StratCom Task Force, operating under the European External Action Service, is the closest equivalent, focused specifically on countering disinformation in the Eastern neighbourhood. StratCom sits at the boundary between legitimate public communication and active influence operations, and democratic constraints on its scope are a recurring tension in field research: allied institutions consistently struggle to define where lawful counter-narrative activity ends and manipulation begins.

Annex C: Methodology and Interview Base

The findings presented in this report rest on a programme of primary field research conducted by the author between 2025 and 2026. That programme comprised over 100 semi-structured interviews with officials, practitioners, researchers, and civil-society figures across the Nordic and Baltic states, Central and Western Europe, Ukraine, Taiwan, the United Kingdom, Canada, and the principal institutions of NATO and the European Union. The research was commissioned by Konrad-Adenauer-Stiftung Canada.

All interviews were conducted on a not-for-attribution basis. This was a strict and consistent methodological commitment across the whole project, extended to every participant regardless of seniority or subject. Accordingly, no statement, finding, argument, or judgement anywhere in the report is attributed to any named individual or to any specific institution, and nothing in this annex should be read as linking a particular body to a particular view. The interviews were semi-structured: each followed a common thematic framework while allowing the conversation to develop according to the expertise of the participant.

The list below is provided to convey the breadth and institutional depth of the primary research rather than to serve as a complete record. It is illustrative, not exhaustive. Institutions are presented as a single consolidated roster, not organised by country, chapter, or theme, and a number of interviews are not reflected here. In some cases naming an institution would, given the specificity of the subject or the small size of the body concerned, risk identifying an individual participant. Where that risk arose, the institution has been described at the level of its category rather than by name, or omitted.

The roster therefore combines named institutions with category-level descriptors, and its purpose is to indicate the character of the engagement rather than to map it.

Among the institutions engaged, those consulted included:

Government, defence, and security

- Ministries of foreign affairs, defence, justice, the interior, and culture across the states studied
- National security and intelligence services
- Armed forces strategic communications and information-operations elements
- National civil-protection, crisis-management, and emergency-supply agencies

Counter-disinformation and strategic communications

- National and multinational counter-disinformation, psychological-defence, and strategic-communications bodies among the states and institutions studied

NATO, European Union, and multinational institutions

- NATO Strategic Communications Centre of Excellence
- NATO Science and Technology bodies
- European Centre of Excellence for Countering Hybrid Threats
- European Union Institute for Security Studies
- European Union external-action and digital-policy bodies responsible for countering foreign information manipulation and interference and for platform regulation

Research institutes, think tanks, and universities

- Stockholm International Peace Research Institute
- Norwegian Institute of International Affairs
- Centre for European Policy Analysis
- Stockholm Centre for Eastern European Studies
- Centre for European Reform
- Department of War Studies, King's College London
- Hertie School
- Aalto University
- Leiden University
- Crisis Management Initiative
- Royal Danish Defence College
- Swedish Defence University
- Norwegian Defence University College

- Foundation for Strategic Research
- Taiwan Asia Exchange Foundation
- McGill University
- York University

Civil-society, fact-checking, and civic-technology organisations

- StopFake
- OpenMinds
- Ukraine Crisis Media Center
- Alliance4Europe
- DisinfoWatch
- eQualitie
- Further fact-checking and digital-resilience organisations engaged across the states studied

News media

- Journalists covering foreign interference, disinformation, and security affairs

Private sector

- Defence-industrial, cybersecurity, and technology firms engaged on information integrity, attribution, and critical-infrastructure protection

2026

Cognitive Warfare: A Democratic Defence

VOLUME 2: COUNTRY SUMMARIES

ELIZABETH ANDERSON WITH AMBASSADOR EITVYDAS BAJARŪNAS

Table of Contents

INTRODUCTION **4**

COUNTRY CASES **7**

CHAPTER 18: UKRAINE 7
The threat environment from the Ukrainian vantage *9*
Kinetic-cognitive integration as Ukraine's operational signature *13*
Civil society as the load-bearing substrate *15*
Strategic communications and cultural resistance *18*
Honest limitations *22*
What travels from Ukraine *24*
Ukraine's partner landscape *25*
CHAPTER 19: FINLAND 30
Historical and Structural Foundations *30*
The Architecture in Practice *33*
Transferability *36*
Honest Limitations *38*
Partner Landscape *39*
CHAPTER 20: SWEDEN 43
Security culture and the Swedish approach to defence *43*
The threat environment *45*
What Sweden has built: MPF as institutional design *48*
Honest limitations *51*
What travels from Sweden *53*
Sweden's partner landscape *54*
CHAPTER 21: NORWAY 57
Security culture and Norway's approach to defence *58*
The threat environment *59*
The architecture in practice *61*
Honest limitations *63*
What travels from Norway *64*
Norway's partner landscape *64*
CHAPTER 22: DENMARK 67
Security culture and Danish terminology *67*
The 180-year design tradition *68*
The threat environment *72*
The Greenland case as test *73*
Coordination architecture and honest limitations *76*
What Denmark builds against the threat and the central exposure *76*
Partner landscape *78*
What travels: lessons from the Danish architecture *79*
CHAPTER 23: ESTONIA 82
Security culture and the bet at restored independence *82*
Threat environment *83*
What Estonia has built *86*

Where Estonia is still exposed ... *88*
What travels ... *90*
Partner landscape ... *90*
CHAPTER 24: LATVIA ... 94
Security culture and the Latvian approach to defence ... *94*
The threat environment ... *95*
What Latvia has built ... *98*
Honest limitations ... *100*
What travels from Latvia ... *102*
Latvia's partner landscape ... *103*
CHAPTER 25: LITHUANIA ... 107
Opening Argument ... *107*
Threat Actors and Methods ... *108*
What Makes Lithuania Distinctive: Three Pillars ... *110*
The Russian-Speaking Minority, Soviet nostalgia and the Information Environment ... *114*
Coordination Architecture ... *116*
Honest Limitations ... *118*
What Lithuania Models for Others ... *119*
Partner Landscape ... *119*
CHAPTER 26: FRANCE ... 122
Security culture and France's approach to information sovereignty ... *122*
The threat environment ... *125*
What France has built: VIGINUM, French Response, and the 2026-2030 Strategy ... *128*
Honest limitations ... *130*
What travels from France ... *131*
France's partner landscape ... *134*
CHAPTER 27: THE UNITED KINGDOM ... 138
Terminology and Framing ... *138*
Threat Actors ... *139*
Institutional Architecture: Strength and Weakness ... *140*
Whole-of-Society Defence Gap ... *143*
Operational Capability Gaps ... *144*
Reform Agenda (Emerging Thinking) ... *144*
Allied Cooperation and External Dimension ... *145*
Points of Convergence ... *146*
CHAPTER 28: POLAND ... 148
Threat Actors ... *148*
What Makes Poland Distinctive ... *150*
Coordination Architecture ... *150*
Honest Limitations ... *151*
Institutional Architecture ... *152*
Partner Landscape ... *153*
CROSS-CUTTING ANALYSIS ... 154
CHAPTER 29: LESSONS ACROSS CASES ... 154
Foundations precede architecture ... *154*

Adversaries do not start fires *161*
Two framework findings the cluster surfaces *162*
Three universal institutional gaps the cluster surfaces *164*
Conclusion *167*

ABOUT THE AUTHOR **169**

ABOUT THE DISTINGUISHED ADVISOR **170**

Introduction

This second volume provides the country evidence base that grounds Volume I's policy argument. It is presented as a separate volume because the two pieces of work answer different questions and serve different readers.

Volume I asks what democracies, and Canada in particular, should do about cognitive warfare, and is structured so ministerial staff can read it and brief on it. Volume II asks what has actually been tried, what has been learned, and what the experience tells the wider Alliance about the design choices ahead.

A reader who needs the policy argument can it in Volume I, and find the evidence in Volume II.

The selected countries cover four analytical clusters. The Nordic-Baltic security architecture provides the densest evidence base, with chapters on Finland, Sweden, Norway, Denmark, Estonia, Latvia, and Lithuania. This is the cluster the report draws on most directly, both because it contains the most institutionally developed cognitive defence architectures in the Alliance and because its members share enough structural commonality to permit comparison. The Western European institutional leadership tier is represented by France and the United Kingdom. France carries particular weight because VIGINUM is the most cited transferable model across the report, and because the lineage running from the G7 Rapid Response Mechanism to VIGINUM has direct Canadian relevance. The frontline pressure cases, Ukraine and Poland, ground Volume II in the operational realities that define what cognitive defence under sustained adversarial pressure looks like in practice.

What is not in this volume is as deliberate as what is. Germany and Canada are treated in Volume I as primary cases, given that the report is commissioned by Konrad-Adenauer-Stiftung Canada and addresses itself principally to those two policy communities. The EU and NATO institutional assessment also sits in Volume I, where it carries the architectural weight of the Canada-Germany-EU corridor argument and the Allied Cooperation recommendations.

Volume II is therefore a partner-state and frontline-state collection: the countries Canada and Germany have most to learn from, the institutions Canada and Germany must align with, and the contexts that show what works and what does not when democratic societies are placed under sustained cognitive pressure.

The volume rests on field research conducted during three European research trips between November 2025 and March 2026, and on over one hundred interviews. Field research was carried out in eleven of the thirteen country contexts, and at the principal European and transatlantic institutions, including the EU and NATO bodies whose assessment is developed in Volume I. The chapter on Ukraine draws on interviews conducted with Ukrainian interlocutors and on the substantial existing literature; the chapter on Poland draws on interviews with interlocutors outside the country and on secondary sources.

The country chapters with primary field research carry the richest interview density and the most detailed institutional readings. Where on-record attribution has been granted, it appears in the endnotes; where it has not, contributions are referenced by role and vantage. This is a deliberate choice to protect the candour of the field research and the working relationships that made it possible.

The primary field-research cases of Finland, Sweden, Estonia, and Lithuania carry the richest evidentiary base and treat the full six-layer cognitive defence architecture in depth. The substantive supporting cases of Norway, Denmark, and Latvia cover analytically distinctive contributions at moderate depth: Norway’s transparency architecture, Denmark’s parliamentary consensus and the December 2025 DDIS decision to name the United States as a threat actor, and Latvia’s position as the host of the NATO Strategic Communications Centre of Excellence and the country managing the cluster’s most acute minority integration challenge. The focused supporting cases of the United Kingdom, and Poland treat specific design elements rather than the whole architecture: the UK Online Safety Act and 77th Brigade, and the Polish institutional architecture across NASK, ABW, SKW, and RCB. Ukraine and France function as referent chapters that other parts of the manuscript cite throughout.

Each country chapter is organised around the same analytical architecture set out in Volume I: two horizontal foundations of social infrastructure below and political will above, and six layers covering societal resilience, information environment integrity, platform architecture, detection and attribution, active defence, and sovereign response capacity. They concentrate on the layers where the country in question has something distinctive to contribute and treat the others more briefly. The framework is the analytical spine of the volume.

The final chapter is a set of cross-case findings. A reader who wants the synthesis without the full evidence base can read the introduction, the executive summary in Volume I, and Chapter 29, and have the analytical core of the volume in hand. A reader who wants the evidence behind the synthesis can read the country chapters.

A closing note on tone. The country chapters are written to be useful to practitioners and honest about their limits. They name what is working, what is not working, and what is unresolved. Where a country has built something the rest of the Alliance should be studying, the chapter says so. Where a country has built something that will not travel, the chapter says that too. This is not a ranking exercise. It is an attempt to read what thirteen democracies have learned about defending themselves in the cognitive domain, and to set that reading on the table for the policy communities now making the next round of design choices.

Country Cases

Chapter 18: Ukraine

Ukraine has long been on a critical fault line between East and West: two different worldviews in contest with one another. The geography is part of the answer but not all of it. Ukraine's European history is centuries old. In 1051, Anna of Kyiv, daughter of Grand Prince Yaroslav the Wise of Kyivan Rus and Ingegerd of Sweden, was crowned Queen of France at Reims Cathedral upon her marriage to Henry I; her sisters became queens of Norway, Hungary, and Poland; the eleventh-century Kyivan dynasty was a hub of European royal marriages a generation before the Norman Conquest. Russia's contemporary war is fought, in part, against the memory of these ties. The Russian Federation wishes to portray Ukraine as not an independent nation but a misplaced part of Russia, that Ukrainian culture is a folkloric branch of Russian culture, and that Ukrainian history is part of Russian history. The position requires erasing Ukrainian independent history and reimagining it as Russia's own. The defensive task is to recognise the distortion as cognitive operation rather than as a perspective deserving of equal weight.[1]

Ukraine's post-1991 trajectory is best understood as a long contest inside Ukrainian society between two orientations: a European orientation that was historical and geographical (with Western Ukraine having been more deeply integrated into the European cultural and political space) and that grew steadily across the post-Soviet period, and a Soviet-era orientation sustained less by generational loyalty than by the institutions, oligarchic networks, and security architectures inherited from the Soviet system that retained influence regardless of which generation occupied them. Older Ukrainians were not uniformly resistant to the European turn. Many participated in it, including at the front of the Orange Revolution and Maidan. What persisted across the period was not a generational divide but the structural inertia of the post-Soviet state itself, in which power, capital, and influence had been organised inside networks that pre-dated independence and that did not dissolve with it. The European orientation prevailed not by default but because it was chosen, under sustained pressure, at increasing cost, and against the structural resistance of those networks. The threefold

character of the Maidan revolution, as the political-science literature now describes it, captures something the simpler generational framing misses: the revolution was simultaneously a national-liberation struggle against Russian imperial reassertion, a political-democratic struggle against an autocratising and corrupt government, and a social struggle against the post-Soviet oligarchic system. Through the 1990s, independent Ukraine pursued principled non-alignment, joining the North Atlantic Treaty Organization's Partnership for Peace in 1994 and signing the Ukraine-NATO Charter in 1997 without aspiring to membership. The NATO Bucharest Summit in 2008 declared that Ukraine "will become" a NATO member, but the path to membership did not consolidate into a near-term institutional outcome in the years that followed. The European Union orientation matured later and more durably. President Leonid Kuchma operated a multi-vector foreign policy through the 1990s and early 2000s, balancing Russia and the West. The Orange Revolution of 2004 to 2005 produced a Western turn under President Yushchenko; the election of Yanukovych in 2010 produced a reversion. The Maidan revolution of 2013 to 2014 was triggered by Yanukovych's rejection, under Russian pressure, of the European Union Association Agreement, and the choice that emerged from Maidan was specifically European Union accession rather than NATO membership. Russia's annexation of Crimea and war in the Donbas followed within weeks. Ukrainian public support for European Union membership has been the durable feature of the post-2014 period. NATO support moved sharply upward after the full-scale invasion of February 2022 but operates inside a more contested institutional and political environment internationally. The European Union accession path remains the more probable institutional outcome, not because of any weaker Ukrainian willingness to join NATO, but because of clear opposition from key Allies, including the United States and Germany, to accepting Ukraine into the Alliance.[2]

The choice was not pre-ordained. It was made, against the structural resistance of post-Soviet networks of power, by a coalition of Ukrainians from across generations, at increasing cost. Russia's war is the kinetic expression of an attempt to reverse the choice. Every kinetic operation Russia conducts in Ukraine serves a cognitive objective that precedes it: the proposition that the choice was illegitimate, that Ukrainian existence as a separate national identity is open to question, and that the post-1991

European order is itself contingent on Russian assent. Due to its position on the fault line of two ideological worldviews both competing for influence, Ukraine has built out of necessity a robust defence against the threat of foreign influence through institutions and through civil society, through digital infrastructure and through cultural production, through state action and through the everyday work of writers, journalists, artists, teachers, and citizens. The architecture was not designed in advance. It was assembled under existential pressure by people who understood, well before their Western counterparts did, that the war they were fighting was a cognitive war fought through kinetic and non-kinetic means simultaneously. Ukraine's continued survival is a testament to both Ukrainians' courage and resilience and their ability to see the battle for hearts and minds as just as legitimate a form of warfare as traditional kinetic military attack.

The threat environment from the Ukrainian vantage

Chapter 3 develops the Russian cognitive warfare doctrine in full and Chapter 4 develops the corresponding theory of adversary success on which Russian operations are calibrated. This chapter does not retell that material; what follows is what is distinctive about how the doctrine operates against Ukraine specifically. The first thing the Ukrainian vantage confirms is that Russia is conducting a single war on multiple fronts. The kinetic war against Ukraine is the most intense expression and the most deadly. The sustained, lower-intensity war against the rest of Europe and the broader West, which Chapter 3 documents as the shadow-war architecture combining cognitive operations, drones, sabotage, arson, GPS jamming, migration weaponisation, subsea cable attacks, assassinations of dissidents abroad, energy coercion, and election interference, is an extension of the same campaign at lower kinetic threshold. The transferability of the Ukrainian experience to partner democracies depends on the recognition that what Ukraine has been absorbing at high intensity since 2014 is what the rest of the West is absorbing at increasing intensity now.

The second confirmation the Ukrainian vantage offers is that the integration of kinetic and cognitive operations on the Russian model, which Chapter 3 describes through the doctrinal frame of reflexive control, is not an analytical observation but a foundational

premise in Russian military thought. In the Ukrainian environment, this is operationally legible in ways it is not yet legible to most Western institutional architectures. Ukrainian practitioners since 2014 have built the analytical and institutional capacity to read Russian operations across kinetic and non-kinetic domains as instruments of a single campaign rather than as separate phenomena to be addressed by separate institutions. The lesson the Ukrainian vantage offers is methodological: defensive architecture should be calibrated against the integrated objective of adversary decision-making paralysis, not against the persuasion metrics Western counter-disinformation institutions have inherited.

A third feature is that Russia does not start the societal fires it exploits at population scale. Russian operations conduct kinetic ignition where it serves the operation, including the arson and sabotage campaign across European Union member states since 2023. At population scale, however, the pattern is amplification rather than ignition. Russia identifies fires already burning inside target societies and pours gasoline on them. The grievances Russian operations amplify are real: inequality, regional disparity, identity insecurity, anti-elite sentiment, the perceived hypocrisy of liberal-democratic states on questions of human rights. Russian operations succeed not because they introduce false premises but because they amplify existing premises target societies have not adequately addressed. The framework chapters arrive at the claim that cognitive defence rests on social-infrastructure foundations preceding any institutional architecture built on top of them through analytical reasoning independent of the Ukrainian case. The Ukrainian operational evidence is the clearest contemporary corroboration of that claim.

A fourth feature distinguishes the Russian operational signature in Ukraine and bears on the framework treatment Chapter 4 develops. Russia does not value the lives of its own people in the way Western states value the lives of theirs, and the operational consequence is that Russia can sustain casualty rates and operational tempo no Western adversary will match. The casualty rates Russia has sustained on the kinetic front in Ukraine, currently averaging approximately five thousand soldiers killed and wounded per week for minimal territorial gain, are not the casualty rates of a state

calculating cost against benefit in any framework Western analysts recognise.[3] The same logic operates in the cognitive domain. Russia continues operations long past the point at which any rational cost-benefit calculus would call for adjustment, because operational tempo no Western adversary will match is itself the cognitive operation: the demonstration of capacity to outlast, which Russia counts as a strategic gain in itself. The mundanisation technique Chapter 4 develops as a framework-level concept finds its sharpest operational expression in Ukraine: each successive winter campaign against civilian and energy infrastructure, each round of mass civilian casualties, accumulates inside the international response not as a discrete event demanding action but as the new background condition against which subsequent events are measured. The same disregard for cost extends from human life to material expenditure, with Russia willing to absorb attritional losses no Western adversary would sustain.

Two further features require attention because they are Ukraine-distinctive (with some exception of the case of the Baltic states) and not developed at the framework level beyond the all-platforms reference to "religious institutions." The first is the role of the Russian Orthodox Church Moscow Patriarchate as intelligence vector. The Russian Orthodox Church operates as a foreign-policy and intelligence instrument of the Russian state, not as a religious institution. Patriarch Kirill served as a KGB agent under the codename Mikhailov, with his predecessor Patriarch Alexis II serving under the codename Drozdov; the Russian Orthodox Church's March 2024 policy document declared the war in Ukraine a holy war and asserted the Church's sole authority over the territory of modern-day Ukraine; Ukrainian foreign intelligence assesses the Russian Orthodox Church as ninety-nine percent controlled by the Russian Federal Security Service and Foreign Intelligence Service; the Ukrainian Security Service has prosecuted dozens of Russian Orthodox Church priests for espionage, with one priest in Sumy Oblast sentenced to fifteen years for relaying targeting information to Russian forces.[4] In August 2024, Ukraine passed legislation banning the activities of the Russian Orthodox Church on Ukrainian territory. Sweden withdrew funding from Russian Orthodox Church-affiliated bodies in February 2024, Lithuanian authorities closely monitor the Russian Orthodox Church because of concerns over its role in supporting pro-Kremlin narratives and Russian influence operations, Estonia designated the

Moscow Patriarchate a sponsor of Russian aggression in May 2024, but most partner governments have continued to engage the Russian Orthodox Church inside frameworks that treat it as a religious institution to which religious-freedom protections apply. This is a category error with operational consequences.

The second is the role of Russian cultural production as the operational substrate of Russian soft power. Russia has invested centuries in the proposition that Russian culture is a civilisational achievement that operates above politics and that confers on Russia a moral standing distinct from the standing of the Russian state itself. Russian cultural promotion is not funded from a Russian Ministry of Culture in the institutional sense Western states would expect. Rossotrudnichestvo, the Russian state agency responsible for cultural diplomacy, draws its institutional positioning from inside the Russian state's foreign-and-security policy apparatus, alongside Rosatom, which manages nuclear energy as a foreign-policy and security instrument rather than a commercial energy enterprise.[5] The institutional placement signals the function. The doctrinal substrate is the "Russkiy Mir" ("Russian World"), an ideological concept promoted by the Kremlin that portrays Russian language, culture, Orthodoxy, and political influence as forming a single civilisational space extending beyond Russia's borders. Its Western-facing instantiation, the narrative of the "good Russian" deployed in audiences sympathetic to the proposition that the Russian state can be distinguished from Russian society, has the operational effect of preserving the imperial substrate that any durable resolution of the Russia-Ukraine war will have to engage. A Russia that has not undergone the kind of national-level reckoning Germany underwent after 1945 will remain a threat actor across multiple domains against its neighbours regardless of who occupies the Kremlin. Cognitive warfare is one domain among several, but it is the domain where Russian state institutional architecture is most fully integrated with state strategic objectives, the domain Russian doctrine treats as the foundational substrate rather than as a supplement to kinetic operations, and the domain Western institutional frameworks are least equipped to recognise as warfare at all.

Kinetic-cognitive integration as Ukraine's operational signature

What Chapter 3 names as the Russian doctrinal integration of kinetic and cognitive operations is, in the Ukrainian environment, the daily operational reality across every front. Russia conducts a single war against Ukraine in which the kinetic and the cognitive serve the same strategic objective and are calibrated to the same operational metrics. The Western framework, which treats kinetic operations as the threshold past which warfare becomes serious and treats non-kinetic operations as the lesser category of hybrid threats, fails not only at the level of analytical precision but at the level of basic recognition. The Ukrainian operational response over a decade has built the institutional and analytical capacity to read the integration as Russia conceives it, and to act inside that recognition. The defensive doctrine the Ukrainian vantage produces, including the application of kill-chain methodology to information-operations infrastructure rather than to discrete narratives, is developed at the framework level in Chapter 3 and is applied through this chapter at the institutional level Ukraine has built.[6]

The campaign against Ukrainian energy infrastructure is the clearest worked example. Russia has conducted four winters of campaigns against Ukrainian energy infrastructure, each more sophisticated than the last. The first phase, from late 2022 through spring 2024, focused on transmission and distribution assets. The second phase targeted generation directly. The third phase, beginning in autumn 2025, expanded to natural gas infrastructure with strikes on production, storage, and distribution facilities designed to deprive Ukrainian households of heating during the fourth winter of war. By late 2025, Ukrainian generating capacity had fallen from approximately 33.7 gigawatts pre-war to approximately 14 gigawatts, with peak winter demand approaching 17 gigawatts; approximately 60 percent of Ukrainian natural gas production capacity had been destroyed; 18 large combined-heat-and-power plants and over 800 boiler houses had been damaged or destroyed; the 30 October 2025 strike alone deployed 705 missiles and drones in a single coordinated barrage.[7] The operational logic is not the destruction of infrastructure as an objective in itself. The campaign targets infrastructure as the kinetic instrument of a cognitive objective: the breaking of Ukrainian will-to-resist through cold, dark, and exhaustion, and through the continued death and destruction of Ukrainians and their way of life. The European

Union Institute for Security Studies has framed the campaign as a hybrid energy war in which physical attacks on infrastructure are coupled with disinformation campaigns targeting the political consensus sustaining Ukrainian energy resilience.[8]

The Ukrainian response demonstrates the integration at the defensive level. The state, with the support of the European Union, its member states, and other donors, has rebuilt energy infrastructure under sustained kinetic attack, decentralised generation, integrated Western air defence into the protection of energy facilities, and continued to operate critical state functions through blackouts. The cognitive defence happens at the population level. Ukrainian society has continued to function, work, study, marry, bear children, and attend concerts and theatre. Ukrainians have read books, written poetry, and sung Ukrainian songs in conditions Russian operational planners assumed would produce social collapse. In Kyiv during the winter blackouts, courtyard parties organised by residents and DJs became viral, with hundreds gathering in residential complexes for nights of music, food, and warmth that local businesses and neighbours rapidly converged to support; the parties were documented across Ukrainian and international media as a population-level refusal to allow Russian operational pressure to dictate the conditions of Ukrainian social life.[9] Russia's targeting of energy infrastructure to break Ukrainian will-to-resist has failed not because Ukraine has absorbed the kinetic damage but because Russia's war has reinforced rather than diminished the connection Ukrainians feel to their culture and their communities. The framework chapters argue that the attack surface adversaries exploit is the absence of connection inside target societies. Ukraine has built a society in which people feel connected to their culture and to each other under sustained kinetic threat, and the connection is what the energy campaign has been calibrated, and failed, to break.

The Ukrainian institutional architecture has now formalised this recognition at the cabinet level. On 14 January 2026, the Verkhovna Rada appointed Mykhailo Fedorov as Minister of Defence. Fedorov had served since 2019 as First Deputy Prime Minister and Minister of Digital Transformation, the architect of Ukraine's civic-digital infrastructure: Diia (the unified state services platform), eVorog (the citizen-reporting application that enabled crowdsourced intelligence on Russian troop movements during the early phase

of the full-scale invasion), Brave1 (the defence-technology cluster coordinating Ukrainian drone and counter-drone development), and the unified drone-operations system. Mstyslav Banik, the launch lead for Diia, was appointed Deputy Minister of Defence on 26 March 2026.[10] The restructuring formalises at the cabinet level what was already happening operationally: the civic-digital infrastructure, the kinetic operations infrastructure, and the cognitive-defence infrastructure are no longer separate domains administered by separate ministries. They are a single fused operational architecture, now administered through a single ministerial portfolio whose previous occupant designed and built the integration. No other case in this volume documents this degree of institutional fusion. The lesson for democracies that have not faced existential threat is not that they should replicate the Ukrainian institutional architecture. It is that the conceptual integration that produced it is a defensive requirement, and that democracies operating inside the inherited Western institutional separations between civilian and military, between kinetic and cognitive, between digital and physical, are operating inside frameworks Russia has designed its operations specifically to defeat.

Civil society as the load-bearing substrate

What the opening framing of this chapter describes in general terms, the institutional and operational record demonstrates in specific terms. The inherited Western assumption treats civil society as a supplement to state institutional capacity, useful where state institutions are inadequate but not load-bearing in any structural sense. The Ukrainian case demonstrates the opposite. From 2014 through 2021, Ukrainian civil-society organisations carried the cognitive-defence function alone. There was no Centre for Countering Disinformation, no Centre for Strategic Communication, no institutional architecture inside the National Security and Defence Council with operational responsibility for the cognitive domain. There was civil society, and the function got carried because civil society carried it.[11] The institutional architecture that has emerged since 2021 has not displaced the substrate. It sits on top of it.

StopFake was founded in March 2014 at the Mohyla School of Journalism in Kyiv, in the immediate aftermath of the Russian annexation of Crimea, by a coalition of journalism faculty and students who recognised, before most state institutions did, that the Russian

invasion of Ukrainian territory was accompanied by an unprecedented information operation. The organisation's methodology, summarised as monitor-archive-debunk, treats Russian disinformation as a system requiring sustained pattern-recognition rather than discrete incidents requiring case-by-case rebuttal. The system's operational architecture is mapped through continuous monitoring of Russian state media, Russian-language social-media networks, and the Russian-influence ecosystem inside target countries. StopFake operates in fourteen languages and is one of Meta's third-party fact-checking partners.[12] The Ukraine Crisis Media Centre was founded in February 2014 in response to the institutional vacuum that followed President Yanukovych's departure: no functional presidential office, unresolved questions of authority, Russian forces already in Crimea, no state institution responsible for communicating accurate information. The Centre has never received funding from the Ukrainian state or from Ukrainian large business actors with political affiliations. The Hybrid Warfare Analytical Group was established within the Centre in 2017, four years before any Ukrainian state institution formally assumed responsibility for cognitive-defence work. The Group's training programmes have included journalists and analysts from African, Latin American, Southeast Asian, and Indian institutions, deliberately targeting the regions where Russian operational success has been most extensive.[13]

A significant analytical contribution from inside the Ukrainian civil-society ecosystem has been the development of what practitioners increasingly describe as narrative intelligence. The concept treats the analysis of adversary narratives as an intelligence discipline analogous to signals intelligence or human intelligence: a discipline that produces operational indicators of adversary intent, capability, and decision-making by tracking the volume, intensity, and pattern of adversary narratives over time. The methodological foundation is the recognition that Russian narratives are systematically produced inside an operational architecture that synchronises narrative production with kinetic operations, political operations, and diplomatic operations. By tracking narrative patterns, analysts can predict subsequent operational moves. StopFake practitioners report having predicted the timing and scope of the full-scale invasion of February 2022 by tracking the intensity and volume of Russian disinformation narratives in the weeks and months preceding it.[14]

The institutional architecture that has emerged inside the Ukrainian state since 2021 sits on top of the civil-society substrate. The Centre for Countering Disinformation, established in March 2021 by a decision of the National Security and Defence Council and operational since November 2021, is a coordinating body within the National Security and Defence Council architecture, not a portfolio ministry. Its open-source methodology operates on publicly available information rather than classified intelligence, which allows its analytical products to be shared with international partners and contributes to the Centre's standing as an international reference institution. The UK House of Commons Foreign Affairs Committee, in its March 2026 *Disinformation Diplomacy* report, named the Centre for Countering Disinformation alongside Sweden's Psychological Defence Agency and France's VIGINUM as the three institutional models the UK should look to in building its own counter-disinformation architecture. The Royal United Services Institute has characterised the Centre as "the most high-profile example" of the kind of dedicated capability the UK lacks, and as functioning as "an international hub for collecting and analysing information to enhance cognitive resilience and help partners mitigate disinformation infrastructure." Inside Ukraine, the perception of the Centre is more mixed. Professional commentary across the Ukrainian counter-disinformation community has identified gaps between the institutional mandate and operational delivery: public communications output that has not consistently matched the analytical mandate, episodes of public controversy including a July 2023 publication that conflated international commentary with adversary-aligned messaging and prompted institutional review, and continuing staff turnover that has constrained the build-out of specialised analytical capacity inside the institution while comparable analytical capacity sits more maturely inside civil society. The Centre is working through these institutional questions, and the trajectory is one of institutional development under operational pressure rather than institutional failure: an institution that partner counterparts cite as a reference model is, by definition, doing more than it is failing to do.[15] The Centre for Strategic Communication and Information Security operated from March 2021 through October 2025 within what was then the Ministry of Culture and Information Policy, with operational scope including government communication coordination, counter-narrative development, the Kyiv Stratcom Forum, and the *In Case*

of Emergency or War civil-defence brochure, prepared in 2022 ahead of and during the early phase of the full-scale invasion and distributed in over 100,000 copies across frontline territories. In October 2025, the strategic communications portfolio was removed from the ministry and is being transferred to a separate institution still being constituted at the time of writing.[16] The Ukrainian government's institutional architecture for strategic communications is in active flux.

The relationship between Ukrainian civil-society organisations and the Ukrainian state is operationally distinct from the relationship between counter-disinformation civil society and state institutions in most other partner democracies. The distinction is not that Ukrainian civil-society organisations work with state institutions; civil-society organisations in most democracies do. The distinction is that the analytical work itself is carried by independent civil-society institutions rather than by state institutions with civil-society engagement as a supplementary input. Ukrainian civil-society organisations operate at their full operational potential because they are independent of Ukrainian state funding and direction. The civil-society organisations work with Ukrainian state institutions across the broader counter-disinformation environment, including with the Ministry of Digital Transformation on artificial-intelligence counter-tooling and with the Ministry of Foreign Affairs on situational awareness, but the operational relationships are structured to preserve civil-society independence. The institutional independence is itself an operational asset: when StopFake debunks a Russian disinformation operation, the rebuttal travels further in international audiences than a state institution's rebuttal would, because international audiences treat independent civil-society analysis differently than they treat state communications about the same operation. This is the operational core of the civil-society-as-load-bearing argument: institutional architecture sits on top of civil society because civil society can do operational work that state institutions cannot, and the integrity of the civil-society function depends on its institutional separation from the state apparatus.

Strategic communications and cultural resistance

Since the full-scale invasion, Ukrainian strategic communications have operated through an architecture that combines centralised messaging from the presidency with

decentralised amplification across civil society, expert networks, journalists, the cultural sector, and the Ukrainian diaspora. The centralised messaging from the presidency, conducted by President Zelenskyy directly and by the institutional team built around him during the war's first years, established a coherent voice during the period when Western publics were forming the framings through which they would interpret the war. The voice was effective because it integrated three communicative registers simultaneously: pragmatic-interest framing (what Western states stood to gain by supporting Ukraine, what they stood to lose by not), ethical-values framing (the proposition that the war was a defensive operation by a democracy against an authoritarian invasion), and emotional-connection framing (the personal, lived, granular reality of Ukrainian suffering, resistance, and aspiration). The integration of the three registers, calibrated to target audiences, is the most operationally significant transferability finding from the Ukrainian strategic communications experience.[17]

The architecture has shifted across the war's phases. The opening framing of the war as a defensive operation by a democracy against an authoritarian invasion produced limited resonance in Global South audiences. The Ukrainian architecture adapted: the ethical-values framing shifted toward rules-based international order versus the right-of-the-might, designed to resonate inside audiences with historical experience of Western military intervention. The arrival of the current United States administration produced a further adaptation toward pragmatic-interest framings calibrated to United States strategic and economic interests in a Ukrainian outcome that does not produce regional collapse. By mid-2026, as United States engagement on Ukraine softened, the architecture shifted once again, back toward European audiences and European Union institutional partners as Ukraine's most durable strategic constituency.[18] The pattern of adaptation is itself a transferability finding: strategic communications in cognitive-warfare environments require continuous calibration to target audience framings rather than fixed messaging conducted as if the messaging were the operational objective.

The decentralised amplification of Ukrainian strategic communications has been operationally as significant as the centralised messaging, and likely more transferable. The pattern is not one-voice policy. It is many-voice coherence. The coherence comes

from shared values and shared information access rather than from centralised message discipline. The architecture has integrated humour, memes, irony, and ridicule as operational instruments alongside the more conventional registers of policy advocacy and public diplomacy.[19] Emotional-register communications are not ancillary to serious policy work; they are part of how serious policy work succeeds in audiences whose engagement with policy questions runs through emotional connection before it runs through rational analysis.

The deepest layer of Ukrainian cognitive defence is cultural. The Russian assertion that Ukraine does not exist as a separate nation is the operational predicate of the war, and Russian operations against Ukrainian cultural institutions, Ukrainian language use, the Ukrainian Orthodox Church separated from the Moscow Patriarchate in 2018, Ukrainian museums and archives in occupied territories, and Ukrainian publishing houses, theatres, and music venues are not incidental to the kinetic operations. They are the cognitive operations the kinetic operations serve. The objective is the erasure of Ukrainian existence as a separate national identity.

Ukrainian cultural resistance operates as the response. Ukrainian cultural events in Kyiv sell out in minutes; the pattern is consistent across Kharkiv, Dnipro, Lviv, and Kherson. Concerts, theatre productions, poetry readings, book launches, art exhibitions, film screenings, and cultural festivals operate at near-capacity inside cities subject to sustained kinetic attack. PEN Ukraine has organised poetry readings at the front lines, with Ukrainian poets travelling to active combat zones to deliver readings to soldiers and civilians. Children's book events are organised in front-line cities including Kherson. The Ukrainian dance competition *Tantsi z Zirkamy* has continued production through the 2024 and 2025 winters, with episodes broadcast during scheduled blackouts and featuring Ukrainian military veterans dancing on prosthetic limbs.[20] The pattern is the population-level demonstration that the Russian operational objective of breaking Ukrainian will-to-resist through death and destruction has failed.

Ukraine has invested across the post-2022 period in the institutional decolonisation of Ukrainian cultural and academic categories from the inherited Russian categories that have framed Ukrainian cultural production in Western institutional contexts. The Office

of the First Lady of Ukraine, under Olena Zelenska, has led the institutional architecture of this work: the Global Coalition of Ukrainian Studies (sixty participating institutions across twenty-three countries as of late 2025), the Ukrainian Bookshelf project (over two hundred Ukrainian bookshelves at universities and cultural institutions across fifty countries), Books Without Borders (between 260,000 and 280,000 Ukrainian books distributed to displaced Ukrainian children across twenty countries), Ukrainian-language audio guides at significant cultural sites globally (eighty-nine in forty-seven countries), and the annual Summit of First Ladies and Gentlemen.[21] The Harvard Ukrainian Research Institute marked its fiftieth anniversary in 2023 with the First Lady's institutional engagement, and the broader project of separating Ukrainian studies from inherited Slavic studies and Russia studies frameworks is now formally underway.

The analytical connection to the volume's framework is straightforward. Chapter 6 argues that connection is the root of cognitive resilience, that every psychological need adversaries exploit is fundamentally a need for connection, that no counter-messaging architecture can compete with manipulation that validates lived experience, and that the attack surface adversaries exploit is emotional before it is informational. The Ukrainian case provides the operational evidence: a population sustained by cultural production and everyday-life continuity under sustained kinetic threat is structurally harder to manipulate, because the population's underlying identity is anchored in a cultural inheritance adversary operations cannot reach. The defensive work is at the level of substrate, not counter-narrative. Democracies that have under-invested in cultural production, in arts funding, and in the institutional infrastructure of cultural and civic life have left themselves vulnerable to adversary operations that target the substrate-level foundation of cognitive defence. The vulnerability is not closed by media literacy programmes, fact-checking architectures, or counter-messaging campaigns. It is closed by both the social infrastructure foundation and the Layer One investment the framework chapters develop, including investments in arts and culture as security infrastructure rather than as discretionary spending. Ukraine made these investments steadily over the three decades since independence and has continued to make them under existential pressure. Most democracies have not made the equivalent investment under any pressure at all.

Honest limitations

The Ukrainian civil-society architecture is currently degrading. The funding that sustained it across the post-2014 period is being withdrawn at exactly the moment when the operational environment intensifies. The United States withdrawal from counter-disinformation funding has decimated significant portions of the architecture. StopFake survives through a commercial-services funding model that subsidises its public-interest work with revenue from analytical services sold to international partners, international media organisations, and Meta's third-party fact-checking programme.[22] Most Ukrainian counter-disinformation organisations cannot build comparable revenue models and are scaling down, with some closing entirely. The capacity democracies might learn from is being lost in real time, and the window to correct course through different international sources of funding is quickly closing.

The Ukrainian state institutional architecture is still consolidating. The Centre for Strategic Communication and Information Security has been moved out of its previous ministerial placement during the chapter's drafting period, with the successor architecture still being constituted. The structural condition producing this institutional flux is that Ukraine is simultaneously fighting a kinetic war, building counter-disinformation capacity from a low post-Soviet baseline, and managing political-authority concentration that comes with wartime conditions. Partner democracies considering institutional architectures comparable to the Ukrainian model should expect that institutional consolidation in their own environments will take longer than the Ukrainian wartime tempo suggests, and should not read the speed of Ukrainian institutional development as the speed at which comparable architectures can be built outside the conditions of war.

The Ukrainian cultural decolonisation work is incomplete and contested. The framing of Ukrainian cultural resistance as a structural feature of the population's cognitive-defence architecture is correct at the analytical level, but it should not be read as suggesting Ukrainian society is uniformly engaged in the work. Approximately a third of Ukrainians continue to speak Russian as a primary language at home, a smaller but operationally relevant proportion continue to consume Russian-language media, and others still

remain inside cultural inheritances the decolonisation work seeks to disentangle from Russian framings. The work is real and accelerating. It is not the experience of all Ukrainians at all times.

The strategic-communications architecture under President Zelenskyy operates inside conditions of wartime political-authority concentration. Under wartime conditions, the centralisation of strategic communications inside the presidential office makes operational sense and has produced the coherent voice that has been one of Ukraine's most significant cognitive-defence assets. Outside wartime conditions, the same centralisation pattern produces democratic risks the chapter does not believe partner democracies should aspire to replicate. The transferability findings are the three-register integration, the decentralised many-voice coherence, the integration of humour and emotional-register communications, and the continuous calibration to target audience framings.

A further honest limitation concerns Ukraine's institutional dependence on a partner-political-will environment Ukraine does not control. The Ukrainian cognitive-defence architecture has been sustained in significant part by partner state and civil-society funding, by partner institutional integration, and by partner political support for Ukraine's territorial integrity. European publics across partner democracies have supported sustained financial assistance and military aid to Ukraine, but the same publics, including in border countries with the most direct understanding of the Russian threat, have not supported putting their own troops on the ground in Ukraine. As United States support declines or nearly disappears, the European Union, its member states, and other like-minded donors should step in more actively to support Ukrainian non-governmental organisations working to counter disinformation and strengthen societal resilience. Ukrainian institutional planning has had to assume political-will environments outside Ukraine that may not produce the commitments Ukraine's operational requirements call for. The Ukrainian defensive task therefore includes the strategic-communications work of building public understanding inside partner democracies sufficient to sustain the commitments the operational environment requires, work that

goes beyond what any cognitive-defence architecture inside Ukraine can produce alone.

What travels from Ukraine

The Ukrainian operational experience produces a set of transferability findings. The integration-across-domains operational architecture is transferable as a conceptual model: the recognition that institutional architectures separating kinetic, cognitive, digital, civic, energy, and cultural operations operate inside frameworks adversary operations have been designed to defeat. The specific Ukrainian wartime cabinet fusion of digital transformation and defence, formalised through the January 2026 appointment of Mykhailo Fedorov as Minister of Defence after his six-year tenure as architect of Ukraine's civic-digital infrastructure, is not transferable in its specific institutional form. The underlying conceptual move, the recognition that civic-digital, defence, and cognitive-defence operations belong inside a single ministerial portfolio rather than across separate ministries, is transferable.

Civil-society investment as load-bearing rather than supplementary cognitive-defence architecture is transferable. The Ukrainian case demonstrates that civil-society organisations carry operational functions state institutions cannot, that the operational integrity of civil-society work depends on its institutional separation from state direction and funding, and that the operationally strongest cognitive-defence architectures are produced by the combined force of independent civil-society capacity and state institutional support sitting on top of it. The combined-force finding is the transferable one: civil society alone is more effective than the state alone, but state architecture sitting on a civil-society substrate is more effective than either independently. The funding architecture for civil-society work should be designed to preserve civil-society independence. The architectural commitment is to independence from direction, not to a particular funding source.

The three-register strategic-communications architecture is transferable. Effective communications inside cognitive-warfare environments require the simultaneous integration of pragmatic-interest, ethical-values, and emotional-connection framings, calibrated to target audience and continuously updated. The architecture should be

supported by decentralised many-voice coherence rather than centralised one-voice messaging. Humour, irony, and emotional-register communications should be treated as operational instruments rather than as ancillary to policy advocacy.

Narrative intelligence as a discipline is transferable. The analysis of adversary narratives as intelligence indicators producing operational information about adversary intent and capability is an analytical practice democracies considering cognitive-defence investments should adopt alongside the more established intelligence disciplines. The application of kill-chain methodology to adversary operations infrastructure rather than to adversary narratives is similarly transferable as operational doctrine.

Cultural investment as security commitment is transferable. Democracies that have under-invested in cultural production, arts funding, and the institutional infrastructure of cultural and civic life have left foundational attack surface no operational architecture built on top of can close. Cultural investment is the protection of one's sovereignty and a security commitment.

The findings that do not travel are also worth naming. The Ukrainian cultural and historical inheritance from which cultural resistance draws is not transferable. The natural counter-propaganda capacity from shared linguistic and cultural exposure to Russia is not transferable. The wartime political-authority concentration that enables the centralised messaging instantiation of Ukrainian strategic communications is not transferable, and the existential-threat conditioning that has produced Ukrainian civil-society capacity is not transferable either. The lessons are not in what to copy. They are in what to recognise about the operational environment all democracies now operate inside.

Ukraine's partner landscape

Ukraine's partner landscape is structured differently from the partner landscapes of other partner democracies. Ukraine sits at the operational front edge of contemporary cognitive warfare, and the partner architecture around it reflects that position. The partners are organised as much around what they can learn from Ukraine and what they can sustain in support of Ukraine as around what they can jointly produce with Ukraine.

This section sets out the five features of that architecture that bear on the chapter's analytical argument.

The Ukrainian diaspora is the first distinctive feature of the partner landscape. The global Ukrainian population living outside Ukraine numbers approximately twenty million, distributed across more than eighty countries. Canada has the second-largest Ukrainian diaspora community outside Russia: approximately 1.3 million Ukrainian Canadians by Statistics Canada's 2021 Census measure, plus over 200,000 arrivals under the Canada-Ukraine Authorization for Emergency Travel (CUAET) programme between 2022 and 2024, inside a Canadian population of forty million.[23] Ukrainian Canadians are not a constituency Canada hosts; they are Canadians, and they have been part of Canada's cultural mosaic since the first Galician settler wave of the 1890s. The political consensus across Canadian parties on Ukraine support is not primarily an outcome of Ukrainian-Canadian advocacy, although that advocacy has been substantial. The deeper structural fact is that virtually every Canadian knows someone of Ukrainian descent through neighbourhood, workplace, school, faith community, or family. The connection that produces the political consensus is a connection inside Canadian society, not an external advocacy effort directed at it. The pattern is instructive in its limits: democracies without comparable historical integration cannot manufacture the equivalent through advocacy alone.

The second distinctive feature is the bilateral security agreement architecture Ukraine has built with partner democracies since the July 2023 G7 Joint Declaration of Support for Ukraine at the NATO Vilnius summit. Ukraine has signed ten-year bilateral security agreements with every partner democracy whose cognitive-defence architecture is examined in this volume: Canada, the United Kingdom, France, Germany, Denmark, Italy, the Netherlands, Finland, Latvia, Lithuania, Norway, Sweden, Estonia, and Poland, with the UK's January 2024 agreement subsequently expanded into a hundred-year partnership in January 2025.[24] The agreements vary in specificity and binding character but converge on a common set of operational commitments: long-term security assistance, defence industrial cooperation, training, intelligence sharing, support for cyber defence and resilience initiatives including hybrid threats, and consultation

mechanisms in the event of renewed Russian aggression. The cyber-defence and hybrid-threats provisions encompass the cognitive domain explicitly. Taken together, the agreements are the closest thing the post-2023 European security order has produced to a multilateral commitment to Ukrainian defence outside formal Alliance membership.

The third feature is the institutional partner architecture at the European Union and NATO levels. The European Union institutional layer is the most operationally significant: the European External Action Service's East StratCom Task Force and EUvsDisinfo, the European Union Foreign Information Manipulation and Interference Toolbox, and the Disinformation Awareness and Resilience Project funded by the European External Action Service and implemented with Ukrainian regional partners, constitute the reference architecture Ukrainian civil-society organisations are integrated with at the European Union level. The North Atlantic Treaty Organization architecture is more operationally substantial than is sometimes assumed. The NATO Strategic Communications Centre of Excellence in Riga runs a named Ukraine StratCom partnership programme as part of its annual programme of work, with research outputs on Russian information operations against Ukraine that inform Alliance-wide doctrine. The NATO-Ukraine Joint Analysis, Training and Education Centre (JATEC) in Bydgoszcz, Poland, opened in February 2025, is the first civil-military organisation jointly run by NATO and Ukraine, and its workshops on total defence, resilience, and strategic communications make it the most institutionally substantive NATO-Ukraine cognitive-defence cooperation to date.[25] The Helsinki-based European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), the only institution enabling the European Union and NATO to work on hybrid threats together, granted Ukraine enhanced partnership status following the 2022 invasion and has developed dedicated training programmes for Ukrainian professionals and analytical partnerships with Ukrainian institutions, including the 2024 report on Ukrainian counter-disinformation methodology produced jointly with the Atlantic Council Digital Forensic Research Lab.[26]

The fourth feature is the channelled-coalition architecture for partner cognitive and cyber support to Ukraine, and Estonia has done the most to construct it. Estonia initiated the Tallinn Mechanism, currently chaired by the United Kingdom with

approximately fourteen members, which coordinates civilian cyber support to Ukraine. Estonia and Luxembourg co-chair the IT Coalition within the Ramstein framework with approximately twenty members, which coordinates military cyber support. The operational significance of these structures is that they channel partner support in forms calibrated to what Ukraine asks for, and they sustain partner attention to Ukrainian operational needs across changing political environments.

The fifth feature is the bilateral learning relationships Ukraine has built with partner democracies. Sweden has translated cognitive-defence materials into Ukrainian and Romanian and funds counter-disinformation training in Ukraine and Moldova. The Baltic states have not only provided significant support to Ukraine in countering disinformation, but have also learned from Ukraine's wartime experience and from Ukrainian approaches to resisting Russian information and cognitive operations as they have evolved under the pressure of full-scale war. The Nordic and Baltic relationships with Ukraine treat Ukraine as the operational reference case rather than as a developing partner, an orientation that distinguishes them from the broader partner environment in which Ukraine is sometimes treated as a recipient of expertise rather than as the source of it. Ukraine is the partner democracy disseminating cognitive-defence knowledge to the rest of the partner-democracy community more than it is jointly cooperating in the way that partner democracies among themselves do. The asymmetry is not because Ukraine has chosen to position itself this way; it is because Ukraine has been operating inside the cognitive-warfare environment longer and at higher intensity than any other partner democracy, and because the operational knowledge that environment produces does not yet exist anywhere else at comparable depth. Sustaining the Ukrainian capacity to continue producing and disseminating this knowledge is, for partner democracies, an investment in their own cognitive-defence architectures rather than an act of solidarity at one remove.

Endnotes

1 Mathew Lyons, "France's Kyivan Queen," *History Today* 72, no. 5 (May 2022).

2 Razumkov Centre, *30 Years of Independence: National Identity and Foreign Policy Orientations of Ukrainians* (Kyiv, 2021).

3 UK Ministry of Defence daily intelligence updates & Ukrainian Ministry of Defence operational reporting. ussian offensive operations in Donetsk Oblast and adjacent fronts.

4 Office of the President of Ukraine official communications.

5 Center for European Policy Analysis reporting on Russian soft-power operations. The framework-level treatment of Russian cultural production as cognitive operation is developed in Chapter 3.

6 StopFake methodology developed across the post-2014 period. The framework-level treatment of reflexive control as Soviet and Russian military doctrine is developed in Chapter 3.

7 Centre for Young International Studies, "The Fourth Winter: Inside Russia's Evolving War on Ukraine's Energy," November 2025.

8 European Union Institute for Security Studies, "Fuel, fear and falsehoods: Defending Europe and Ukraine from Russia's hybrid energy war," December 2025.

9 *The New Voice of Ukraine*, "How Blackout Parties Are Reshaping Life in Kyiv Courtyards," January 2026.

10 Kyiv Post reporting on the appointment of Mstyslav Banik as Deputy Minister of Defence on 26 March 2026.

11 The civil-society-from-2014 finding is corroborated independently by interviews with both StopFake and the Ukraine Crisis Media Centre, and is consistent with the public-record institutional histories of both organisations.

12 StopFake published institutional materials; Mohyla School of Journalism documentation of StopFake's founding; International Fact-Checking Network documentation.

13 Centre published institutional materials; documented training and analytical engagement across regions where Russian operations have established significant presence.

14 StopFake published methodology and the broader academic literature on narrative analysis as intelligence practice, particularly Ajit Maan on narrative intelligence applied to security contexts.

15 House of Commons Foreign Affairs Committee, *Disinformation diplomacy: How malign actors are seeking to undermine democracy* (HC 703, 27 March 2026.

16 *In Case of Emergency or War* civil-defence brochure documentation (prepared 2022, distributed across frontline territories from the early phase of the full-scale invasion).

17 Public-record analysis of Ukrainian strategic communications since 2022 and of Ukrainian engagement with Global South and United States audiences across the post-2024 period.

18 Ukrainian Ministry of Foreign Affairs public statements; Razumkov Centre and KIIS polling on Ukrainian public perceptions of United States and European Union partners in the spring of 2026.

19 Peter Pomerantsev, *How to Win an Information War* (PublicAffairs, 2024).

20 BBC reporting on the 2025 *Tantsi z Zirkamy* Christmas episode broadcast under blackout conditions; broader public-record analysis of Ukrainian cultural events under wartime conditions.

21 Office of the President of Ukraine official communications; Ukrinform reporting on the Global Coalition of Ukrainian Studies; Harvard Ukrainian Research Institute fiftieth anniversary materials.

22 StopFake published institutional materials on its analytical-services offering to international partners; International Fact-Checking Network documentation of StopFake's certified-signatory status; Meta third-party fact-checking programme documentation; practitioner commentary inside the Ukrainian counter-disinformation community on the institutional sustainability of civil-society organisations operating under conditions of reduced international donor funding.

23 Statistics Canada, 2021 Census of Population, ethnic or cultural origin data.

24 G7 Joint Declaration of Support for Ukraine, Vilnius, 12 July 2023; Carnegie Endowment for International Peace, "Getting Ukraine's Security Agreements Right," July 2024; European Council on Foreign Relations, "The power of a promise: Understanding Ukraine's bilateral security agreements," 2024.

25 NATO Strategic Communications Centre of Excellence Programme of Work, including the Ukraine StratCom partnership programme, at stratcomcoe.org.

26 Hybrid CoE publications and training programmes for Ukrainian professionals, including capacity-building work with Ukrainian university faculty on countering hybrid threats; Atlantic Council Digital Forensic Research Lab and Hybrid CoE, *How Ukraine fights Russian disinformation: Beehive vs. Mammoth* (January 2024); NATO public information on the European Centre of Excellence for Countering Hybrid Threats as the only institution enabling EU-NATO joint work on hybrid threats.

Chapter 19: Finland

Finland's benchmark status in the cognitive defence literature is cultural before it is programmatic. It is about having a society that is alert without being afraid and institutions that coordinate naturally rather than being tightly controlled. Finland is the Alliance's benchmark for the two horizontal foundations that make every cognitive defence layer operable: the social infrastructure beneath, and the political will and elite coherence above.[1]

The concerned-not-afraid disposition is double-edged. At the onset of the COVID-19 pandemic, Finnish public debate divided sharply over whether mask mandates infringed personal freedom; once the government decided, compliance was near-universal. The pattern is broader than any single episode. It can be seen in Finland's near-universal acceptance of conscription and national service with no meaningful public pushback or how Finns observe their Independence Day: soberly by remembering those lost in the struggle for independence, gathered around television screens to watch the President receive guests in endless procession at the presidential palace. The culture subordinates individual preference to collective judgement once the state has ruled, because Finns read authority as the instrument of something larger than any political party. The same discipline can produce over-confidence: because Finns understand themselves to be exceptionally prepared, public conversation about vulnerabilities is comparatively closed.[2] The discipline is an asset against ambient manipulation and a vulnerability when preparation for the last threat does not match the shape of the next.

Historical and Structural Foundations

Finland is a small country with 5.5 million people, sharing an 832-mile land border with Russia, the longest of any EU member state. Finland has ranked first in the World Happiness Report for nine consecutive years, including the 2026 edition, with a score of 7.764 on the Cantril life-evaluation ladder; the underlying drivers, high institutional trust, low corruption, social support, and equality, are the same social-infrastructure foundations on which Finland's cognitive defence architecture depends. The Winter War, the Continuation War, and forty years of post-war Finlandisation are the lived

inheritance every preparedness investment is grounded in. Finnish and Swedish are both official languages under the Constitution.[3] Approximately ninety-two percent are native Finnish-speakers and five percent native Swedish-speakers. Finnish belongs to the Finno-Ugric branch of the Uralic language family, closely related to Estonian and more distantly to Hungarian. Unlike most European languages, it is not Indo-European, which has historically served as a natural filter against influence operations reliant on linguistic fluency. Ninety-five percent of Finnish imports and exports transit the Baltic Sea. Finland treats Baltic maritime security as existential. The networks inside the security establishment are small and many in the field know each other. An interviewee joked that the head of the National Emergency Supply Agency, NESA, and the chief executive of a critical infrastructure company are likely to be related.

Finland's is a country that prepares to go it alone. Territorial concessions after the Winter War, decades of Finlandisation, and a post-1995 EU membership that did not foreclose armed neutrality all produced a disposition toward self-reliance in extremity. Finland's formal posture through this period was non-alignment: neither a Cold War bloc member nor a NATO ally, retaining the ability to choose its own course in a crisis. NATO accession in April 2023 ended non-alignment as doctrine, but its habits of mind have taken longer to shift than its treaties have. The consequence is that Finland has built one of the strongest militaries in the Alliance on a per-capita basis, and the instinct to coordinate is a newer muscle than the capability itself. Several interviewees made the same observation: Finnish capability is exceptional, but the cultural reflex to seek outside cooperation before acting alone is comparatively recent. This shift happened roughly in the last decade, during which defence cooperation has become, in the Finnish Institute of International Affairs (FIIA) assessment, the most important driver of Finnish external affairs.[4] Since NATO accession, Finland is hosting an enhanced Forward Presence battlegroup led by Sweden from 2026 in Rovaniemi and Sodankylä, with contributions from Denmark, France, Iceland, Norway, and the United Kingdom; is hosting NATO's Multi Corps Land Component Command; and contributes routinely to the Standing NATO Maritime Group One and Mine Countermeasures Group One in the

Baltic Sea, North Sea, and North Atlantic.[5] The mentality is new and maturing at the tempo the threat environment requires.

Finland's security mindset has not shut off in generations. Where Sweden and several other Western European states dismantled civil defence/total defence architecture after the Cold War, the Finnish whole-of-society model has run consistently across decades, and the continuity of mentality matters more than any single programme. A separate but related feature is the physical infrastructure that mentality has sustained. Civil shelter capacity covers approximately 4.8 million of the 5.5 million population, with Helsinki alone capable of sheltering close to its full population underground within seventy-two hours.[6] Sauna halls, parking garages, and shopping centres convert to shelters on a pre-planned basis. The military reserve, one million from a population of 5.5 million, is proportionally larger than any NATO peer. General conscription produces shared experience across class, region, and linguistic background. Conscription is understood as social infrastructure before military readiness.

Beneath these investments sits a political culture in which the state is understood as more than the party in government. Finland is a parliamentary republic with a directly elected President whose constitutional role is deliberately apolitical. The President leads foreign policy in cooperation with the government and functions as a figure of national continuity rather than partisan alignment.[7] The President of Finland also serves as the commander-in-chief of the Finnish Defence Forces. Senior civil servants, parliamentarians, bishops, and business leaders treat national service as a duty independent of political affiliation, and no board complains when a chief executive is away for three weeks.

The Finnish Defence Forces maintain one of the strongest militaries in Europe per capita, with a wartime strength of approximately 280,000 expanding to a reserve of one million.[8] Finland has retained extensive artillery, armoured, and mechanised capacity through decades when others shed it. Finland also invests in diplomacy at a scale that proportionally outpaces most mid-sized peers, with a dense footprint across Europe, the Nordic-Baltic region, the United States, and key Asian partners.[9] President Stubb has

described the underlying theory in direct terms: for a small country, "information is power," and presidential-level diplomacy consists in the daily exchange of information with partners.[10] Seriousness about diplomacy is the other side of seriousness about defence: both reflect the judgement that small states preserve sovereignty through sustained investment in the instruments that make them legible to larger ones.

The Architecture in Practice

Finland does not generally use "cognitive warfare" as its working term. The Finnish government and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) based in Helsinki prefer "societal security" and "information influence," framings that locate the problem inside civilian resilience architecture rather than military operations.[11] The terminological preference reflects a substantive position: Finland's comprehensive security tradition and general conscription already treat what other states would call cognitive defence as the ordinary business of citizenship, which is why NATO's adoption of the cognitive-warfare concept requires less conceptual change in Finland than elsewhere in the Alliance.[1]

The institutional spine of Finnish comprehensive security is the diamond model, a framework of seven societal functions with assigned organisational leads in legislation: psychological resilience; leadership; international network activities and cooperation including the EU and NATO; the functionality of society and services in all situations; economy, infrastructure, and security of supply; defence capabilities; and internal security.[12] Each ministry simultaneously maintains its own preparedness plans independent of the central Security Committee, making the architecture redundant by design. Disruption of central coordination does not collapse the system. The Security Committee is an inter-ministerial coordination body located within the Finnish Ministry of Defence, responsible for comprehensive security policy. Its Secretary-General coordinates permanent secretaries from all relevant ministries plus the business sector, meets monthly, and produces collective recommendations and a yearly national security strategy.

The information environment is anchored by media literacy embedded in mother-tongue education from preschool since the 1990s.[13] The ambient awareness that exists now is the thirty-year product of a political decision made before the threat was visible. The critical current vulnerability is that AI-driven translation has closed the Finnish language filter: as recently as 2023, poor machine translation of Russian operations made them detectable through linguistic anomalies, and that protection is now largely gone. NESA is the operational expression of public-private preparedness, with thirty-five to thirty-seven sector pools, legal obligations on companies to signal government immediately when something goes wrong, and compensation mechanisms for compliance.[14] The architecture was tested during the post-2022 Baltic Sea cable and pipeline incidents, several timed around national holidays, and the contractual signalling obligations functioned as designed.[15]

Detection and attribution is where the architecture's through-line to cognitive warfare is clearest. The Finnish threshold is now evidentiary rather than political: the Chinese parliament hack was attributed promptly once evidence sufficed, and Russian historical narrative operations, including sustained disinformation claiming Finnish responsibility for wartime atrocities in occupied Karelia, have been documented and countered as the history-warfare method that Chapter 3 develops in full.[16] What remains weaker is the public-facing component. Finland does not publish a single, unified annual national threat assessment of the kind seen in some peer democracies, but instead provides threat analysis through multiple institutions and reports, including the Finnish Security and Intelligence Service, the Finnish Defence Forces, and the Security Committee. A key feature of Finland's approach to countering disinformation, similar to Sweden's, is its strong emphasis on freedom of expression; as a result, organised debunking efforts can be perceived as a form of censorship. Information influence does not yet have a clear institutional home. A live reform to centralise communications coordination under the Prime Minister's Office remains unresolved and viewed with scepticism by a well-placed practitioner: administrative consolidation without operational clarity resolves less than it appears to. Detection is strong on evidence and threshold, weaker on consolidated public communication.

Sovereign response is the second of Finland's more developed operational layers. The emergency border pushback law, passed under classified intelligence briefings and renewed twice without ever being applied, responded to Russia's 2023-2024 instrumentalisation of migration at the eastern border, read in Helsinki as a cognitive-domain operation. The goal was to force Finland either to abandon people at the border in winter or accept the reputational damage of admitting them under pressure.[17] Russia knows the authority exists and has not tested it again at scale. The cognitive trap remains, because the physical border infrastructure could be turned against Finland through humanitarian imagery designed to fracture Finnish and European support. Freedom-of-expression exceptions from post-Second World War legislation enable action without fresh legislative authority. When the phenomenon of Quran burnings spread across the Nordic region, Denmark and Sweden required new legislation to respond; Finland was able to prohibit them under existing law. Neither the border law nor the Quran-burning prohibition drew sustained public pushback, for the same reason that makes the rest of the architecture operable: a civic culture of deference to authority that accepts hard state action on security grounds once the state has decided it is warranted.

Political will and elite coherence is where the architecture is most distinctive. The National Defence Courses bring bishops, parliamentarians, chief executives, civil society leaders, and senior civil servants together for three weeks, with no state salary during participation, no contact with their organisations, and a waiting list for attendance. The established institutional trust and culture of civic duty that sustains participation is what makes the National Defence Courses work; regional delivery extends the model beyond Helsinki, the feature that makes it scalable to other contexts.[18]

A second instrument is the Foreign Affairs Committee, meeting on dates established by law in advance, brings together the President and all coalition party leaders, producing a venue for cross-party political coherence on foreign and security questions that the ordinary cycle of parliamentary politics does not provide. The 2019 Act on the Oversight of Intelligence Gathering complements this with a legally mandated cross-party

Intelligence Oversight Committee, which has extensive statutory rights of access to all intelligence material, including content shared by NATO partners, and which institutionalises the cross-party briefing relationship rather than leaving it to executive discretion.[19] Together the National Defence Courses, the Foreign Affairs Committee, and the Intelligence Oversight Committee produce coherence across political lines that survives electoral cycles, the condition every other layer depends on.

The architecture nonetheless faces the weakness every democracy shares. Mika Kerttunen, a Finnish cybersecurity and international norms expert, characterised the adaptation problem as always chasing the last threat: after Crimea came the little green men, then election interference, then instrumentalised migration, then sabotage.[11] The next iteration is unknown, and the cultural disposition toward quiet self-assurance can make this harder to name.

Transferability

Four political choices are available to any democracy. The first is embedded media literacy. Finland decided in the 1990s to treat critical thinking about information as a literacy skill rather than a security intervention, embedded in existing subjects rather than built as a standalone programme. The decision can be made anywhere; the thirty years of ambient awareness that resulted cannot be imported.

The second is inter-agency coordination by design. The Finnish convening architecture described above, the Security Committee's monthly cadence, the diamond model's named functional owners, the NESA sector pools binding companies and regulators by statute rather than goodwill, rests on a 1958 statutory frame. The transferable core is the pattern: obligatory convening on named topics, with named owners, on a continuous rather than episodic basis, resourced modestly. The approach requires legislation and political will rather than cultural change, and produces results in months rather than decades.

The third is the elite socialisation architecture. The National Defence Courses model requires only political will and organisation, and regional delivery makes it replicable

without centralising participation in a capital city. What is not transferable is the underlying principle on which the courses rest, the belief in civic duty that drives attendance and sustains the waiting list, which bridges directly to the fourth point.

The fourth is a commitment to fostering civic duty and a culture of service. Most democracies will not be invaded in the way Finland has been, and the specific Finnish instruments, general conscription, civil shelters for nearly the entire population, and 72-hour personal preparedness expectations,[6] are historically contingent. What is transferable is the underlying mentality: the judgement that citizens are participants in the security of the state, not clients of it, and the institutional investments that make that participation credible. Adoption requires a society willing to foster civic duty in ways most democracies have not recently attempted.

What none of these choices will produce, in non-Finnish conditions, is a Finnish outcome. However, they will produce better outcomes than doing nothing, in a shorter timeframe than waiting for cultural change. That is the honest case for adoption.

Finland's resilience model also benefits from factors that do not transfer easily: a smaller population, stronger historical memory of existential threat, social cohesion that has not been tested by the same scale of demographic change as several peer Nordic states, and exceptionally high institutional trust. Countries seeking to emulate Finnish resilience must recognise that the model rests on social foundations that take generations to build and can erode faster than they were constructed. The Finnish approach offers a north star, but reaching it requires diverse, lower-trust societies to treat social cohesion not as a precondition that already exists but as a deliverable that must be built deliberately, in parallel to the state capacity to counter cognitive threats.

The point is reinforced by what is happening across the region: Lithuania runs its own version of the National Defence Courses, several Nordic and Baltic states have built variants of inter-agency coordination, and citizen engagement is increasingly understood as a deliverable that requires sustained investment rather than an

inheritance. The "Finnish model" is best understood as a guiding vision whose elements can be adapted, rather than a system that copies whole.

Honest Limitations

Finland faces three broad limitations. First, the untested assumption of adequacy. Finland does many things extraordinarily well, and a culture that subordinates disagreement to collective judgement produces rapid compliance, but it also produces a public conversation in which very few voices press the question of what is not yet being done well. Kerttunen has made the comparison explicitly: while Finland's political class is briefed comprehensively through the Intelligence Oversight Committee architecture, and threat analysis flows internally through the Finnish Security and Intelligence Service, the Defence Forces, and the Security Committee, Finland does not produce a single, unified public-facing threat document of the kind Estonia issues annually. The gap is between the political class and the population: the Finnish habit of processing threats privately rather than in public discourse leaves a population that is culturally prepared without being specifically informed.[11] The deeper problem is that the architecture has never been stressed at the scale the adversary is capable of producing. The danger is not what you know is weak, but what you do not realise is weak yet, because the political culture does not hold leaders accountable for weaknesses that have not yet been exposed.

Second, prebunking losing the race. The assessment from inside the Finnish ecosystem is direct: automated disinformation is spreading faster than corrections can be produced and distributed. Finland relies on prebunking as its primary information-environment defence rather than on rapid rebuttal, a deliberate choice given that thirty years of embedded media literacy make the population a more receptive audience for inoculation than for correction. The choice is defensible on its logic but vulnerable at its speed.

Third, the unresolved institutional home for information influence. At time of interview, information influence had no clear home in the Finnish government, and the live Prime Minister's Office reform was viewed with scepticism by a well-placed practitioner. The

architecture is strong on prevention and culture; rapid response is less developed than that of leading peers such as France, which has organised VIGINUM as a named operational agency with a clear attribution remit. Finland remains the societal resilience benchmark while trailing the front of the pack on rapid response. The EU DisinfoLab factsheet on Finland reaches the same finding from outside the Finnish ecosystem: "an authority that would be responsible for the development of Finland's cognitive security is needed, together with further cooperation between relevant actors." That Finland hosts the European Centre of Excellence for Countering Hybrid Threats and yet lacks a domestic agency with operational ownership of the cognitive defence file is itself the diagnostic: Finland is a Tier 3 cognitive defender by structure, operating at Tier 1 societal-resilience capability through the foundations beneath the operational layers. Implementation of the EU Digital Services Act in Finland is coordinated by Traficom, the Finnish Transport and Communications Agency, which serves as the national Digital Services Coordinator and is the institutional contact point through which European platform-accountability instruments reach the Finnish information environment.

Partner Landscape

Finland's partner architecture operates on a primary bilateral, a regional institutional base, a sub-regional coordination venue, and substantial bilaterals beyond the immediate region. All layers are simultaneously active.

The Finland-Sweden bilateral is the primary relationship. Swedish is one of Finland's two official languages under the Constitution; Section 17 guarantees the right to use Swedish before state authorities. The attempted joint NATO accession in 2022-2024 expressed the closeness, and Finland's decision to accede alone in April 2023, when Turkish and Hungarian ratification delayed Sweden's, was culturally difficult precisely because of it.[20] Finnish and Swedish defence ministers met fifty-six times during one five-year posting period between 2013 and 2018, a cadence constituting a near de facto defence union before NATO membership.[21]

The Finland-Estonia bilateral relationship is also of note, not least because of linguistic proximity. Finland and Estonia coordinate across the Gulf of Finland on GPS

interference, where similar attack vectors produce similar solutions, and on undersea cable and pipeline security following the post-2022 Baltic Sea incidents, which both governments treated as hybrid operations requiring shared investigative and attribution capacity.[15] The working model is person-to-person coordination through officials who know each other, operating faster than any formal alliance mechanism; both countries have built the Gulf relationship on shared threat assessment, shared linguistic and cultural reference to the Russian information environment, and shared membership of NB8 and the EU.

Nordic defence cooperation provides the regional institutional base. NORDEFCO, the framework among Denmark, Finland, Iceland, Norway, and Sweden since 2009, adopted Vision 2030 at the April 2024 ministerial meeting, focusing on interoperability, capability cooperation, military mobility, logistics, and security of supply.[22] NORDEFCO is the longer-standing and more structurally organised of Finland's regional formats, the basis for the Finnish assessment that the Nordic Five matters more than formal institutional size suggests. The Finland-Norway MoU on Defence Cooperation, signed in Bodø in June 2024, replaces the 2021 framework.[23]

The Nordic-Baltic Eight (NB8) is the active sub-regional coordination venue and the format most directly relevant to cognitive defence cooperation. NB8 is less formally institutionalised than NORDEFCO, but the Haukkala and Raik policy brief, jointly published across all eight Nordic and Baltic international affairs institutes, argues that regional cooperation formats must add value through clearly defined division of labour rather than compete with NATO and the EU.[24] NB8 earns its place by doing operational problem-solving (cable and pipeline security, GPS resilience, hybrid-threat coordination) that the formal structures do not. The Joint Expeditionary Force, UK-led and including all five Nordic states, the three Baltic states, and the Netherlands, sits alongside NB8; Canadian accession is welcome from the Finnish perspective.[25]

Three bilaterals beyond the Nordic-Baltic architecture warrant naming. Germany is the most consequential European partner outside the immediate region. The German brigade deployment to Lithuania situates Germany in the Nordic-Baltic security

architecture Finland helped build, and Finland has offered to share the comprehensive security model at a stage of German institutional redesign driven by the Zeitenwende.[26] The United States is the second. The Defence Cooperation Agreement, signed in Washington in December 2023 and in force since September 2024, provides the binding framework for US forces' presence, prepositioning, and exercises on Finnish territory, supplemented by an Infrastructure Implementing Agreement in August 2025.[27] President Stubb has framed the bilateral pragmatically: Finland and the United States disagree on climate and on aspects of the international institutional order, and cooperate on defence in their mutual interest. Canada is the third. Canada was the first country to ratify Finland's NATO membership, and the relationship has now moved from shared values to shared interests: Foreign Ministers Anand and Valtonen announced the Canada-Finland Strategic Partnership on Foreign and Security Policy in Helsinki in August 2025, and President Stubb and Prime Minister Carney issued a follow-on Joint Statement in Ottawa in April 2026 with an action plan across comprehensive security, Arctic and maritime security including Russia's shadow fleet, hybrid threats, cyber, critical minerals, and a dedicated Joint Statement on Sovereign Technology and AI Cooperation.[28] The Icebreaker Collaboration Effort, a Canada-Finland-United States trilateral on Arctic icebreaker production, is the current operational anchor.

Finland treats the EU and NATO as distinct instruments rather than substitutes. The EU is paramount for global influence and for institutional adoption of the comprehensive security model, which is why Finland has invested so heavily in the Niinistö Report's EU-level uptake. NATO is essential for collective defence, and Finland has operationalised that commitment through the DCA with the United States and full participation in NATO structures since 2023. Finland also plays an active role in EU and NATO cooperation on countering hybrid threats by hosting and providing financial support to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki. Operational cognitive defence cooperation flows through NB8, bilaterals, and coalition formats rather than NATO structures, because those are the venues where the problem is currently being solved at working level.

Endnotes

1 Miina Kaarkoski, *NATO's Concept of Cognitive Warfare*, Finnish Defence Research Agency Research Bulletin 2-2026 (10 February 2026), at puolustusvoimat.fi.

2 Sinikukka Saari et al., *Russia's full-spectrum influence activities in Finland in the 2000s: Softly made, yet hard to sleep on*, FIIA Report 01/2026 (Finnish Institute of International Affairs, January 2026), at fiia.fi.

3 Constitution of Finland (731/1999), as amended, Section 17, at finlex.fi.

4 Matti Pesu, "What non-alignment? Finland's security and defence policy stems from partnerships," FIIA Briefing Paper, Finnish Institute of International Affairs, at fiia.fi.

5 NATO, "NATO's military presence in the east of the Alliance," at nato.int; Finnish Ministry of Defence, "Finland to join NATO's 2026 peacetime activities," May 2025, at defmin.fi.

6 Finland, National Emergency Supply Agency, "72 hours" citizen preparedness campaign, at 72tuntia.fi; Ministry of the Interior civil defence documentation, at intermin.fi.

7 Constitution of Finland (731/1999), Sections 58 and 93, at finlex.fi.

8 Finnish Defence Forces, force structure documentation, at puolustusvoimat.fi/en.

9 Finnish Ministry for Foreign Affairs, Annual Report, at um.fi.

10 Alexander Stubb, "Comprehensive Security: The Finnish Model for 21st Century Threats," keynote address at the Hertie School, Berlin, 8 May 2024, at hertie-school.org; Rosemary Barton interviews with President Stubb, CBC News, 15 April 2026 and 19 April 2026, at cbc.ca.

11 Field research interviews with Mika Kerttunen, independent Finnish cybersecurity and international norms expert, named with consent.

12 Finnish Government, *Security Strategy for Society*, Government Resolution adopted 16 January 2025, at valtioneuvosto.fi.

13 Marin Lessenski, *Media Literacy Index 2026*, Open Society Institute Sofia, at osis.bg.

14 Finland, National Emergency Supply Agency (Huoltovarmuuskeskus), strategy documentation, at huoltovarmuuskeskus.fi.

15 *Countering Information Influence Operations in the Nordic-Baltic Region*, NATO Strategic Communications Centre of Excellence, Riga, 2025, at stratcomcoe.org.

16 EU DisinfoLab, *Disinformation Landscape in Finland*, V2, April 2025, at disinfo.eu.

17 Finnish Government, Act on Temporary Measures to Combat Instrumentalised Migration (HE 53/2024 vp), July 2024, at valtioneuvosto.fi.

18 Finnish Security Committee, "Comprehensive Security" documentation, at turvallisuuskomitea.fi/en/comprehensive-security.

19 Act on the Oversight of Intelligence Gathering (121/2019), Finland, at finlex.fi; Eduskunta, Intelligence Oversight Committee, at eduskunta.fi.

20 NATO, "Finland joins NATO as 31st Ally," 4 April 2023, at nato.int.

21 Field research interview with a senior Finnish source with direct experience of the Finland-Sweden bilateral cooperation framework.

22 NORDEFCO Vision 2030 political steering document, signed 30 April 2024, at nordefco.org.

23 Finnish Ministry of Defence, International Conventions, at defmin.fi/en/areas_of_expertise/international_defence_cooperation/international_conventions.

24 Hiski Haukkala and Kristi Raik, *The circles of security: The role of the NB8 in (Northern) European security*, Nordic-Baltic Eight Institute Series of Topical Briefs, Policy Brief 2/2026 (16 April 2026), at fiia.fi.

25 Finnish Ministry of Defence, JEF Policy Direction Framework Arrangement, international conventions documentation, at defmin.fi.

26 Sauli Niinistö, *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*, Report to the President of the European Commission, 30 October 2024, at commission.europa.eu.

27 Finland-United States Defence Cooperation Agreement, signed 18 December 2023, in force 1 September 2024, Treaty Series 69 and 70/2024, at defmin.fi.

28 Government of Canada, "Canada and Finland Joint Statement on Foreign and Security Policy Strategic Partnership," 19 August 2025, at canada.ca; Prime Minister of Canada, "Joint Statement by the Prime Minister of Canada Mark Carney and the President of the Republic of Finland Alexander Stubb," 14 April 2026, at pm.gc.ca.

Chapter 20: Sweden

Sweden is rebuilding its post-war defence architecture in real time. It is building on the Cold War Total Defence conceptual foundations but refitting them for the digital age. What makes the rebuild distinctive is that it is happening through institutional design rather than cultural inheritance. Sweden dismantled its defence institutions following the end of the Cold War and is now starting from scratch. The Myndigheten för Psykologiskt Försvar (MPF), the Swedish Psychological Defence Agency established in January 2022, is Sweden's institutional bet that a democracy can build cognitive defence by empowering its citizens. Alongside France's VIGINUM, MPF is one of the two models European democracies are now studying most closely.[1] The architecture is strong. The significant gap that has yet to be addressed is reaching the populations the Swedish state has never learned to communicate with in their own languages.

Security culture and the Swedish approach to defence

Sweden is a kingdom with imperial roots that has not fought a war for two centuries. Its historical rule over present-day Finland, Estonia, and Latvia has produced lasting connections across the region. It is consistently ranked in the top five of global democracy assessments, and its institutional trust is among the highest in the world.

Two elements of Swedish mentality are load-bearing for what follows. The first is that security in Sweden is not a function the state performs on behalf of a civilian population. It is a shared civic obligation with legal teeth. Under the *Total Defence Duty Act* (1994:1809), every person residing in Sweden between the ages of sixteen and seventy is obligated to contribute to the country's defence in times of crisis or war.[2] Total Defence (*totalförsvar*) is the Swedish doctrinal term for what the broader security community now calls a whole-of-society approach. It predates that framing and carries obligations no whole-of-society framework requires.[3] Total Defence extends to the private sector: approximately ninety percent of surveyed Swedish companies identify a clear role for themselves within the defence system.[4] Civic engagement on defence is also carried by long-standing grassroots initiatives such as Folk och Försvar (People and Defence), which work alongside government to sustain public awareness and engagement on national security. Swedish citizens and Swedish companies accept that

they are part of the country's defence architecture: a different social contract than most democracies. Adopting the Swedish model elsewhere would require a genuine public policy debate about the depth and reliability of that society’s relationship with the state.

The second element is the Swedish cultural commitment to freedom of speech and freedom of information. Two of Sweden's four constitutional acts specifically protect these freedoms, with protections stricter than EU frameworks for one of the oldest free presses in the world.[5] This shapes every downstream choice Sweden makes about cognitive defence: media literacy rather than content regulation, empowerment rather than counter-messaging, education rather than prescription. For this reason, Sweden was initially critical of bans on Russian state media in the Baltic states and Eastern Europe, viewing them as a breach of free expression. Sweden's position has since cautiously evolved, but the initial reflex underlines how deeply free speech protections shape Swedish policy choices.

The Swedish security environment was transformed between 2014 and 2024. Russia had been testing Sweden well before 2014 through unauthorised airspace approaches near the Stockholm archipelago and suspected submarine incursions in Swedish territorial waters. Russia's annexation of Crimea in March 2014 produced a sober reassessment, and in 2015 the Swedish government took the formal decision to rebuild Total Defence capabilities dismantled in the 1990s. Conscription returned in 2017 as selective service. Russia's full-scale invasion of Ukraine in 2022 accelerated implementation and spurred public opinion to swing in favour of joining NATO, which Sweden did in March 2024.[6] Sweden is contributing to NATO's Forward Land Forces battle group in Latvia (the Canada-led multinational formation), conducted its first NATO Air Policing mission in Iceland from January 2026, and deployed fighter jets to patrol over Greenland under NATO's Arctic Sentry mission from February 2026. A decision has been taken for Sweden to lead a new Forward Land Forces mission in Finland, with deployment planned for 2027 to 2029.[7] This posture is necessity-driven rather than ambition-driven, which matters politically because Swedish strategic culture is averse to visible force posture expansions and to the rhetoric of assertive power projection. The

political class is forward-leaning on the threat assessment across the spectrum, carrying the public with them so far.

The threat environment

The Swedish Security Service and the Swedish government name Russia, China, and Iran as the adversaries against which Sweden's cognitive defence is organised.[8]

Russia is primary. Its objective is not to persuade Swedes toward an alternative view but to erode the coherence of Swedish democratic decision-making, reduce support for Ukraine, and exploit any division the adversary can find or amplify. The Russian pattern across the West is not to create divisions but to pour gasoline on fires already lit. What is Sweden-specific is where the gasoline lands.

China operates through longer time horizons: academic and STEM research influence, friendship-city cultural exchange programmes, teacher placement in Swedish schools through Chinese cultural institutes, the Belt and Road Initiative office in Sweden, and the four to five Chinese overseas police stations Sweden, like Canada, identified and closed.[9] Swedish authorities have moved against the most visible of these vectors: the Confucius Institutes, the Belt and Road office, and the overseas police stations. Research influence and friendship-city programmes remain harder to contain.

Iran operates through Middle East-origin information operations targeting Sweden's Muslim diaspora communities and the country's image in Arabic-speaking media, amplifying Russian narratives and pursuing its own interests around Sweden's human rights posture.

Three cases define how Sweden has come to understand this threat environment.

The social services campaign (2021–22): the wake-up call

Through late 2021 and 2022, a disinformation campaign alleged that Swedish social services were systematically removing Muslim children from their families to forcibly convert them to Christian Swedish identity. The claim was absurd in a country that is among the most secular in the world. It was not absurd to the communities it targeted. Many of the families receiving these messages had come from countries where state

removal of children does happen and where police and authorities are not trustworthy, and the allegations about Sweden were experientially plausible even if factually false. The communities were frightened, not convinced. Parents did not know whether the campaign was true, but they feared it could happen to them. The Swedish social workers at the centre of the campaign watched their work being weaponised against the communities they were trying to serve. The Swedish state had no institutional capacity to reach the communities the campaign was operating in, through their languages or through any of the channels those communities actually trusted. The Swedish Institute, the Foreign Ministry agency that monitors Sweden's international image, tracked the campaign's reach at several million views in Iran alone.[10]

The campaign targeted Swedish social services, which operate under municipal authority in a highly decentralised system. The municipality of Stockholm has approximately seven thousand employees; the smallest Swedish municipalities have ten to twelve. A municipality of a dozen staff cannot detect or respond to a coordinated foreign information operation unaided, and the campaign exploited precisely this. The realisation was that cognitive warfare against Sweden would target ordinary citizens by exploiting architectural gaps in state governance, not the political elites themselves. MPF had been established weeks before the campaign peaked, however it had no operational capacity yet and no set governance structure. Sweden had built MPF technically in time, but not quite early enough.

Beyond Operation Doppelganger (2024): the signature investigation

Operation Doppelganger is the name given to a large-scale Russian influence operation active across Europe since 2022, run by the Social Design Agency and other Russia-based contractors working for the Kremlin. The operation creates cloned versions of legitimate Western media websites, hence "doppelganger", and seeds them with disinformation designed to be shared as if from the original publication. French intelligence publicly exposed the operation in 2023.[11] The operation continued, unchanged. In 2024, MPF published *Beyond Operation Doppelganger*, an analytical report based on approximately three thousand leaked internal documents from the Social Design Agency.[12] The report established three things. First, the operation is

professionally run, well-funded, and operates under direct Kremlin direction, with documents showing how directives are issued and outputs measured. Second, a leaked three-minute internal video shows Social Design Agency staff celebrating after the French exposure: being named was not a deterrent. Third, and most consequential for Swedish doctrine, attribution alone does not change Russian behaviour. Public attribution by itself is not defence; defence is building resilience that makes the operation less effective regardless of whether it is named.[13] *Beyond Operation Doppelganger* is the foundational text for Sweden's inform-and-empower doctrine, and the clearest public example of what a dedicated psychological defence agency can produce when it has analytical and outreach capacity in the same building.

The Quran burnings (2023): the crisis with strategic cost

In 2023, a series of public Quran burnings in Sweden, including one outside the Turkish embassy, triggered an international crisis. The episode drew convergent exploitation from Middle Eastern state media, Russia-aligned channels, and Islamist actors who amplified the burnings across Arabic and Turkish-language environments. The domestic terrorism threat level rose. Sweden's image in Muslim-majority countries, already damaged by the social services campaign, deteriorated sharply. Shortly after, a terrorist attack in Brussels killed two Swedes. The strategic cost was that Sweden lost the joint NATO accession with Finland it had hoped for: Türkiye prolonged the negotiations, and Sweden's accession was delayed by approximately a year.[14] The episode cost Sweden a concrete strategic objective, illustrated how convergent exploitation can weaponise a domestic incident into an international crisis, and demonstrated that Sweden has not yet found the architecture that would allow it to manage the domestic triggers of such crises without compromising its freedom of expression protections, which remain an asset to be defended rather than a constraint to be traded away. The Quran burnings sit on the same fault line as the social services campaign and the 2022 Easter riots that erupted around Rasmus Paludan's earlier Quran-burning provocations, the riots that prompted Prime Minister Andersson's public admission that Sweden had developed parallel societies.

Three crises, one fault line, examined in turn through three different lenses: foreign policy cost in 2023, integration failure in 2022, language and trust gap in 2021-22. The Honest Limitations section that follows treats the underlying vulnerability the three crises expose.

What Sweden has built: MPF as institutional design

MPF was established on 1 January 2022 in the Ministry of Defence as a dedicated agency for foreign information manipulation and interference, spun out of the larger Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB, which was itself renamed the Swedish Civil Defence and Resilience Agency, MCF, in January 2026). MPF and MCF are distinct agencies with complementary roles in Sweden's Total Defence architecture: MCF covers civil protection, emergency management, and critical infrastructure resilience; MPF is dedicated to psychological defence against foreign information operations. The agency has approximately eighty-five staff. Its mandate is the collective ability of Swedish society to defend itself against foreign information manipulation and interference. Its statutory restriction is that it does not operate within the Swedish information domain protected by freedom of speech: MPF looks at foreign actors using Sweden's information space, not at Swedish voices.[15]

The MPF mandate is constructed around a constitutional constraint that distinguishes the Swedish model from FIMI-oriented architectures elsewhere. As a state agency, the MPF is forbidden from monitoring domestic Swedish actors and is restricted to identifying, analysing, and countering foreign malign information influence directed at Sweden or at Swedish interests. The constraint is not incidental. It is the operational expression of the democratic principle that the state’s information-defence apparatus should not be turned on its own citizens, a principle inherited from the Cold War psychological-defence tradition and preserved deliberately in the 2022 reconstitution. The consequence is that the domestic disinformation ecosystem in Sweden, including the LVU campaign and other actors whose disinformation production is internal rather than externally directed, falls outside MPF’s reach by design. Detection of those domestic actors depends on civil society fact-checkers, the Swedish Security Service operating under its own mandate, and the journalistic media. This is a feature of the

Swedish architecture, not a defect. It is also the constraint that makes the Swedish model exportable to constitutional democracies that would not accept a domestically focused state agency.

MPF integrates three functions in a single civilian body: analysis through open-source intelligence and threat assessment to identify foreign information manipulation and interference; coordination and capacity-building across all departments and agencies responsible for resilience; and training, knowledge enhancement, and public outreach, including direct engagement with media, research funding, and participation in Sweden's dense media literacy network. Together, these functions allow MPF to identify, analyse, and respond to foreign information manipulation and interference in the context of modern hybrid threats. The integration of analysis and outreach in the same agency is MPF's unique selling point, the feature no other national agency combines. MPF keeps analysis and public education in one building because both functions are core to the mission: the analysis exists to inform citizens, and the public education exists to ground the analysis in democratic citizenship. Neither is subordinate to the other. VIGINUM does analysis without the outreach. Many national intelligence agencies do analysis without reaching publics. MPF does both, under one roof, and moves material from one to the other fluidly.[15]

The doctrinal foundation on which MPF's analytical methodology rests is the body of work commissioned by MSB and developed at Lund University under James Pamment in the late 2010s. Pamment et al., *Countering Information Influence Activities: The State of the Art* (MSB research report, 2018) and the companion handbook *Countering Information Influence Activities: A Handbook for Communicators* (MSB, 2018, revised) remain the operational reference texts that codified the Swedish approach to identifying and countering foreign information influence; MPF inherited this analytical genealogy when it was spun out as a dedicated agency in 2022, and its 2026 textbook *Psychological Defence and Information Influence: A Textbook on Theory and Practice* extends the lineage into a doctrine specific to the agency's integrated three-function mandate.

MPF has a public communications mandate that operates in three modes. First, direct public communication by the agency's leadership, calibrated up around major events such as national elections: the Director General appears on television regularly and has appeared alongside the Prime Minister to address election-period threats. Second, content injection into Sweden's dense media literacy network, which includes the Swedish Press, Radio and TV Authority, roughly twenty partner organisations, public libraries, cultural heritage institutions, schools from basic education through universities, and the folkbildning network of community colleges and study circles that forms the civil society backbone of Swedish civic education. MPF reaches publics at scale through channels those publics already trust. Third, analytical products like *Beyond Operation Doppelganger* that shape government attribution decisions and educate the broader public. Public communication about the threat environment is MPF's mandate; public attribution of specific foreign actions is a government decision that MPF supports with analysis.

The operating doctrine is empowerment. The goal is better democratic citizens in the digital age, not better digital citizens. Sweden is not pursuing digital literacy as a technical competence in the manner of Estonia. Sweden is pursuing the democratic capability to make collective decisions in an information environment where the conditions for that capability are being systematically attacked.[16] The doctrine carries with it a deliberate refusal to conduct offensive cognitive operations targeting foreign civilian populations. Sweden's defensive toolkit is active rather than passive. Sanctions enforcement and financial targeting of the companies and networks operating on behalf of the Kremlin, analytical work that supports government attribution decisions, educational work across the civilian population, and coordination work across the Swedish state. What Sweden does not do is run offensive information operations at adversary civilian audiences. That restraint is consistent with the position this report advances elsewhere: active defence is necessary; offensive cognitive operations targeting foreign civilian populations corrode the democratic norms they are meant to protect.

The coordination architecture extends outward from MPF through the rest of the Swedish state. The National Security Council was established in 2022 with its reporting structure under the Prime Minister, and the position of Minister for Civil Defence was reinstated after approximately fifty years. Civil defence cyber function centralised under FRA, the National Defence Radio Establishment, from January 2026.[17] Swedish ministries are small and inter-ministerial coordination is tight, partly a function of the Swedish administrative principle that agencies operationalise and ministries set policy. These institutional changes, taken together, move Sweden from an ad hoc response model to an architecture where MPF can identify an issue, work with the responsible agency to build capacity to own the response, and then step back. Most of MPF's work therefore flows through partner agencies rather than appearing under MPF's own name. This is deliberate and accepted.

Honest limitations

The most consequential gap in Sweden's cognitive defence architecture is the state's inability to reach some populations in their own languages, and the deeper relational distance between the Swedish state and the minority communities most targeted by foreign information operations. Norway, Finland, and Denmark have applied related architectures with stronger outcomes for community trust and reach, and any honest comparative assessment will not place Sweden ahead of its Nordic peers on this dimension.

The gap has two compounding components. The first is a communications problem MPF can partially address. Government information in Sweden runs primarily in Swedish and English. The communities most targeted by foreign information operations speak Arabic, Somali, Dari, Farsi, Tigrinya, Turkish, and other languages. MPF could publish in these languages, hire staff who speak them, and engage these communities directly; the agency has the institutional flexibility to make this an exception to the general Swedish-and-English rule where the threat environment warrants. Doing so would not close the integration gap on its own, but it would remove a specific, addressable barrier that currently amplifies the cognitive vulnerability these communities face.

The second component is deeper, and MPF cannot close it. The fault line documented through the threat cases above runs through the integration architecture the cognitive defence architecture sits on top of. In April 2022, in response to the Easter riots that erupted around Paludan's Quran-burning provocations, Prime Minister Magdalena Andersson stated publicly that segregation in Sweden had been allowed to go so far that the country had developed parallel societies, with citizens living in the same country but in completely different realities.[18] Sweden's foreign-born population is approximately twenty percent of the total resident population, roughly 2.17 million people as of 2024, and has roughly doubled since the early 2000s. Integration policy has not kept pace. Residential segregation in neighbourhoods such as Rinkeby in Stockholm and Rosengård in Malmö produces communities that the Swedish state's outreach architecture, however well-designed, struggles to reach with the trust required for messages to land.

The post-2022 security clearance overhaul, following a spy case that exposed a significant number of Swedish intelligence assets,[19] compounded the problem. It barred dual nationals from working in government service, removing a significant portion of Swedish nationals with Middle East and North Africa expertise from government service, a Layer 4 (intelligence, detection, and attribution) capability loss precisely when MENA-origin threat vectors were most active. More consequentially, the overhaul further erodes the trust necessary for integration between the Swedish state and the Muslim communities most targeted by disinformation. A state that fires its own dual nationals signals to its minority communities that they are not fully trusted; those communities then have little reason to trust the state's outreach. The integration problem runs through education, social policy, housing, employment, and the lived experience of diaspora communities in Sweden's larger cities. MPF can contribute to closing the communications component. The relational component requires policy work across the whole of Swedish government for which cognitive defence doctrine alone cannot substitute.

A final limitation warrants being added: the private-sector reporting gap. Corporate espionage is now directed more at Swedish companies than at Swedish public

institutions, because adversaries recognised the private-sector centrality of Swedish Total Defence before Swedish authorities fully did. Companies underreport incidents, in part because the Swedish legal process exposes proprietary information and in part because the current espionage legislation treats corporate espionage as a competitive business matter rather than a national security matter. Multi-year reform is underway to bring corporate espionage under national security framing. Until it lands, Sweden is making resilience decisions with incomplete information about what is happening in the part of its economy that carries most of the country's productive capacity.

What travels from Sweden

Three elements of the Swedish model are transferable.

The integrated two-sided agency model. A civilian body combining foreign-actor analysis and public outreach in one institution, with a clear mandate that does not encroach on domestic speech, is the single most transferable institutional choice. Other democracies split these functions across multiple agencies and lose the integration benefit. The condition is institutional trust: in contexts where a government agency speaking publicly on information threats would be treated sceptically or received as state propaganda rather than civilian resilience support, the model does not translate. Canada's institutional trust, while lower than Sweden's, is high enough for the model to be viable in adapted form.

The empowerment doctrine. The commitment to empowering citizens to be better democratic citizens in the digital age, rather than counter-messaging at them or running offensive information operations against adversary populations, is a doctrinal choice. It requires accepting that the work is slow and that its effectiveness is hard to measure against individual campaigns. The condition is political: empowerment doctrine requires leadership willing to defend a patient, civilian, educational approach against pressure to "do something" visible and aggressive after every adversary operation. Sweden's political class has so far defended the doctrine. The doctrine travels best as one component of a broader cognitive defence posture that also includes active defence (sanctions enforcement, attribution, cost imposition, infrastructure-level disruption of adversary operations).

The Total Defence social contract. The Swedish understanding that security is a shared civic obligation extending to citizens, private companies, and civil society, with legal teeth, is the foundational mentality from which everything else in the Swedish model flows. This is transferable in principle but requires a genuine public policy debate about whether the adopting country wants to rewrite its social contract in that way. The debate concerns what citizens owe the state, what companies owe the country, and what the state owes both in return. Sweden had this conversation historically and retained enough of the conceptual architecture to reactivate it. Canada, Germany, and most Western democracies have not had this conversation seriously in the post-Cold War period. Having it is the work that has to happen before Total Defence can be operationalised. This report names it as the conversation that should take place.

Sweden's partner landscape

Finland is Sweden's closest partner on cognitive defence and the senior partner Sweden most consistently references in the field. The two share social models, administrative traditions, and now NATO membership, and Sweden treats Finland as the model to learn from on civic preparedness. Norway and Denmark are the other Nordic peers: Norway is considering whether to establish an MPF-equivalent and has consulted MPF extensively;[19] Denmark operates through different institutional channels. The Nordic 5 format, which includes Sweden, Finland, Norway, Denmark, and Iceland, is the primary cooperation vehicle for values-aligned engagement on Arctic interests and social welfare alignment. The NB8 format, which adds Estonia, Latvia, and Lithuania, is the broader operational cooperation vehicle for regional engagement. Sweden treats the Nordic and Baltic clusters as analytically distinct: Nordic engagement rests on shared values, Arctic interests, and social welfare alignment; Baltic engagement rests on shared geographic security across the Baltic region, shared historical experience of Russian aggression, and the forward edge of NATO deterrence. The Baltic states are more aggressive on public attribution than Sweden, reflecting the existential threat they face across shared borders with Russia. Sweden is also a member of the UK-led Joint Expeditionary Force, which brings together all NB8 members plus the Netherlands.

At the European level, Sweden is invested in working through EU architecture. Sweden has seconded staff to the European External Action Service StratComs, and European Commission President Ursula von der Leyen committed during her 2024 re-election campaign to creating an EU version of the Swedish model, a statement Sweden takes seriously as the direction of European convergence. Sweden treats NATO and the EU as complementary but distinct cognitive defence architectures: NATO is the deterrence and defence pillar, the alliance through which collective defence against state adversaries is organised and where offensive capability gaps are debated; the EU is the resilience and regulatory pillar, the framework through which platform accountability, media literacy investment, economic sanctions enforcement, and democratic infrastructure are shaped.[19] France, through VIGINUM, is Sweden's closest bilateral methodology partner. MPF has learned from VIGINUM on analysis, VIGINUM has learned from MPF on outreach. Sweden has a secondee at NATO StratCom CoE in Riga and a position at NATO headquarters in Brussels added after accession. Sweden is an active member of the G7 Rapid Response Mechanism. Beyond Europe, Sweden engages through the Hybrid Centre of Excellence at Helsinki and views the EU democracy shield construct as the operational pathway for multilateral cognitive defence cooperation at scale.

Ukraine is the source of the most operational learning for Sweden, particularly on offensive reach-in techniques Sweden does not currently operationalise but recognises it may need to understand if the security environment deteriorates. Sweden has translated cognitive defence materials into Ukrainian and Romanian, funds training in Moldova and Ukraine, supports upcoming Armenia democratic work, and views Georgia as the cautionary tale of what happens when authoritarian power captures the state while Western democracies fail to come to the defence of a struggling partner.

Canada is an emerging partner of growing strategic interest. In November 2025, Prime Minister Mark Carney and Prime Minister Ulf Kristersson signed the Strategic Partnership between Canada and Sweden, a political framework across five policy areas: economic development and trade, security and defence, Arctic cooperation, science and innovation, and climate and energy.[20] The Strategic Partnership's security

and defence pillar explicitly establishes an enhanced strategic dialogue "on security and defence, including societal resilience, civil preparedness and the Swedish total defence concept," language that maps directly to the cognitive defence framework this report develops.

MPF is three years old. It is working. It is watched. What Sweden does next, particularly on the integration gap, will shape what other democracies choose to build.

Endnotes

1. Myndigheten för Psykologiskt Försvar (MPF), *Psychological Defence and Information Influence: A Textbook on Theory and Practice* (January 2026); & Jesper Orden, "A Genealogy of Swedish Psychological Defence," *Cooperation and Conflict* (Sage, 2025).

2. Total Defence Duty Act (*Lag 1994:1809 om totalförsvarsplikt*); Swedish Civil Defence and Resilience Agency (MCF), "Total defence – you are part of Sweden's overall emergency preparedness," mcf.se.

3. Kristin Ljungkvist, "Participatory War and Its Challenges for Total Defense," Carnegie Endowment for International Peace, August 2025; Orden (2025).

4. Field research, Stockholm. The ninety percent of companies figure is drawn from surveys by the Confederation of Swedish Enterprise (*Svenskt Näringsliv*) and based on self-identification with the Swedish Total Defence architecture.

5. Sweden's constitutional framework comprises four fundamental laws: the Instrument of Government (*Regeringsformen*), the Act of Succession (*Successionsordningen*), the Freedom of the Press Act (*Tryckfrihetsförordningen*), and the Fundamental Law on Freedom of Expression (*Yttrandefrihetsgrundlagen*).

6. Swedish Armed Forces (*Försvarsmakten*), "Sweden and NATO," forsvarsmakten.se, updated 2 December 2025.

7. Reuters, "Sweden to send fighter jets to patrol around Greenland as part of NATO's Arctic Sentry," 12 February 2026.

8. Field research, Stockholm. The public naming of Russia, China, and Iran is consistent across Swedish Security Service (Säpo) annual reports, MPF public communications, and government statements.

9. Field research, Stockholm & Swedish Security Service public communications. Swedish political science researchers raised early concerns about Chinese influence in higher education before STEM research communities did.

10. Field research, Stockholm. The Swedish Institute (*Svenska institutet*), under the Ministry of Foreign Affairs, tracks the international image of Sweden and produced analysis of the campaign's reach in Middle East markets.

11 VIGINUM / Secrétariat général de la défense et de la sécurité nationale, public attribution of Operation Doppelganger, 2023.

12 MPF, *Beyond Operation Doppelganger* (2024), available at mpf.se.

13 NATO StratCom CoE and Ukrainian Centre for Strategic Communications, *Attributing Russian Information Influence Operations: Testing the Information Influence Attribution Framework with Real-World Case Studies* (February 2026). The finding reshaped MPF's operational doctrine toward inform-and-empower rather than name-and-shame.

14. The delay of Sweden's NATO accession until 11 March 2024, approximately one year after Finland's accession on 4 April 2023, is public record.

15. MPF, *Psychological Defence and Information Influence: A Textbook on Theory and Practice* (January 2026); & MPF institutional documentation at mpf.se; field research, Stockholm.

16 field research, Stockholm; MPF public communications, including the agency's public-facing educational materials and Director General media appearances. The doctrine is developed institutionally in the MPF Textbook (January 2026).

17. Field research, Stockholm; Swedish government public documentation at government.se.

18. Prime Minister Magdalena Andersson, press conference, 28 April 2022, Stockholm, announcing measures against organised crime following the Easter 2022 riots that erupted around the Quran-burning provocations of Rasmus Paludan.

19 Le Monde, "When Sweden tracks down undercover Russian spies," 21 August 2023.

20. "Joint statement by Prime Minister Carney and Prime Minister Kristersson," Office of the Prime Minister of Canada, 18 November 2025, pm.gc.ca.

Chapter 21: Norway

Following Norway's occupation by Nazi Germany for five years during the Second World War, the country has built a total defence doctrine that is still operationally serious and continuously refined. Norway, a member of NATO, shares a direct land border with Russia, hosts the NATO Alliance's closest contact with the Russian Northern Fleet, and sits at the convergence of the High North, the Baltic Sea, and the North Atlantic. Russia is Norway's primary adversary in the cognitive domain. Norway is a real leader in civil preparedness, less frequently cited in international comparative literature than Sweden's psychological defence model or Finland's comprehensive security architecture but substantively comparable: total defence doctrine was reduced after the Cold War but not formally abandoned, and has been rebuilt since 2014 in response to the changing security environment; the architecture is NATO-tethered in a way that distinguishes it from the non-aligned Nordic lineage Sweden and Finland shared, extends to every municipality and every household, and the reflex of non-panic is a deliberate national project rather than a rhetorical one.

While that leadership has not yet crossed over into cognitive defence as a coherent institutional domain, the public service is starting to operationalize. The Ministry of Defence is pushing cognitive security and cognitive warfare as recognised terms at the political level, and the Norwegian Defence Research Establishment (FFI) contributes substantially to NATO's cognitive warfare research. The Norwegian political level lags. New legal authorities (Penal Code sections 130 and 130a) and an MFA Special Representative for Hybrid Threats are steps in the right direction, but disinformation remains housed in the Ministry of Culture rather than a security-oriented ministry like Justice and Public Security or Defence, no dedicated cognitive defence institution exists, and Norway maintains no public attribution posture comparable to France's VIGINUM or Lithuania's MOD-integrated strategic communication and civil society partnership model.[1] Russian cognitive operations have concentrated in the north with limited national-level impact. Norway has not yet been seriously tested.

Norway's civil preparedness leadership rests on three interlocking decisions that, applied to the cognitive domain, give Norway more protection than its current cognitive

architecture alone explains. Its total defence doctrine was reduced after the Cold War but not formally abandoned, and rebuilt from 2014. It takes transparency as a conscious decision based on the belief that an informed public is a more resilient public. And institutional trust is maintained through design rather than assumed as inheritance. Norway's longer-standing Arctic posture of measured engagement with Russia sits alongside these decisions as strategic context. The decisions are working. They are also more fragile than they appear.

Security culture and Norway's approach to defence

Norway is an old European kingdom on the northern edge of Europe with a particular relationship to threat. The state's modern form dates to 1905, but the institutional lineage runs centuries older, and the monarchy remains a functioning constitutional office that forms part of the trust architecture this chapter describes. Norway ranked sixth in the 2026 World Happiness Report, with the other Nordic states occupying five of the top six positions; the high-trust, low-corruption institutional environment captured in those rankings is the social-infrastructure foundation on which Norway's civil preparedness reflex rests. The five-year Nazi occupation remains in the public consciousness. Total defence doctrine, *totalforsvaret*, was built in the early Cold War as the whole-of-society response to the lessons from that time. It was significantly reduced and deprioritised in the post-Cold War decades but never formally abandoned, and rebuilding has been underway since 2014 in response to the changing security environment.[2]

The Long-Term Defence Plan 2025–2036, adopted unanimously by the Storting in 2024 and reinforced in March 2026 with an additional NOK115 billion bringing projected defence spending to 3.5 per cent of GDP by 2035, is the formal expression of that rebuilding. It commits Norway to maritime, air defence, and Arctic land force investments anchored in High North geography and structured around Norway's role as a reception and transit country for allied reinforcement of the Nordic region.

The Norwegian posture toward Russia reflects a broader cultural disposition. The word Norwegians use is *sindig*, carrying a sense of steady, level-headed, not easily provoked. The posture is consistent across administrations of left and right: engage where possible, respond proportionately, do not escalate rhetorically, maintain technical channels through

political rupture. Part of what keeps the north contained is Norwegian refusal to amplify provocations into national-level confrontations. This is both a Norwegian asset and an adversary condition: Russia has historically preferred measured stability in the Arctic, and Norway has reciprocated.

The threat environment

Russia is Norway's primary adversary in the cognitive domain. China is treated by the Norwegian intelligence services primarily as an intelligence threat inside Norway, focused on collection against industry and research. The 2010 Nobel Peace Prize to Liu Xiaobo is a distinct case: it triggered a coercive influence campaign by Beijing against Norway, a six-year diplomatic and trade freeze, and remains the paradigm case of Chinese pressure on Norwegian policy.[3] Since then, China has been less active in the influence operation sphere. Field research identified a more concerning medium-term vector than either: the United States. The Norwegian government threat assessments do not name the US as a threat, distinguishing Norway from Denmark on this point. What the United States has that Russia lacks in Norway is a receptive ideological community: cultural-war narratives around immigration, trans-rights, and urban-rural divides resonate with genuine Norwegian divisions in ways Russian narratives do not. The Norwegian Institute of International Affairs (NUPI) has documented the Norwegian-specific dynamics of Russian hybrid pressure most systematically through its 'Norway as an in-between for Russia: Ambivalent space, hybrid measures' project, funded by the Norwegian Ministry of Defence. Its policy brief 'Differentiating Hybrid Threats against the High North and Baltic Sea Regions' (Godzimirski et al.) argues for differentiating threats rather than boxing them into a single category, and names the structural risk that as Norway is seen by Moscow as an increasingly active 'NATO in the North', the policy of balancing deterrence with reassurance becomes harder to signal credibly. Three cases illustrate the Russian threat environment Norway is working inside.

The north-south divide and the Kirkenes pattern. Norway's political geography contains a durable north-south divide grounded in distance from Oslo and the particular identity of Finnmark, liberated by Red Army forces in 1944 and retaining a complicated relationship to both Moscow and Oslo. Oslo is roughly 1,700 kilometres from Kirkenes.

For Russia, this is the exploitable surface. The Russian Consulate General in Kirkenes is an open-source hub for operations in eastern Finnmark, where proxies and at times municipal-level interlocutors have been used to probe Norwegian responses, and where Soviet war memorials commemorating the 1944 liberation have been reactivated as vectors for memory politics directed at local and national audiences.[4] GPS jamming along the border is a continuous condition, now observable at lower altitudes and affecting fishing vessels. The pattern is Russia's theory of the case applied to Norway: concentrate where distance from Oslo makes national coherence hardest, where existing grievances offer amplification surfaces, and where the cost of sustained low-level pressure is low. The Norwegian response has been deliberate: invest in the north, investigate specific incidents, attribute privately, refuse the public escalation Russia would welcome.

Svalbard as threshold-testing. The archipelago's sovereignty and demilitarisation are governed by the 1920 Svalbard Treaty. Russia maintains a settlement at Barentsburg and operates the coal mine there. Russian activity has recently tested the edge of what Norwegian authorities will tolerate: a large Orthodox cross raised in a protected area and later relocated; a military-style Victory Day procession at Barentsburg; a vehicle closely resembling a Russian police car. While individually small, cumulatively they test what Norway will treat as provocation. The Norwegian response has been firm at the operational level without escalation at the strategic level. Svalbard shows both the utility and the limit of the *sindig* posture: measured response denies the adversary the political theatre it is prospecting for, but each incident raises the question of when the pattern itself becomes a cost Norway can no longer absorb.[5]

The 2025 pro-Russia party: transparency as defence at the national level. In the run-up to the September 2025 parliamentary election, a small political formation aligned with Russian narratives and funded under circumstances that raised immediate concerns contested for seats in the Storting on a platform of opposition to Norwegian military aid to Ukraine. It failed decisively, not crossing the 4% threshold for compensatory seats.[6] The decisive factor was visibility. Annual public threat assessments, election integrity brochures distributed to every household, and editorial coverage grounded in those assessments had already informed the public of the patterns foreign-influenced actors

use, and the party's messaging read to voters as foreign-directed rather than authentically domestic.

The architecture in practice

Norway does not officially use the term cognitive warfare. The Norwegian vocabulary is hybrid threats, in Norwegian *sammensatte trusler* or composite threats, alongside influence operations, malign influence, and disinformation. Hybrid warfare is avoided because it implies armed conflict, and the Norwegian position is that the threat sits below that threshold. FIMI is not used because Norway is not an EU member state, nor is the term psychological defence.[7] The absence of a clean terminological umbrella leaves the Norwegian response fragmented across instruments and ministries that each engage a piece of the threat rather than treating the cognitive dimension as a coordinated strategic challenge. This is a political-level constraint rather than a public-service one: within the defence establishment, concepts of cognitive security and cognitive warfare are being actively developed and pushed toward political leadership but have not yet been adopted.

What Norway has built rests on three interlocking decisions. The first concerns total defence. Russia's 2014 annexation of Crimea was the inflection point that triggered the rebuilding effort, after the post-Cold War decades had reduced the operational system to skeletal form. The eleven-year revitalisation that followed is led by the Directorate for Civil Protection and Emergency Planning (*Direktoratet for samfunnssikkerhet og beredskap*, DSB).[8] The *2026 total defence year* is its current operationalisation: approximately 400 municipalities across ten counties running their own county-specific tabletop exercises, with local recognition built in so scenarios feel close to home rather than generic. The purpose is to build the reflex of non-panic through rehearsal, so when something real happens the population and its local authorities have already walked through the problem. Household preparedness materials work the same way at individual level: the concrete answer to "what can I do." This architecture was not designed as cognitive defence. It delivers cognitive defence benefits as a by-product of civil preparedness done well.

The second decision is transparency. Annual public threat assessments from three independent Norwegian intelligence services, the Norwegian Intelligence Service (E-tjenesten, foreign), the Police Security Service (PST, domestic), and the Norwegian

National Security Authority (NSM), ground government communications in independent institutional analysis rather than in government narrative.[9] Household preparedness materials are distributed to every home and updated annually. Election integrity brochures are distributed in advance of major votes. DSB maintains an open crisis scenario library with approximately twenty-five scenarios which are publicly accessible and operationalised at municipal level. Norway does not describe this architecture as cognitive defence. It is civil preparedness and population-facing threat communication. That it denies strategic surprise and political leverage to actors who would claim the government is hiding something is a by-product.

Underwriting both is a third decision, less visible because it is not a security decision at all. Norwegian institutional trust has been maintained through design. Parliamentary oversight bodies, a sustained anti-corruption culture, the consolidation over the past two decades of twelve independent police districts into a unified national force, and transparent governance practices that have produced a citizenry that believes institutions function for them. Trust is the asset the other two decisions rest on and something those decisions deliberately maintain. It is also cracking. The OECD Survey on Drivers of Trust in Public Institutions, conducted in late 2023, recorded Norway as one of two OECD countries where the share of the population reporting high or moderately high trust in national government declined substantially from the 2021 base.[10] Younger Norwegians in particular have shown a decline as many drift toward algorithmically mediated news sources at the expense of editor-led media.

The coordination architecture is triangulated rather than centralised. The Ministry of Justice and Public Security has held a civilian coordinating role across approximately seventeen ministries since the 1960s, working in tandem with the Ministry of Defence. A Justice-Defence-Foreign Affairs triangle convenes regularly at working level. The sector principle provides the constitutional baseline: each minister bears security responsibility within their own sector, and no central authority can compel cross-sectoral coordination. The destination Norway is building toward is a joint task force across the three core ministries with written procedures and a formal mechanism for escalating disagreements rather than suppressing them. Sections 130 and 130a of the Norwegian Penal Code, in

force from 2024, criminalise activities on behalf of or in agreement with a foreign intelligence actor intended to influence decisions or public opinion where such activities can harm significant societal interests, and expand PST's authority to use covert surveillance methods.[11] Neither provision has yet been tested.

Honest limitations

Norway's current posture carries three structural gaps. The first is that the political level has not yet treated cognitive defence as a named institutional domain. The mechanism is the sector principle, identified as a problem in official Norwegian white papers for nearly thirty years without resolution. The expression of the mechanism is the 2024 disinformation strategy, placed with the Ministry of Culture rather than with a security-oriented ministry: a document grounded in media regulation and cultural policy rather than security strategy. The Ministry of Culture is the wrong lead for coordinating cognitive defence across the heavier security ministries because it lacks the mandate to compel them.

The second gap is detection, attribution, and response capability. Norway has had no joint-level information operations officers in its standing forces for over a decade until very recently; PSYOP capacity existed only for expeditionary operations; the Norwegian defence industry has had no demand signal to develop cognitive defence capability; and Norway maintains no public attribution posture comparable to France's VIGINUM or Lithuania's MOD-integrated strategic communication and civil society partnership model. Norway's private attribution culture is consistent with the *sindig* posture but leaves a capability gap that public functions elsewhere have begun to fill.

The third gap is regulatory. A draft Norwegian law implementing the EU Digital Services Act was circulated for consultation in July 2025, with application targeted for summer 2026, roughly two years after the Regulation began applying in EU member states.[12] The pattern repeats across the Digital Markets Act, the AI Act, and the NIS2 directive. Norway adopts at a lag and shapes from outside the room. The lag is political rather than administrative.

What travels from Norway

Two elements of the Norwegian approach are genuinely transferable, each with a condition for adoption.

The transparent threat communication architecture. Annual public threat assessments from independent intelligence services, household preparedness materials, election integrity communications, and an open crisis scenario library together produce a population that receives threat information from independent institutions rather than partisan mediators. The condition for adoption is commitment: transparency is how trust is built, not a reward offered once trust is already in place. Democracies that withhold public threat information because they do not trust their publics produce the distrust they fear.

The decentralised municipal implementation model. County-specific tabletop exercises, locally-grounded scenarios, and a reflex-of-non-panic orientation make population-level cognitive resilience a municipal function rather than a federal broadcast. The condition for adoption is functional municipal capacity and federal-to-local connective tissue. This is harder in federal or confederated states like Canada and Germany, where sub-national autonomy and jurisdictional layering work against the clean Norwegian federal-to-local pipeline. The principle can still be transferred with care, but the institutional form has to adapt to the constitutional structure rather than being imported directly.

Norway's partner landscape

Norway’s primary reference points for building cognitive defence are the United Kingdom and Finland. The UK is the model of a functioning resilience framework and one of Norway’s closest bilateral defence and intelligence partners. Norway looks to the UK for the institutional scaffolding cognitive defence would require inside a sector-principle state, an architectural challenge continental European models do not directly address. Finland is the benchmark for institutional continuity and whole-of-society engagement. Norway looks to Finland less for borrowing specific structures than for what sustained public-political alignment on threat perception looks like over decades, and the relationship is

close across defence, intelligence, and comprehensive security cooperation. Nordic-Baltic cooperation runs through NORDEFCO and the European Centre of Excellence for Countering Hybrid Threats in Helsinki, on whose board Norway sits. Norway is a founding member of the UK-led Joint Expeditionary Force. The NATO Strategic Communications Centre of Excellence in Riga is the research hub. Germany is a partner through the Council of Baltic Sea States format and bilateral defence cooperation. Norway and Canada are increasingly cooperating: the two signed a new five-pillar partnership agreement in Oslo in March 2026 during Prime Minister Carney's first visit to Norway, and the Norwegian Prime Minister hosted a Nordic 5 + Canada leaders format meeting the next day, a format that has gained traction in recent years.[13] The United States remains Norway's most important defence partner through NATO and through bilateral security arrangements including Arctic surveillance and intelligence sharing. For cognitive defence specifically, the relationship is becoming more complicated: recent US unreliability, including direct pressure on Nordic and NATO members, introduces a variable into Norwegian partnership calculations that did not exist in previous cycles.

The structural question underneath Norway's partner landscape is the European Union. Norway held membership referendums in 1972 and 1994 and voted no both times, though the 1994 result was narrow at 52.2% against. Membership has been off the Norwegian political agenda since, with the EEA Agreement serving as the practical substitute for single-market participation. Two shifts are pressing against that settlement. Iceland, Norway's closest EEA peer, will hold a referendum on 29 August 2026 on whether to resume accession talks suspended in 2013.[14] Norwegian opinion polling has narrowed to roughly 41 per cent for membership and 48 per cent against, the closest gap in three decades. The Norwegian Government has ruled out reopening the debate for now but is watching Iceland closely. What Norway does next on cognitive defence will depend as much on how its partnerships hold as on how its own architecture evolves.

Endnotes

1 Jana Wrange, Rikard Bengtsson and Douglas Brommesson, 'Resilience through total defence: Towards a shared security culture in the Nordic–Baltic region?', *European Journal of International Security* 9:4 (November 2024), pp. 511–532, at cambridge.org; James Kenneth Wither, 'Back to the future? Nordic total defence concepts', *Defence Studies* 20:1 (2020), pp. 61–81; and Christian Fjader and Juuso Schalin, *Building Resilience to Hybrid Threats: Best Practices in the Nordics*, European Centre of Excellence for Countering Hybrid Threats, May 2024, at hybridcoe.fi.

2 Norwegian Ministry of Defence historical documentation at regjeringen.no; Meld. St. 9 (2024-2025), *Total Preparedness: A Whole-of-Society Approach to Norwegian Security and Emergency Preparedness*, Norwegian Ministry of Justice and Public Security, May 2025, at regjeringen.no/en/documents/meld.-st.-9-20242025/id3082364. and Wrange, Bengtsson and Brommesson (cited above) on the post-2014 directional shift back toward whole-of-society total defence.

3. NIS, *Focus 2026*, February 2026, at etterretningstjenesten.no/publikasjoner/focus.

4. Norwegian Intelligence Service, *Focus 2026*, February 2026, and field research with Norwegian security and intelligence officials, Oslo, autumn 2025.

5. "An Arctic Gateway at Risk: Protecting Svalbard from Russian Aggression," U.S. Naval Institute Proceedings 152, no. 5 (May 2026), usni.org.

6 Norwegian parliamentary election, 8 September 2025. The election's headline result was the return of the Labour Party-led government under Prime Minister Jonas Gahr Støre; the pro-Russia formation described in this paragraph did not cross the 4% threshold for compensatory seats. Field research, Oslo, autumn 2025.

7 The 2026 Norwegian Intelligence Service assessment *Focus 2026* and the 2024-2025 Total Preparedness white paper (Meld. St. 9, 2024-2025) both use *sammensatte trusler* (composite threats) and hybrid threats interchangeably in Norwegian and English.

8 *Total Preparedness: A Whole-of-Society Approach to Norwegian Security and Emergency Preparedness*, Norwegian Ministry of Justice and Public Security, May 2025.

9 NIS, *Focus 2026*, February 2026, at etterretningstjenesten.no/publikasjoner/focus; PST, *National Threat Assessment 2026*, at pst.no; NSM, *Risk 2026*, at nsm.no.

10 Organisation for Economic Co-operation and Development, *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results: Building Trust in a Complex Policy Environment* (OECD Publishing, Paris, 2024), and country note for Norway.

11 *Lov om endringer i straffeloven og straffeprosessloven*, implementing Prop. 42 L (2023-2024), introducing Sections 130 and 130a of the Norwegian Penal Code (*Straffeloven*) on influence from foreign intelligence, in force from 2024.

12 Norwegian Ministry of Digitalisation and Public Governance, *Høring – forslag til lov om digitale tjenester (digitaltjenesteloven)*, public consultation circulated 2 July 2025, consultation deadline 1 October 2025.

13 Prime Minister of Canada, "Joint statement on Strategic Cooperation between Canada and the Kingdom of Norway," Oslo, 14 March 2026, at https://www.pm.gc.ca/en/news/statements/2026/03/14/joint-statement-strategic-cooperation-between-canada-and-kingdom-norway.

14 Government of Iceland, 'The Icelandic Government's proposed referendum on continued EU accession negotiations', government.is, 2026.

Chapter 22: Denmark

Denmark has spent 180 years building a society organised around democratic formation, civic association, decommodified housing, shared public space, and educated citizenship. This architecture is its primary cognitive defence asset. That is the diagnostic this chapter delivers. The Danish foundation layer was not built for security purposes and is not described in security terms by the Danish state, the Danish educational establishment, or the practitioners who maintain it. It nevertheless functions as the most effective cognitive defence infrastructure in this research set, and it is the reason a population with the highest interpersonal trust scores in the world resists the fracture operations targeting peer European democracies more effectively than countries with formal cognitive defence agencies and total-defence doctrines do. Denmark has no Swedish Psychological Defence Agency analogue, no French VIGINUM analogue, and a coordination architecture built for hybrid threats that meets as needed rather than continuously. Against this foundation-layer strength and coordination-layer modesty, the Kingdom has faced pressure of a different order: a formal Ally has applied instruments of power against the *rigsfællesskab*, the constitutional community that ties together Denmark, Greenland, and the Faroe Islands as one Kingdom under shared defence and foreign policy while preserving Greenlandic and Faroese self-government on domestic affairs. A December 2025 assessment by Danish Defence Intelligence named the threat: the United States is willing to use instruments of power against Allies, and uncertainty about the American security guarantee for Europe is now a settled finding of the Danish defence establishment.[1] The chapter reads Denmark's architecture against both the long historical record and the present stress test, and returns to the diagnostic the case makes visible.

Security culture and Danish terminology

Denmark is a maritime country of approximately six million people whose security identity has long been organised around Alliance membership rather than self-sufficient deterrence. Denmark joined NATO at its founding in 1949. Cross-spectrum parliamentary consensus on Ukraine has held across Russia's full-scale invasion and

stands as the clearest Danish example of a security question on which elite agreement holds firmly enough that adversaries cannot exploit divisions among the political class.

Danish institutional vocabulary on the cognitive threat environment is not unified. Defence uses *cognitive domain* or *cognitive dimension* in operational discussion and reverts to *information warfare* as the default institutional term.[2] The NATO cognitive warfare concept is known in the Danish defence-academic community but has not been institutionally adopted, both because the concept has not completed formal NATO approval and because there is some scepticism within the Danish defence community that *cognitive warfare* names anything new not already covered by information warfare, hybrid warfare, and psychological warfare doctrine already in operational use. The Ministry of Foreign Affairs works within the EU framework of Foreign Information Manipulation and Interference (FIMI). The Defence Intelligence Service (Forsvarets Efterretningstjeneste, DDIS) and the Danish Security and Intelligence Service (Politiets Efterretningstjeneste, PET) use *disinformation, propaganda, and other influence activities* across their respective external and domestic mandates.[3] The working unifying term in civilian and defence-academic contexts is *cognitive resilience*.[4] The architecture that would unify the threat landscape across defence, MFA, and intelligence agencies has not been built. More consequentially, Denmark has working vocabulary for what adversaries do and no institutional vocabulary for what Denmark itself has built, that is, no recognition that the country's social, educational, and civic infrastructure functions as cognitive defence at all.

The 180-year design tradition

Denmark's foundation-layer cognitive defence is the cumulative outcome of five overlapping design traditions, built from the 1830s through to the present. Each layer reinforces the others, and each works against the conditions adversarial cognitive operations exploit: isolation, low trust, weak associational density, hollowed public space, housing precarity, civic disengagement, and the loss of dialogue across difference.

The folk (public) high school heritage (1830s onwards). N.F.S. Grundtvig's vision of education for democratic formation, articulated from the 1830s and put into practice

from 1844 onwards by Christian Kold and others, is widely credited by Danish and Nordic scholarship with paving the way for Denmark's transition to parliamentary democracy at the turn of the twentieth century.[5] The folk high schools (*folkehøjskoler*) were built on the premise that democracy requires citizens capable of dialogue across difference and that education must serve life rather than examination, captured in Grundtvig's principle that the school must be for life, not just for the school (*Skolen for Livet*). The Danish Folkeskole's official three-part purpose, formally stated, requires the school to provide knowledge and skills, to contribute to the all-round personal development of pupils, and to prepare them for participation, co-responsibility, rights, and duties in a democratic society marked by freedom of spirit, equality, and democracy.[6] This is the philosophical root from which every subsequent layer of the Danish architecture grows.

The associational tradition (1849 onwards). The 1849 Constitution established the right of association, and Danish society has organised itself through associational life (*foreningsliv*) ever since. Denmark today has approximately one association for every 80 inhabitants, approximately 90 percent of adults belong to at least one association, and approximately 40 percent regularly volunteer, primarily through associations.[7] Associations cover sports (two-thirds of voluntary associations are sports clubs), politics, religion, hobbies, culture, hunting, and effectively every domain of social life. Comparative European data place Denmark, alongside Norway, Sweden, and Finland, among the densest civic infrastructures in the developed world.

The educational layer and Klassens Tid. Inside the Folkeskole sits the practice we treat as a defining foundation-layer cognitive defence practice in the Danish system. Klassens Tid is a long-standing Danish school practice embedded in the structural framework of the Folkeskole, where approximately one lesson per week at each grade level is devoted to the life of the class through the school's time-bank allocation. Children from early grades practice three capacities a democratic citizen in a contested information environment needs: holding different perspectives simultaneously and remaining in conversation across disagreement, recognising their own emotional reactions and those of others, and a sense of belonging to a community in which their

voice matters. The second is the capacity that connects most directly to the report's wider argument about emotional regulation as a foundation of cognitive defence. The practice's principal articulator describes the cognitive defence mechanism as a pause: the cognitive interval between an emotional reaction and its expression as action, which is the precise capacity adversarial operations, exploiting fear, outrage, and grievance, work to overwhelm.[8] Children who practice the pause weekly through twelve years of schooling enter adult civic life with structural protection against the fastest and most damaging adversarial cognitive operations. The practice has been tested as a design element across European contexts through an Erasmus+ methodology developed with partners in Slovakia, Italy, Austria, and Slovenia. The binding transferability condition is that the adults carrying the practice must have the relational and emotional capacity to embody what children are learning, and curriculum transplant without teacher formation does not produce the effect.

The housing layer (1930s onwards). Approximately 20 percent of the total Danish housing stock, approximately 500,000 homes, is held in *almene boliger* (literally common housing), a permanent non-profit form deliberately designed for the whole population rather than as residual social housing for the poor.[9] Mixed neighbourhoods of students, families, elderly residents, workers, and low- and middle-income tenants are the system's design goal. Rents are capped at 25 percent of income and tenant democracy operates through resident governance. The system emerged from cross-party compromises in the 1930s and has remained politically untouchable across all Danish governments since. The Danish cohousing movement (*bofællesskab*) produced the world's first modern intentional cohousing communities at Sættedammen (1972) and Skråplanet, and approximately 110 documented intergenerational cohousing communities exist in Denmark today.[10] The shared finding across the Danish housing tradition is that housing is not a speculative asset but the foundation of community.

The public space layer (1962 onwards). On 17 November 1962, Copenhagen converted Strøget, the city's main thoroughfare, into a pedestrian street as a temporary experiment. The first year produced a 35 percent increase in pedestrian use and a 400 percent increase in baby carriages observed in the street. Over forty years Denmark

converted approximately 100,000 square metres of central Copenhagen from vehicle space to pedestrian space. The principle is that the form of the built environment shapes the social life that occurs within it: designing for human encounter rather than vehicle throughput produces measurably different civic outcomes. This effort was met at the time with criticism that public space use was contrary to Nordic mentality and that Danes were not Italians; the criticism turned out to be wrong because the architecture was the determining factor, not the culture.[11]

The cumulative outcome: among the highest interpersonal trust levels in the world. The 2022 wave of the Integrated Values Survey records 74 percent agreement among Danes that most people can be trusted, the highest figure in the world, ahead of Norway (72 percent) and Finland (68 percent).[12] The 2026 World Happiness Report places Finland, Iceland, and Denmark in the top three globally, with five of the top seven countries Nordic; Denmark scores particularly highly on social support and institutional trust, the indicators most directly relevant to cognitive defence. [33] Denmark and Sweden also report the lowest perception of corruption in the OECD, both under 20 percent against an OECD average of 54 percent. The Danish political scientist Gert Tinggaard Svendsen has estimated that interpersonal and institutional trust accounts for approximately 25 percent of Danish national wealth.[13] Several elements of the Danish architecture, including the folk high school heritage and the associational tradition, sit within a regional Nordic inheritance rather than being uniquely Danish, with Denmark distinguished particularly by *almene boliger* at scale, *bofællesskab*, *Klassens Tid*, and *Cities for People*; Chapter 29 develops the Nordic-cluster comparison in cross-case terms. [34] Trust is the cumulative outcome of the layered design tradition described above, and the substance that makes Danish civic and political life resistant to fracture.

The non-recognition diagnostic. None of these layers is described in Denmark as security infrastructure. Each layer was designed to address a specific historical problem within Denmark, none of them adversarial cognitive operations, and yet each layer functions against the conditions those operations exploit. The Danish state has not framed any of this as cognitive defence, and the cognitive defence community internationally has not yet recognised it as such. NATO's own resilience framework,

organised since 2016 around Article 3 and seven Baseline Requirements, is closely adjacent to the cognitive defence space but does not reach the educational, associational, or housing layers Denmark has built.[14] That non-recognition is the central exposure Denmark faces.

The threat environment

Russia is the primary influence adversary. Official Danish assessments rate the Russian influence threat against Denmark as low. Field research from a limited set of conversations suggests this rating may understate the volume of Russian activity in the Danish information space, with some Danish analysts judging that middle would be a more appropriate calibration.[15] The directional observation matters: most Russian disinformation involving Denmark uses Denmark as subject matter rather than as audience. Russian-origin content about Danish migration policy, Danish positions on Ukraine, or Danish involvement in NATO Arctic activity is circulated to broader European publics to shape European perceptions of Denmark, with Danes encountering it only secondarily through European media. Direct in-Denmark targeting is comparatively rare. The cognitive defence implication is that Danish information-space monitoring catches less than the full Russian threat, because much of the threat operates outside Denmark and against Danish reputation rather than against Danish opinion. Three political candidates of Russian background chose to resign before elections in recent years, documented domestic influence exposure with limited but real reach.

Operation Overlude, also called Operation Matryoshka by European factchecked media, is a campaign active since 2024 that has sent European media including Danish outlets misleading emails directing coverage toward specific issues. Danish factchecked media have documented the campaign extensively and named it publicly. Traditional Danish media engage each instance as a separate editorial question rather than recognising the pattern.[16] This coordination failure between the factchecked-media ecosystem and the traditional-media ecosystem is a finding at the information-environment-integrity layer of the framework, specific to the Danish information environment but not unique to it: the same coordination gap appears in several of the cases this report examines and is widely shared across European democracies.

A second finding sits at the same information-environment-integrity layer and concerns artificial intelligence training data. Two high-volume low-quality disinformation networks, Grafterr and EurAmo, produce content in Danish alongside other European languages. The density of that content in web-scale data sets, the open web data on which large language models are trained, increases the probability that the models surface versions of the narratives those networks produce. The mechanism is straightforward: when a Danish user asks a large language model about a topic these networks have flooded, the model is more likely to repeat shaped framings that originated as deliberate disinformation. Disinformation exposure for Danish users does not end with the content they read on platforms the EU regulates; it extends into the AI tools they use for work, education, and information seeking, an emerging structural vulnerability the Digital Services Act architecture does not yet reach.

China operates in Denmark as a backstage rather than frontstage influence actor, concentrated in espionage, commercial presence, and academic and research activity. Chinese activity in Greenland decreased after 2019 and has not, to public knowledge, resumed.[17] Chapter 3 develops the pattern of Chinese digital activity that amplifies anti-Danish narratives during periods of diplomatic friction.

The United States was not named as a threat actor in Danish institutional assessments before 2025. It is now.

The Greenland case as test

The shift in Danish posture towards the United States consolidated in December 2025. A 2019 fabricated letter, purporting to be from Greenland's Minister of Foreign Affairs to United States Senator Tom Cotton and requesting funding for an independence referendum, established Greenland as a named influence target seven years before the current crisis.[18] During the spring 2025 Greenlandic parliamentary election, Danish media covered a podcast featuring a United States consulate employee in conversation with Greenlandic independence activists; had a Russian consular employee conducted the same activity, the framing as foreign interference would have been immediate. In May 2025, following Wall Street Journal reporting that United States intelligence had been directed to step up activity in Greenland, the Danish MFA summoned the United

States chargé d'affaires.[19] On 27 August 2025, Danmarks Radio (DR) published an investigation based on eight sources in Denmark, Greenland, and the United States identifying at least three Americans with ties to President Trump conducting covert influence operations in Greenland: one had compiled a list of United States-friendly Greenlanders and collected names of individuals opposed to the administration while two others cultivated contacts with Greenlandic politicians and businesspeople. DR knew the names and chose not to publish them, to protect sources. The Danish Foreign Minister summoned the United States chargé d'affaires the same day. PET, which before August had framed foreign interference in Greenland without naming the United States, acknowledged Greenland as the target of influence operations aimed at damaging its relationship with Denmark.[20] The December 2025 DDIS Intelligence Outlook consolidated the posture institutionally.

Denmark's response has been structured around the *rigsfællesskab*, and is recognisably the same logic Denmark has applied for 180 years: deliberate community building, decommodification of basic goods, genuine inclusion across constitutional asymmetry, and investment in the autonomous capacity of partners. The strategy rests on three components: material incentives beyond constitutional requirements (Danish financing of functions Greenland would otherwise self-finance, including significant investment in the Greenlandic Health Service); genuine political inclusion beyond constitutional requirements, intensified during the crisis; and a principled self-determination line captured in the Danish Prime Minister's repeated position that Greenland is not for sale and that its future belongs to the Greenlanders. The underlying logic is an analytical-capacity argument. Classified intelligence sharing, secure communications, funded academic positions at the Universities of Greenland and the Faroe Islands, and a Royal Danish Defence College education programme for Greenlandic leaders from 2025 are components of a single strategy. A partner reaching its own conclusions from its own intelligence picture produces decisions more resilient to external manipulation than one dependent on Copenhagen.[21] Greenlandic Prime Minister Jens-Frederik Nielsen's statement at a January 2026 joint press conference in Copenhagen, declaring that Greenland would stand with Denmark rather than the United States and has huge faith in the NATO Alliance, is the clearest public indicator

the strategy has held.[22] The Greenland response is not improvisation under pressure. It is the design tradition extended outward under stress.

The Faroe Islands sit in a different position. Geographically more exposed than Greenland, located among the most contested maritime corridors in the North Atlantic, they have been slower to embrace a security-policy framing of their external relationships. Danish cyber defence authorities operate in the Faroe Islands by invitation only. Foreign direct investment legislation of the kind Greenland is developing is not on the Faroese horizon. The Faroese maintain an active fisheries agreement with Russia that permits vessel port access; after 2014, the Faroe Islands expanded commercial exports to Russia as European markets closed; after 2022, Faroese sanctions alignment with the European line has increased meaningfully but remains incomplete.[23] The paradox is that the more geographically exposed component of the *rigsfællesskab* carries the less advanced security posture, and the Danish design tradition has not yet been fully extended to the Faroe Islands.

NATO has been the load-bearing deterrence vehicle. The Arctic Endurance exercise in January 2026, with allied NATO participation, was the inflection point at which escalation risk was contained. The deterrence mechanism was diplomatic: the prospect of NATO credibility rupture with the larger European Allies was the cost the United States was not willing to incur. NATO's Arctic Sentinel framing, consolidating activity in the European High North, Iceland, and Greenland under a single strategic concept, allowed Denmark to counter the American characterisation of an Arctic security vacuum with the demonstration that NATO was occupying the space.[24] France was particularly forward-leaning in its public support, including President Macron's March 2025 visit to Greenland. Polish support was limited. Latvia and Lithuania did not publicly back Denmark as strongly as some other European partners; Estonia carried a more nuanced public position. The Danish reading is that the visible Baltic restraint reflects those states' existential dependence on United States security guarantees rather than a structural divergence in values. The perception of weak Baltic backing matters even where the underlying analysis is honest about its causes, and is worth noting candidly.

Coordination architecture and honest limitations

Denmark does not operate a dedicated psychological defence agency, nor a VIGINUM-style attribution and analytical capacity. The Ministry of Resilience and Preparedness (Ministeriet for Samfundssikkerhed og Beredskab), established in 2024, leads the cross-government effort on civil preparedness, hybrid threat coordination, and societal resilience under conditions of conflict short of armed attack. Consolidating activities from eight ministries, it houses the Danish Emergency Management Agency and the Danish Agency on Resilience and coordinates communication with public and private organisations on hybrid and cognitive threats. The Ministry's creation has opened a live debate on the sectoral responsibility principle (*sektoransvarsprincippet*) under which each ministry bears security responsibility within its own sector. The architectural problem is the same one Norway has carried for thirty years: a new ministry cannot, by itself, compel cross-sectoral coordination on an agency system built to disperse it.[25] What the new Ministry can do, and is doing, is provide a single coordination point and a single political voice for the resilience agenda within Cabinet, a meaningful step short of the structural reform the sectoral principle would require. The inter-ministerial task force on foreign interference convenes the Ministry of the Interior, the Ministry of Defence, the Ministry of Resilience and Preparedness, DDIS, and PET, and meets as needed.

Section 108 of the Danish Criminal Code (*straffeloven*) criminalises cooperation with foreign intelligence services to alter democratic opinion or political decision-making in Denmark, with aggravated sentencing where the alteration occurs during parliamentary elections.[26] The provision has not produced significant prosecutions; a Danish propagandist has won defamation cases against individuals who labelled him an agent of influence, because the term implies betrayal of the country, a higher evidentiary threshold than defamation plaintiffs have been willing to meet.[27] The analytical judgment within Danish security practice is that naming and shaming through factchecked media produces more resilience effect than courtroom action.

What Denmark builds against the threat and the central exposure

Denmark's preferred response doctrine on the active-defence side is prebunking, learned from Ukrainian practice and now institutionally adopted at EU and NATO level.

Danish monitoring of the COVID-era domestic conspiracy environment produced the assessment that the 2020 platform restrictions on anti-vaccination and QAnon content were effective: ringleaders migrated to Telegram and retained peer-to-peer communication but lost reach to ordinary audiences. The precedent supports the judgment that time-limited, proportionate platform restrictions can function as legitimate tools, provided the framing is specific to the threat rather than a general instrument of speech regulation.[28] Denmark's active-defence contribution runs through EU architecture: the EEAS East StratCom Task Force, the Digital Services Act, and the EU Democracy Shield initiatives. Among Danish defence-academic interlocutors, the assessment is frank: VIGINUM is a strong model that Denmark cannot replicate at resource or intelligence-service scale, France having it benefits all European democracies, and Denmark's contribution is better placed in the foundation-layer and coordination roles where its comparative advantage sits.

Denmark has spent 180 years building one of the most cognitively resilient societies in this research set. The folk high school heritage, the associational tradition, the educational layer with Klassens Tid at its core, the housing layer with *almene boliger* and *bofællesskab*, the public space layer with *Cities for People*, and the trust outcome are the architecture that holds the population's resistance to adversarial cognitive operations in place. None of this architecture is recognised in Denmark as security infrastructure. It is educational policy, social policy, housing policy, urban planning policy, and a sociological outcome. The Danish vocabulary on the cognitive threat environment has not unified across defence, MFA, and intelligence agencies, and it does not reach the foundational layer at all. The structural vulnerability the Arctic case has made visible, where non-traditional security actors, including Indigenous organisations, sub-state governments, and the constituent parts of the *rigsfællesskab*, namely Greenland and the Faroe Islands as self-governing components within the Danish Kingdom, are the entry points adversaries exploit, is one expression of a wider structural fact: Denmark has not built a security framework that recognises its own foundations.

The exposure is more serious than non-recognition alone. Standardisation pressure on the Folkeskole, financialisation pressure on housing, privatisation pressure on public space, and bureaucratisation pressure on associational life are real and ongoing. None of these pressures is framed in Denmark as a security threat. Each erodes one element of the architecture that holds Danish cognitive resilience in place. The country that has done the most to build the foundations of democratic defence has the least developed institutional vocabulary for recognising what those foundations are and what threatens them, and this is the diagnostic the Denmark case contributes to the rest of the report.

Partner landscape

Denmark does not, at present, work closely on cognitive defence specifically with any partner outside Sweden and Finland. Within those bilateral relationships, deepened since Finland's and Sweden's NATO accession, cooperation runs through threat-picture sharing and joint work on Russian disinformation in the Nordic information space. The formal regional architecture sits in the Nordic Council and the Nordic Council of Ministers, with rotating annual presidencies and Copenhagen-based secretariats. Denmark holds the 2026 Presidency of the Nordic Council of Ministers under *The Nordic Region: Strong ties in changing times*, focused on societal security and the protection of children and young people in the digital age.[29] The informal Nordic 5 and Nordic-Baltic 8 formats cover foreign and defence policy among the five Nordic states and, in the NB8 case, with the three Baltic states; neither carries a specific cognitive defence coordination mandate.

Denmark's most diplomatically important European partners beyond the Nordic-Baltic frame are France, Germany, and the United Kingdom. None currently carries close working cooperation on cognitive defence specifically with Denmark; cooperation runs through EU structures (EEAS, FIMI Toolbox, Democracy Shield) and NATO. France stood out during the Greenland crisis for the speed and forwardness of its public support, including President Macron's March 2025 visit. The February 2026 analysis by Bruun, Zilmer-Johns, and Yücel for the Danish Foreign Policy Society and the Royal Danish Defence College frames the broader strategic reorientation: Danish security policy can no longer rest primarily on United States guarantees and must anchor in a

more European NATO, a stronger EU (especially after Denmark abolished its long-standing defence opt-out in 2022 and joined the EU's Common Security and Defence Policy), and close defence cooperation with the Nordics, France, Germany, and the United Kingdom.[30]

Canada is Denmark's most immediately relevant non-European partner, viewed as a like-minded country under structurally similar adversarial pressure from the United States. The 14 June 2022 agreement on Hans Island (Tartupaluk), the Lincoln Sea, and the Labrador Sea continental shelf boundaries ended one of the longest-running peaceful boundary disputes in the world and means Canada now shares a maritime border with the *rigsfællesskab* through Greenland.[31] Active cooperation on cognitive defence specifically remains limited at present, which this report argues should change.

What travels: lessons from the Danish architecture

Six elements of the Danish architecture travel, from most directly transferable to hardest.

Klassens Tid travels most directly. The Erasmus+ methodology developed with Danish, Slovak, Italian, Austrian, and Slovenian partners between 2019 and 2022 provides the practitioner template, and the binding condition is that teachers and other adults carrying the practice must have the relational and emotional capacity to embody what children are learning. Curriculum transplant without teacher formation does not produce the effect.

Decommodified housing on the *almene boliger* principle is directly transferable. Housing as foundation of community rather than speculative asset, organised through non-profit housing associations with permanent non-profit status, mixed neighbourhoods designed deliberately, and rents capped relative to income, is replicable in any democracy. Vienna, Singapore, and the Netherlands operate variants. The Danish lesson is that sustained cross-party political support is the precondition.

Cities for People has already been exported widely; the additional Danish lesson is that public space design should be treated as civic infrastructure within democratic resilience strategies, not as urban-amenity policy.

The associational layer is partially transferable. The constitutional right of association exists in most democracies; what Denmark adds is the dense, normalised participation pattern produced by 175 years of practice and supportive policy, including tax treatment, public funding for voluntary organisations, and the cultural assumption that association membership is part of citizenship.

The *rigsfællesskab* strategy travels as a template for managing internal constitutional stress under external pressure: material incentives and political inclusion beyond constitutional requirements, a principled self-determination line, held together by investment in the component's own analytical capacity. Federations and plurinational states facing comparable external pressure on their constituent parts can apply the same logic.

The overall design tradition itself is the hardest to transfer because it requires generational time horizons and political-economic conditions most democracies have not maintained. The diagnostic the tradition produces is portable: democracies in this era cannot rely on cognitive defence agencies and FIMI doctrines alone, and must reckon with the foundations of their own social architecture as security infrastructure. The consensus condition is not directly replicable. What travels is the infrastructure that makes consensus possible: national defence courses for parliamentarians, cross-party security briefings, and elite socialisation into a shared threat assessment before the crisis arrives.

What Denmark has built has held. What Denmark does not yet name as security infrastructure is what has made the holding possible, and that non-recognition is the contribution the Denmark case makes to the rest of this report.

Endnotes

1 Forsvarets Efterretningstjeneste (Danish Defence Intelligence Service, DDIS), *Intelligence Risk Assessment 2025*, 10 December 2025, fe-ddis.dk..

2 Field research, Copenhagen. The terminological mapping reported here is drawn from interviews with serving and recently retired Danish defence-policy officials, defence-academic interlocutors at the Royal Danish Defence College and Aarhus University, and intelligence-service interlocutors at PET and DDIS.

3 PET, *Vurdering af terrortruslen mod Danmark* (annual); DDIS, *Intelligence Risk Assessment* (annual); PET, *Illegal foreign interference*, pet.dk.

4 Field research, Copenhagen.

5 Niels Lyhne Jensen et al., *A Grundtvig Anthology* (Cambridge: James Clarke & Co., 1984).

6 Danish Ministry of Children and Education (Børne- og Undervisningsministeriet), *Folkeskolens formål*, uvm.dk.

7 Lars Skov Henriksen and Klaus Levinsen, *Hvem deltager? Civilsamfundsundersøgelsen* (Frydenlund Academic, 2019).

8 The description of Klassens Tid's mechanisms and their relationship to societal resilience draws on written correspondence with Iben Sandahl, October 2025, used with permission, and on her forthcoming minibook *Klassens Tid: The Danish Practice of Empathy, Dialogue and Democratic Formation*.

9 Bent Madsen (President, Housing Europe), interview, *Housing Ireland Magazine* 2023/2024

10 Henrik Gutzon Larsen, "Three Phases of Danish Cohousing: Tenure and the Development of an Alternative Housing Form," *Housing Studies* 34, no. 8 (2019).

11 Global Designing Cities Initiative, "Pedestrian Only Streets: Case Study | Strøget, Copenhagen," globaldesigningcities.org.

12 Integrated Values Surveys, 2022 wave, accessed via Our World in Data.

13 Gert Tinggaard Svendsen, *Trust* (Aarhus University Press, 2014).

14 NATO, *Resilience, civil preparedness and Article 3*, nato.int.

15 Field research, Copenhagen.

16 On Operation Overlude (also labelled Operation Matruschka by European factchecked media): EU DisinfoLab, annual disinformation monitoring publications, 2024–2026; Tjekdet.dk, multiple Danish-language reports, 2024–2026; field research, Copenhagen.

17 Hans Peder Kirkegaard, "Risk of Influence Warfare in the Arctic: Lessons from Greenland," Belfer Center for Science and International Affairs, Harvard Kennedy School, 27 March 2026, belfercenter.org.

18 Kirkegaard (March 2026), citing Center for Cybersikkerhed analysis of the 2019 fake letter.

19 *The Wall Street Journal* reporting on United States intelligence agencies directed to step up intelligence activity in Greenland, May 2025.

20 Danmarks Radio (DR), investigation published 27 August 2025.

21 Field research, Copenhagen. Royal Danish Defence College (Forsvarsakademiet), institutional communications on the defence education programme for Greenlandic leaders, 2025.

22 *Time*, "In Rebuke of Trump, Greenland Declares: 'We Choose Denmark,'" 13 January 2026.

23 field research, Copenhagen; Government of the Faroe Islands public communications; Nordic Council of Ministers analysis.

24 On NATO Arctic Sentinel and the Arctic Endurance exercise: NATO public communications, 2025–2026; Reuters, "Sweden to send fighter jets to patrol around Greenland as part of NATO's Arctic Sentry," 12 February 2026; field research, Copenhagen.

25 Ministry of Resilience and Preparedness (Ministeriet for Samfundssikkerhed og Beredskab), established 29 August 2024, consolidating activities from eight ministries.

26 Straffeloven (Danish Criminal Code), Section 108, retsinformation.dk.

27 field research, Copenhagen; coverage in Danish factchecked media including Tjekdet.dk and *Mandag Morgen*.

28 Field research, Copenhagen.

29 Nordic Council of Ministers, *The Nordic Region 2026: Strong ties in changing times. Denmark and the Faroe Islands' Presidency of the Nordic Council of Ministers 2026*, norden.org, November 2025.

30 Signe Prip Bruun, Michael Zilmer-Johns, and Hüseyin Yücel, *Dansk sikkerhed og forsvar efter Trump: En opdatering af den sikkerhedspolitiske analysegruppes rapport: "Dansk sikkerhed og forsvar frem mod 2035"* (Danish Security and Defence After Trump), Det Udenrigspolitiske Selskab (Danish Foreign Policy Society) in cooperation with Forsvarsakademiet (Royal Danish Defence College), 18 February 2026, udenrigspolitik.dk.

31 Government of Canada, "Canada and the Kingdom of Denmark, together with Greenland, reach historic agreement on long-standing boundary disputes," Global Affairs Canada news release, 14 June 2022, canada.ca.

33 *World Happiness Report 2026*, John F. Helliwell, Richard Layard, Jeffrey D. Sachs, Jan-Emmanuel De Neve, Lara B. Aknin, and Shun Wang, eds. (Sustainable Development Solutions Network and Wellbeing Research Centre, University of Oxford, 19 March 2026), worldhappiness.report;.

34 Elsewhere in this report, we compare the Nordic-cluster in cross-case terms, identifying which elements of the Danish foundation-layer architecture are shared across the Nordic countries and which are particularly distinctive to Denmark.

Chapter 23: Estonia

Estonia borders Russia. Approximately a quarter of its population is Russian-speaking. It experienced the Alliance's first major cyberattack in 2007. By every conventional measure it should be one of the most cognitively vulnerable democracies in the Alliance. Instead it is one of the most resilient. Having regained independence from the USSR, Estonia operated under tight constraints and made its core security decisions out of necessity first, and only later as a matter of principle. It was a country with nothing to lose, and it made its foundational security bet from that position. Estonia bet everything on digital government before anyone else, made citizens the owners of that government's information, and spent thirty years building institutions that earn the trust the bet required. What this chapter asks is which elements of the Estonian architecture are political choices any democracy can make, and which rest on conditions that took thirty years to produce.

Security culture and the bet at restored independence

Estonia's security bet was constitutional before it was technical. Estonia in 1991 had no functioning bureaucracy it could trust, no inherited defence architecture that had ever belonged to Estonia rather than to an occupying power, and no fiscal capacity to build the kind of analogue state that wealthier democracies already ran. The choice to digitalise the state was forced by those conditions and made from necessity. What gave the choice its character was a parallel political decision that citizens would be the owners of their own information (a model shaped by Nordic practice), not the subject of a state that managed information on the citizen's behalf. That principle shaped what was created: a state architecture in which citizens can see what the state holds on them, can see who has accessed it, and can be confident that no central database exists through which the whole system could be compromised in a single breach.[1]

The Estonian doctrinal container for this work is *Lai Riigikaitse*, the whole-of-society defence concept coordinated from the Prime Minister's Office and continuously revised since the early 1990s.[2] It is Estonia's equivalent of Swedish *totalförsvar* and Finnish comprehensive security, and the Annex glossary carries the comparative treatment. Estonia does not use the term cognitive warfare institutionally, but the substance of

cognitive defence sits inside Lai Riigikaitse, which treats national defence as a living, continuously revised, whole-of-society responsibility rather than a function the state performs on behalf of a passive population.

Threat environment

Estonia names its adversaries publicly every year. The Estonian Foreign Intelligence Service publishes *International Security and Estonia* as an annual unclassified threat assessment, continuous since 2018, naming adversaries and treating the population as a partner rather than a recipient.[4] Russia is the dominant and categorically different threat. Its strategic objective is not to advance a specific narrative but to break down: fracture social cohesion, erode trust, prevent collective decision-making. The Estonia-specific vectors are consistent with the broader Russian toolkit described there, with particular intensity around Russian-language information operations, memory politics (notably the 2007 removal of the Bronze Soldier, a Soviet soldier monument, from central Tallinn), persistent GPS jamming, and amplification of right-wing populist narratives that find traction among Estonian ethnic communities rather than Russian speakers. The Forest Brothers framing (Baltic partisans who fought Soviet occupation into the 1950s, cast in Russian narratives as Nazi collaborators), used without differentiation across all three Baltic states to support rehabilitation-of-Nazism narratives, is the primary historical narrative tool Russia deploys. Since the full-scale invasion of Ukraine in 2022, the operational tempo of Russian influence operations against Estonia specifically has reduced, with resources reallocated to Ukraine directly and to higher-priority Western targets.[5] The structural threat has not diminished. China is present but not comparable: first espionage convictions have occurred, with the focus on economic surveillance and infrastructure targeting.

Estonia’s approach to its Russian-speaking minority, approximately twenty-five percent of the population, has historically been permissive in ways that notably distinguish it from Latvia. Russian speakers could use Russian in education, commerce, and civic life. Russian passports were tolerated without administrative pressure to renounce them or convert them into Estonian citizenship itself. The assumption was that integration would come through time, opportunity, and demonstrated prosperity rather than

coercion. Field research suggests roughly twenty to twenty-five percent of the broader Russian-speaking population remain openly or latently hostile to the Estonian state. The majority have moved against Russian narratives since February 2022. The vulnerability is structural rather than individual: language divides can be exploited by coordinated influence operations that aim to deepen mistrust and create parallel realities within the same country, which is why the response runs through inclusive communication, media diversity, and integration policy rather than through suspicion of citizens. The forceful integration push since 2022, including full transition to Estonian-language schooling in Russian-speaking-majority regions, has produced consolidation and backlash alongside integration, and Estonia is now actively re-imagining an approach that held for thirty years.[6] The Narva case below is what that re-imagining looks like when it meets a current Russian operation.

The 2007 Bronze Soldier cyberattack is the hinge that preceded Estonia's mature cognitive defence doctrine rather than a demonstration of it. The lesson Estonia drew was that anything could be weaponised, and the post-2007 response produced the national cyber coordination architecture, the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, and a leading public attribution as doctrine.[7] Three subsequent cases show the mature architecture at work.

The 2017 vulnerability in the Estonian electronic identity card (EID) is the trust-earning case. A cryptographic flaw was discovered in the chip architecture of approximately one third of active Estonian ID cards. Nothing had been breached and the vulnerability would have remained invisible to citizens unless the government disclosed it. The Prime Minister went public immediately. The government suspended certificates, issued replacements, and explained the cryptographic mechanism in plain language through a coordinated national communications effort in which eighty communications professionals showed up unpaid to help. The disclosure cost the government short-term reputational damage and cost nothing in actual breach because no breach had occurred. What it produced was the specific kind of trust that arrives when citizens discover their government chose to tell them about a problem rather than manage around it. Twenty years of that pattern is why Estonia ranks first on the OECD's

measure of citizen trust in digital government services.[8] Estonia is also among the few Western democracies fully employing electronic voting.[14]

The Orthodox Church impasse is the current live failure case, and it shows what happens when the architecture creates a ready-made narrative for the adversary. The government attempted legislation to administratively sever the Estonian Orthodox Church from the Moscow Patriarchate. The move was canonically impossible from the outset: an administrative state cannot sever the ecclesiastical jurisdiction of a religious community, only the community itself can do so through its own procedures. The President of Estonia has rejected the legislation three times on democratic and constitutional grounds, and the matter is now before the Supreme Court. Russia has converted the government's attempt into a ready-made narrative about religious freedom suppression, deployed from the Vatican to the United Nations. The case is simultaneously a failure and a demonstration of the architecture's self-correction: the President's public rejection is the transparency doctrine working even against the government of the day, and the trust-citizens principle applies to the government too.[9]

The Narva People's Republic campaign in March 2026 is the current live operational test. Propastop, Estonia's government-funded but operationally independent civil society counter-disinformation platform working in Russian-language social media, documented a coordinated campaign across Telegram, VKontakte, and TikTok promoting a separatist concept branded as the Narva People's Republic. The operation used the 2014 Donetsk and Luhansk People's Republics template: flag, coat of arms, military insignia, anthem, and explicit territorial framing covering Narva and Ida-Virumaa County. The Estonian Internal Security Service characterised it as a simple and low-cost information attack aimed at undermining social unity, and the Estonian Foreign Intelligence Service doubted direct Russian state involvement. Estonian intelligence did not anticipate an imminent military attack, and the architecture was structured to say so rather than inflate the threat.[10] The script is not new. Local councils in Narva and Sillamäe attempted an unlawful autonomy referendum in 1993, declared unconstitutional by the Estonian Supreme Court, and pro-Kremlin activists circulated a similar autonomy questionnaire after the 2008 Russian invasion of Georgia. Behind the

script lies a longer pattern: Narva has changed hands between imperial powers at least nine times since the sixteenth century, moving between Muscovy, Sweden, Russia, independent Estonia, the Soviet Union, Nazi Germany, and the Soviet Union again before being restored to Estonian sovereignty in 1991. Estonians take foreign visitors to Narva for a reason. Ivangorod Fortress sits visible across the river on the Russian bank, within metres of the Estonian shore of the Narva River. The border is not abstract. Narva lives in the Estonian psyche as the place where the country's fragility and its recovery are always simultaneously visible.[11] The amplification paradox, named by former Estonian Undersecretary for Defence Meelis Oidsalu, is the architecture's honest limitation: once Propastop named the operation, the primary channel grew from roughly seventy subscribers to more than eight hundred within days, and Russian state media recoded the Estonian response as the new story. Detection is not the error. Detection paired with a calibrated response doctrine, what gets named, at what threshold, in what framing, to what end, is the next generation of the architecture Estonia must now develop.[12]

What Estonia has built

Estonia's cognitive defence architecture rests on three pillars that function as a single system expressed in three domains. Taken separately, each is partially replicable. Taken together, they are the reason the country is the benchmark it is.[13]

The first pillar is digital governance as democratic trust infrastructure. The e-Estonia architecture is not a technology platform. It is the mechanism through which government and citizens relate to each other, and the foundational principle is that citizens are the owners of their information. E-elections have run since 2005, and the digital identity (e-ID) that authenticates citizens for online state and private-sector services since approximately 2002. X-Road, a secure data-exchange layer, enables interoperability across public and private services without a centralised database: every institution owns its own data, the exchange layer is the secure connective tissue, and if one node is breached the others remain protected. The architecture scaled because government, banks, and telecommunications providers built it together. The state made the e-ID free and mandatory, the private sector adopted the same identity for banking and services,

and most Estonian digital signatures today are issued through private-sector banking transactions.[14] The result is a state architecture in which trust in digital services sits at the top of the OECD ranking while trust in political institutions and mainstream media is comparatively low.[3] Estonians trust the services because the services perform. Performance builds trust. Messaging alone does not.

The second pillar is coordination from the centre of government. Responsibility for security policy sits with the Government Office, meaning the Prime Minister's Office, not the Ministry of Defence or the Ministry of Interior. That placement gives coordination political authority rather than bureaucratic authority, and it is the same design logic that enabled the digital governance build in the 1990s. Six years before this research, civil emergency planning and national defence planning were merged under the same roof. A unified legal framework (Bill 668 SE, the Civil Crisis and National Defence Act) consolidating the Emergency Act, the State of Emergency Act, and the National Defence Act passed first reading in September 2025, with entry into force planned for 1 July 2026.[15] The Government Security Committee is mandated by the Security Authorities Act and meets every two weeks: composition and coordinating function are set in statute, with the Prime Minister as chair and the ministers of defence, foreign affairs, interior, finance, justice, economic affairs, and entrepreneurship as statutory members, joined by the Chief of Defence and the heads of the security authorities. The Legal Chancellor attends under the constitutional right to participate in government sessions, and the State Auditor by established practice.[21] That is how the tension between security imperatives and democratic values is managed continuously rather than adjudicated after crisis. The fortnightly format is the structural answer to a tendency a well-placed source identified with precision: security agencies under operational stress default to action before authorisation, as Estonia has seen in two domestic cases corrected through public debate: an automated police camera programme that prompted debate over surveillance scope, and money-laundering detection automation that prompted parallel debate over due process. Even during table-top crisis management exercises such as NATO's Crisis Management Exercise (CMX), Estonia stands out to other participants: the actual Prime Minister, ministers, and heads of security agencies take part directly. This contrasts with the more common

practice across many EU and NATO member states, where senior officials simulate or stand in for political leaders. The hands-on involvement strengthens decision-making under pressure, improves coordination at the highest level, and ensures that those who would lead in a real crisis are already familiar with its dynamics and constraints. Estonia approaches crisis preparedness with a level of realism and political engagement that is difficult to replicate through delegated participation.[21]

The third pillar is transparency as strategic doctrine. Estonia attributes publicly, prosecutes publicly, and communicates crises publicly. Counter-intelligence trials have been held in open court for over twenty years. The 2017 EID cryptographic crisis was handled openly. The annual Estonian Foreign Intelligence Service (EFIS) threat assessment identifies adversaries and operations by name. The architecture is deliberately structured to prevent the government from becoming an arbiter of truth: strategic communication coordinates, but independent institutions and civil society organisations adjudicate specific claims. That design choice is what makes Propastop possible as a credible counter-disinformation voice rather than a state propaganda organ. Estonia's 2014 use of existing EU sanctions to close the Sputnik office, without a broadcast ban or content-based decision, is a specific expression of the doctrine that this report's recommendations chapters return to as a transferable legal template. The broader principle is what a source described as the so-called start-up principle: Estonia digitalised quickly in part because, in the early period, it did not think carefully enough about risks because it did not have the luxury to do so, while Western countries often think so carefully they never act. Imperfect architecture that works is worth more than perfect architecture never built. The three pillars integrate because they have to. Digital governance produces trust, central coordination enables coherent response, transparency sustains trust when things go wrong. Remove any one and the other two degrade.[16]

Where Estonia is still exposed

The central exposure is the schizophrenia problem. After the full-scale invasion of Ukraine in 2022, Estonian officials used very strong public language describing Russia as an existential threat, primarily to communicate urgency to Western partners who had

not yet absorbed what Estonia had been saying for years. That messaging has rebounded domestically. A March 2025 representative survey by the public-opinion agency Turu-uuringute found seventy-seven percent of Estonian residents felt anxiety about possible war, with twenty-eight percent reporting anxiety to a large or very large degree, with the highest levels among fifteen-to-twenty-nine-year-olds. The State Chancellery engaged technology journalist Henrik Roonemaa to reduce fear-of-war effects, an institutional acknowledgement that the domestic communication problem is now a policy issue. Roonemaa was later appointed Deputy Director of the Government Communications Bureau. The strong language worked on Western audiences. It also reached Estonian audiences who were not the primary target of the messaging, and the architecture of trust does not automatically solve the problem of messaging calibration across audiences with different stakes in the same war.[17]

The shelter gap worsens the schizophrenia problem. Finland has roughly eighty percent population shelter coverage from Cold War infrastructure; Estonia is building from scratch because Soviet architecture included very limited shelters for the Estonian population; the programme accelerated after 2022, and September 2025 legislation sets a 1 July 2026 deadline for non-public shelter construction. Current investments, including the Code of Conduct for Crisis Situations booklet, shelter network revision and marking, the April 2024 Reservists' Week, and the decision to widen the personnel base of the Defence League (Kaitseliit, roughly 26,000 volunteers) are catching up but cannot compress decades of infrastructure into a parliamentary cycle. The absence is cognitively consequential because the gap between fear-of-war messaging and the physical capacity to shelter citizens if war came is visible to anyone who looks. Messaging without infrastructure corrodes the trust that messaging is trying to mobilise.[18]

Two additional exposures are specific to the cognitive architecture. The digital infrastructure is aging in a domain-specific way: it was built to prove you are you, and the emerging risk is preventing someone else from becoming you. Identity-assurance logic from the early 2000s is not identity-assurance logic for the generative AI era, and the architecture will require re-foundation rather than incremental update to remain load-

bearing for another decade. The military cognitive defence capability beyond the roughly two-hundred-strong psychological warfare reserve unit remains underdeveloped. Estonia has built the civilian architecture extensively. The integration of civilian and military cognitive capability under Lai Riigikaitse is a near-term institutional priority rather than an achieved condition.[19]

What travels

Two elements of the Estonian architecture travel to other democracies. Each carries a condition for adoption.

The first is the citizen-as-owner principle as a constitutional-level political decision rather than as an administrative-level technical choice. A democracy can make this decision at any moment, but the condition is that it requires commitment at the level of founding law, constitutional revision, or equivalent legislated restructure at a moment of institutional origin or reconstruction. A retrofitted adoption, grafting citizen-as-owner onto an existing architecture built on the opposite assumption, will fail to produce the trust Estonia produced because the principle's work is upstream of the technical layer that implements it.

The second is transparency as strategic posture. The condition is that the state must be willing to accept the reputational and operational costs of public attribution, public crisis communication, and public error. Most democracies default toward communications inhibition under pressure, particularly from security services that prefer operational concealment. The transferable lesson is that the default costs more than the discipline: every act of inhibition that later becomes public erodes the trust the inhibition was meant to protect, while prompt honest calibrated disclosure compounds trust over decades. The digital architecture itself is not transferable; the political decision that produced it is what travels, and that decision is the first element above.

Partner landscape

Finland is Estonia's primary model and closest reference point on doctrine and shared values. Finnish comprehensive security, particularly the approach to psychological

defence born of the Winter War, is the benchmark Estonian officials cite when asked what adequate looks like. The bilateral working relationship on cognitive defence is dense and operationally continuous rather than ceremonial.

Latvia and Lithuania are Estonia's closest operational peers. The three Baltic states share the same adversary profile, and Russia's state media does not meaningfully differentiate between them. The Forest Brothers and Nazi-rehabilitation narratives are deployed against all three without tailoring. The Baltic peer relationship produces shared threat assessment, coordinated public attribution, and joint response to cross-cutting narratives, and its operational depth exceeds most of the bilateral relationships within the broader NB8.

The United Kingdom, Germany, France, and Poland are the broader operational partners across signals, cyber, countering foreign information manipulation, and military cooperation. The UK is the framework nation for NATO's Forward Land Forces battlegroup in Estonia and leads the Joint Expeditionary Force in which Estonia participates. The bilateral cognitive defence relationship is the deepest Estonia maintains outside the Baltic peer set, with continuous practitioner exchange on hybrid threats and strategic communication. The UK, Germany, and France are treated as non-negotiable for European security. Germany's forward-stationed brigade in Lithuania matters more for the Baltic cognitive landscape than any other Allied posture because it is visibly permanent. Troops have brought their families. The deployment is not a rotational presence that can be quietly wound down but a structural commitment any Estonian or Russian observer can see and count on. In cognitive terms, what is visible and durable deters more than what is announced and temporary.

Estonia's own institutional contributions to the partner architecture are three. The Tallinn Mechanism, Estonia-initiated and currently chaired by the United Kingdom with approximately fourteen members, coordinates civilian cyber support to Ukraine. The IT Coalition within the Ramstein framework, co-chaired by Luxembourg and Estonia with approximately twenty members, coordinates military cyber support to Ukraine. The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn is the Alliance-level centre of gravity for cyber defence research and exercises.[20]

The Nordic-Baltic 8 is valuable as a trust-building forum but is not a delivery mechanism. Mistaking it for one produces overconfidence in Allied coordination depth that operational practice does not support.

The United States was the structural backbone of Estonia's NATO deterrence architecture for three decades. In the current period, Estonia is planning operationally for cognitive defence cooperation without assuming American participation, and Estonian officials have been more willing than their Latvian or Lithuanian counterparts to state this in public: Foreign Minister Margus Tsahkna said in early 2025 that Europe must be prepared to replace American support for Ukraine if it is withdrawn. What matters for the partnership landscape is that the partnerships on which Estonian cognitive defence actually runs now sit within Europe and with the United Kingdom.

Endnotes

1 Republic of Estonia Information System Authority (RIA), *Cyber Security in Estonia 2025*, at ria.ee.

2 Regarding *Lai Riigikaitse* as Estonia's whole-of-society defence concept: the framework is coordinated from the Government Office (Riigikantselei) under the Prime Minister, and the comparative treatment alongside Swedish *totalförsvar* and Finnish comprehensive security is developed in the Annex glossary.

3 Organisation for Economic Co-operation and Development, *Trust Survey* and *Digital Government Index*, most recent editions available at oecd.org.

4 Estonian Foreign Intelligence Service (Välisluureamet), *International Security and Estonia* 2026, annual unclassified threat assessment, Tallinn, 2026, available at valisluureamet.ee.

5 Field research, Tallinn; & EU DisinfoLab, *Disinformation Landscape in Estonia*, January 2025, available at disinfo.eu.

6 Dmitri Teperik, "Total Defence as a Mindset: Cognitive Resilience and Democratic Security in Estonia and the Baltic Region," International Centre for Defence and Security, Tallinn, 2023, available at icds.ee.

7 NATO Cooperative Cyber Defence Centre of Excellence at ccdcoe.org, institutional history and founding documentation; Estonian Information System Authority (RIA), institutional history at ria.ee.

8 Arnis Parsovs, "Estonian Electronic Identity Card and its Security Challenges" (PhD dissertation, University of Tartu, 2021), thesis documentation at utlib.ut.ee.

9 Estonian Presidential Office public record, 2024-2026 sequence, at president.ee. & Russian Ministry of Foreign Affairs public communications and Russian Orthodox Church Moscow Patriarchate statements across 2024-2026.

10 Meduza, "Anonymous social media accounts are calling for the secession of an Estonian county on Russia's border," 23 March 2026, at meduza.io; & Atlantic Council, "Could Russia use fake separatists to destabilize Estonia and discredit NATO?", Ukraine Alert, March 2026, at atlanticcouncil.org; Politico Europe.

11 Field research, Tallinn and Narva.

12 Meelis Oidsalu, "A New Russian Game on the Borders of the Baltics," Center for European Policy Analysis (CEPA) Europe's Edge, 19 March 2026, at cepa.org.

13 Illimar Ploom, Zdzislaw Sliwa, and Michelle Haas, "Lessons Identified from Ukraine: The Bid for the Estonian Total Defence Concept," *Journal on Baltic Security* 11, no. 1 (2025), pp. 58-87, Baltic Defence College, peer-reviewed open access.

14 Estonian Information System Authority (RIA), institutional documentation at ria.ee; e-estonia.com government portal.

15 Estonian Ministry of Defence, defence planning institutional structure at kaitseministeerium.ee. & Government Office documentation on the work of the Security Committee at riigikantselei.ee.

16 Field research, Tallinn. & propastop.ee institutional documentation. The startup-principle framing, that imperfect architecture that works is worth more than perfect architecture never built, is an off-the-record structural observation from field research.

17 Turu-uuringute AS, "Eesti elanikest 77% tunneb seoses võimaliku sõjaohuga ärevust," 21 March 2025, at turu-uuringute.eu.

18 Estonian Ministry of the Interior documentation at siseministeerium.ee; comparative Finnish shelter architecture at intermin.fi. & the Code of Conduct for Crisis Situations booklet, and other related documents at the Estonian Defence League - kaitseliit.ee.

19 Field research, Tallinn & Estonian Defence Forces institutional documentation at mil.ee.

20 Estonian Ministry of Foreign Affairs, "Tallinn Mechanism" institutional documentation at vm.ee; & Estonian Ministry of Defence, "IT Coalition" institutional documentation at kaitseministeerium.ee.

21 Security Authorities Act (Julgeolekuasutuste seadus), Riigi Teataja consolidated text at riigiteataja.ee/en/eli/503062020002/consolide; & Government Office documentation of the Security Committee's work at riigikantselei.ee.

Chapter 24: Latvia

Latvia sits on the Baltic Sea coast between Estonia to the north and Lithuania to the south, and borders Russia and Belarus to the east. Approximately 23 percent of its population is ethnic Russian and approximately 35 percent speak Russian as the language used at home, the demographic legacy of a four-decade Soviet colonisation operation that brought approximately one million civilian settlers to Latvia between 1944 and 1988, predominantly Russian-speaking but drawn from across the Soviet Union. Estonia and Lithuania, to a lesser extent, experienced the same demographic operation. Latvia today has the largest absolute Russian-speaking population among the three Baltic states. Approximately 180,000 people, just under nine percent of the population, hold non-citizen passports, a legal category Latvia adopted at independence and shares only with Estonia. Russian is understood by more than ninety percent of the adult population.[1] Geography, demography, and the linguistic environment together make Latvia one of the most operationally exposed cognitive defence cases in the Alliance. The Russian-speaking community has been one of Russia's principal cognitive targets since Latvia regained independence, although its viability as a target has narrowed since the 2022 full-scale invasion of Ukraine. The larger and increasingly more important attack surface is the gap: the parallel Russian-language information environment that was allowed to persist into the post-independence period, the policy gaps the permissive 1990s integration approach left open, and the network of local intermediaries Russia has built across three decades to work through the community and into the Latvian-language information environment. Latvia is now closing the 1990s integration gaps and building the cognitive defence architecture the contemporary threat picture requires, doing both simultaneously and under live operational pressure.

Security culture and the Latvian approach to defence

Latvia's security culture is built around its demographic inheritance and the cognitive operation that produced it. Before the Second World War, Latvians were approximately 77 percent of the population. By the late Soviet period the share had fallen to roughly 52 percent. The shift was not a demographic accident. The Latvian Occupation Museum names the 1944 to 1988 period under three terms together, Sovietisation, Russification,

and colonisation, characterising the demographic project as a cognitive instrument designed to dilute the Latvian cultural environment and erode collective memory. Two large Soviet deportations of native Latvians, 15,443 people in June 1941 and 42,125 in March 1949, are the two best-known of the multiple Soviet deportations that removed roughly three percent of the population. The result is a multi-ethnic society Latvia is now working to integrate through democratic policy rather than through the coercive instruments that produced its current composition.[2]

Latvia regained independence in 1991 with its Soviet-era demographic composition unchanged. The 1990s integration approach was gentle, premised on the assumption that time, opportunity, and EU and NATO accession would eventually resolve what coercion could not. The judgement of practitioners across institutions today is that the gentle approach was the foundational design error. It left citizenship policy gaps, sustained parallel school systems, and preserved a separate Russian-language information environment that the Russian Federation cultivated as a strategic asset. The 2014 Russian annexation of Crimea forced constitutional and legal change. The 2022 full-scale invasion of Ukraine forced the integration and institutional rebuild Latvia is now executing. Latvia's National Defence Concept has named the information space as a domain of national defence since 2016; the operative terminology is influence operations countered by strategic communications, and the State Security Concept names societal trust in government and the military as the paramount cognitive defence objective.[3]

The threat environment

The most analytically important correction the chapter can offer is that the Russian-speaking community is not, and has never been, a hostile bloc Russia can activate, contrary to the framing Russian narrative operations have promoted since Latvia regained independence and contrary to Russia's consistent attempts to instrumentalise Russian-speaking communities as political and informational leverage. Māris Andžāns, Director of the Centre for Geopolitical Studies Riga and Associate Professor at Riga Stradiņš University, has characterised the community in approximate thirds: one third loyal to Latvia, one third opposed, and one third politically abstinent and not mobilised

by either pole. The genuinely pro-Russia segment that would respond if Russia attempted to activate it is approximately ten percent of the Russian-speaking population, not the population as a whole. The Russian narrative depends on collapsing this internal differentiation into a monolithic frame, and the polling trajectory since 2022 has actively narrowed the community's viability as a Russian target: SKDS / Riga Stradiņš University surveys show the share of Russian-speaking respondents blaming Russia for the war in Ukraine rising from 32 percent in 2022 to 38 percent in 2024, with the abstinent share dropping from 33 percent to 22 percent. The ethnic Russian share of the population has declined from 34 percent in 1989 to 24.1 percent in 2025.[4]

Russian operations against Latvia have evolved beyond the persuasion-of-a-target-community model that defined the 1990s and 2000s. The majority of Russian narrative operations today target not only the Russian-speaking community but also the Latvian-language audience, disseminated through local Latvian-language intermediaries, social media influencers, politicians, and right-wing populists rather than Russian state broadcasts, which since the National Electronic Mass Media Council's (NEPLP) 2022 channel bans are no longer accessible in Latvia. The shift matters because Latvians have always been broadly bilingual, with approximately 91 percent of adults understanding Russian to some degree, meaning Russian-language content was never effectively quarantined from the Latvian-language information environment. The operational mechanism is frame rather than fact. Russia does not need to assert false propositions; it produces multiple partial-true versions of the same event, none completely true, none entirely false, and lets the resulting confusion both fragment public understanding and sustain consumption of adversary content. The pattern is documented in the academic literature as the "firehose of falsehood" model. Debunking addresses fact but not frame, and Latvian researchers and audiences alike report fatigue with the debunking format.[5]

Three cases illustrate the pattern: a sustained narrative campaign laundered through Western media (the 2023 to 2024 deportation case), an institutional communications failure that produced doctrinal learning (the October 2024 drone), and the live operating environment at submission (the spring 2026 drone incidents). The first is the 2023 to

2024 deportation case. In August 2023 the Latvian Ministry of Interior notified approximately 6,000 Russian citizens, the residual subset who had neither passed the Latvian-language A2 examination nor renewed a temporary residence permit, that they were required to leave or regularise their status. By mid-2024 the public record was unambiguous: more than 4,500 had sat the language exam or renewed permits, over 600 had departed voluntarily, and fewer than ten had faced forcible removal. The Russian narrative was ethnic cleansing and mass expulsion of Russians, and it found echoes in coverage by established Western outlets, including the BBC, in early 2026. Prime Minister Evika Siliņa characterised the broader pattern: “Russian propaganda always chooses how to twist Latvian news in its own way.” Latvian and Baltic counter-propaganda analysts, including the Estonian Propastop and the EU DisinfoLab, have documented the structural mechanism: when Russian narrative operations frame a Latvian policy as a human rights violation, that framing can be picked up by Western outlets reporting in good faith on the human rights dimension, producing the appearance of independent corroboration. The chapter does not suggest that the BBC or any other outlet acted with anything other than good faith; the cognitive defence challenge is that good-faith Western journalism often operates inside a frame that adversary information operations have actively cultivated for thirty years.[6]

The second case is the October 2024 drone that crashed in Latvia. Before the Latvian government communicated officially, which took several hours, competing interpretations were already circulating: Ukrainian or Russian, deliberate or accidental, who bore responsibility? Russian-language sources moved first, framing the incident as evidence of NATO recklessness in supporting Ukraine; Latvian-language social media split into multiple incompatible accounts before the official Latvian narrative was established. The communications failure was the lesson-learned moment, and the Latvian Ministry of Defence redesigned its incident-response strategic communications system after it. The pattern of drone-related incidents would recur, culminating in the May 2026 Rēzekne strike that triggered the government crisis examined in honest limitations. The third case is the live operating environment in spring 2026. Between 23 and 25 March, Ukrainian drones jammed by Russian electronic warfare crashed into Latvia, Lithuania, and Estonia while transiting to strike Russian Baltic coast

infrastructure. On 27 March 2026 the Latvian Ministry of Defence publicly named the Russian framing, that the Baltic states were complicit in Ukrainian strikes against Russia, as a large-scale coordinated information operation aimed at discrediting NATO, dividing society, reducing trust in state institutions, and weakening support for Ukraine, with social media bots targeting Russian-speaking and youth audiences. Case 1 shows the laundering chain running through Western media; Case 3 shows the same frame-not-fact pattern operating at scale through Russian state and proxy channels. Latvia is the proximate target; the Alliance is the strategic one.[7]

What Latvia has built

Latvia's cognitive defence architecture is distributed across military, civilian, and independent actors and operates within Latvia's comprehensive national defence framework, a whole-of-society model that since 2018 has formally treated civil resilience, social cohesion, and information defence as inseparable components of national defence. The Ministry of Defence holds policy authority for the Russian threat; the National Armed Forces (NAF) hold operational lead for incident response, with J10 strategic communications and J9 civil-military cooperation handling analytical and outreach functions. The incident-response system refined after the October 2024 drone failure is built around what Latvian practitioners call the first-informer principle: Latvia must be present in the information environment before adversary framing, not in response to it. The Constitution Protection Bureau (SAB), the State Security Service (VDD), and the Military Intelligence and Security Service (MIDD) handle attribution and counter-intelligence, with MIDD's 2025 first detailed public threat assessment marking a publication innovation.[8]

The civilian architecture sits beside the military one. The Latvian State Chancellery hosts a Strategic Communications Coordination Department and operates the "Black on White" public platform, launched in late 2023, which catalogues current disinformation cases and offers citizens a direct mechanism to report misleading content. The Chancellery is also the contact point between the Latvian state and major technology platforms. NEPLP, Latvia's statutory media regulator, holds the legal authority under Section 13.5 of the Law on Electronic Mass Media to restrict or suspend access to

electronic media services, including television channels, radio broadcasts, and online platforms, where they are deemed to threaten national security, public order, or democratic values; it used that authority to ban approximately eighty Russian media outlets in August 2022 and even opposition Dozhd / TV Rain in December 2022. The Latvian Public Broadcasting service (LSM), the investigative fact-checking platform Re:Check operated by Re:Baltica, the cyber detection authority CERT.LV, and the National Defence Information Centre complete the operational layer.[9]

Two relatively recent legal developments warrant specific attention. In May 2024 the Latvian Saeima (the Latvian parliament) amended the Criminal Law to explicitly criminalise the deployment of AI-manipulated audio, video, or imagery to mislead voters, with penalties of up to five years imprisonment, or a fine, alongside criminal liability for deploying automated systems to obstruct voting. The amendment placed Latvia ahead of most NATO Allies on AI-enabled electoral interference. In 2025 the VDD prosecuted a pro-Kremlin activist for statements made in a public discussion in Moscow that the Service assessed as targeting Latvian security. Together with the existing restrictions on Russian-language broadcast and the channel-ban architecture, these developments constitute one of the most legally developed active-defence regimes among NATO Allies.[10]

Latvia hosts the NATO Strategic Communications Centre of Excellence (StratCom COE) in Riga. Founded in 2014, the COE is the Alliance's primary institution for strategic communications research, terminology development, and partner-country support. It contributes to ongoing NATO doctrine development on cognitive warfare, conducts the annual Riga StratCom Dialogue, and produced the 2025 study on Nordic-Baltic countering information influence operations that this report draws on across the cluster chapters. The chapter's honest observation is that the COE's Alliance-level institutional contribution exceeds its direct operational delivery into Latvian domestic cognitive defence: hosting the institution is itself a form of national contribution that the chapter does not minimise, but the operational value to Latvian cognitive defence specifically is more limited than the international profile suggests.[11]

Latvia's cognitive defence architecture is one piece of the work; the other is the substance of minority integration, the school reform, efforts to address regional development disparities that partly contribute to ethnic divisions, the renewed conscription, and the State Language Centre's role, that closes the policy gaps the 1990s approach left open and that Russia has cultivated. These are not strictly cognitive defence instruments, but they are the substance that makes cognitive defence possible. The 2025 school reform transitioned publicly funded primary and secondary education to Latvian-language instruction, ending the parallel Russian-language school system that the Soviet occupation had imposed and that thirty years of permissive policy had preserved. It is the reversal of a deliberate Soviet-era engineering project that produced the separate Russian-language information environment Russia subsequently cultivated. The reform will take a generation to deliver, and that timescale is the point: the gap Russia has worked through is generational, and closing it is generational. The conscription system, reintroduced after years of delay and currently in its third year, performs a parallel function. Russian-speaking representation in conscript intakes is approximately five percent, generally in line with their underrepresentation in the National Armed Forces. The cognitive defence logic operates indirectly: shared service produces interpersonal contact between Latvian-speaking and Russian-speaking young men under common discipline, and the experience travels back into families and communities through word-of-mouth from returning conscripts. The mechanism is slow and partial, but it is one of the few formal contact points between the two language communities at population scale. The 2026 defence budget of 4.91 percent of GDP, the largest in Latvia's history, funds the supporting infrastructure for the long horizon, including a new military secondary school opening in the town of Malta in eastern Latvia's Latgale region, placing a new military educational institution in the region of greatest cognitive vulnerability.[12]

Honest limitations

Latvia's strategic communications is reactive, not proactive. The four-year political cycle is the structural driver. The information domain work explains decisions after they are taken rather than building forward strategic narratives, and senior Latvian defence practitioners name this as the principal institutional gap. The Military Intelligence and

Security Service's first detailed public threat assessment appeared only in 2025, years after comparable Estonian and Lithuanian publications. The intelligence culture has historically prioritised operational security over public threat communication, a pattern Latvian practitioners now describe as a constraint on the kind of transparent threat communication that builds trust and societal resilience over time.[13]

The May 2026 government crisis traced in the threat environment, in which the Rēzekne drone incident triggered the resignations of Defence Minister Andris Sprūds of the Progressives (junior coalition partner) on 10 May, and Prime Minister Evika Siliņa of New Unity (senior coalition partner) on 14 May after the Progressives withdrew support, is what reactivity looks like under live operational pressure. The drone incident was the proximate trigger rather than the sole cause; political fragility on the defence portfolio had been accumulating since the early April 2026 Saeima dismissal motion against Sprūds had narrowly failed at 43 votes to 50. The operational architecture continued to function through the crisis, with detection, attribution, and Ministry of Defence communication chains operating, though Latvian commentators noted that the official response remained slower than the political situation required. The information environment around the incident itself became contested terrain: false claims circulated online attributing the drones to NATO provocation or to a Latvian government cover-up, and the Latvian State Police issued a formal warning that deliberately spreading false harmful information is a criminal offence under Latvian law. The crisis demonstrates that Latvia's cognitive defence story is not only what it costs to build the architecture, but what it costs to operate it under live political conditions.[14]

Three structural exposures sit alongside the reactivity. The first is that Latvia is, in cognitive defence architecture terms, behind its Baltic neighbours. Estonia and Lithuania have invested longer in transparent threat communication, in inter-agency coordination structures, and in proactive narrative capability than Latvia has. Latvia leads the Alliance on the legal deterrence dimension, with the May 2024 Criminal Law deepfake amendment and the channel-ban architecture among the most developed in NATO, but on the institutional architecture side, Latvia is catching up rather than setting pace. This is most visible in the Latgale region: the eastern region with the largest

Russian-speaking concentration and a direct border with both Russia and Belarus has the most acute cognitive threat profile in the country, but Latvia has not built a systematic differentiated programme matching that profile. Targeted military exercises and modest NGO grant funding exist; a programme proportional to the regional vulnerability does not. The second exposure is threat fatigue, which is a live research concern, not a theoretical risk. Latvian researchers are drawing on the Taiwan case, where sustained threat communication eventually produced public disengagement rather than alertness, and are beginning to observe analogous patterns domestically. Years of debunking content have produced format fatigue, and parallel war fatigue from sustained defence spending and the associated welfare-state trade-offs creates the broader vulnerability that domestic populist movements exploit at the same time as adversary operations. The third is that trade with Russia remained meaningful in 2025, with Latvian exports to Russia totalling €962.5 million, sustaining commercial channels through which influence continues to operate in ways the institutional architecture cannot address.[15]

What travels from Latvia

Two elements travel principally, and a third travels conditionally. The first, and the most significant, is the legal architecture for active defence. Latvia's May 2024 deepfake amendment is the kind of provision other democracies can study and adapt, criminalising AI-manipulated electoral content with proportionate penalties and constitutional grounding. The 2025 VDD prosecution demonstrates the architecture in operation. The condition for adoption is that legal architecture for active defence must rest on procedural democratic legitimacy: Latvia moved earlier and harder because lived institutional memory of occupation and acute threat perception generated the political will. The Latvian Constitutional Court (Satversmes tiesa) is currently reviewing the public-service broadcasting regulator's 2024 restrictions on Russian-language programming, a test of whether the active-defence regime survives Latvia's own constitutional scrutiny. The Latvia case demonstrates that the legal tools are constructible within democratic constraints; it does not demonstrate that they are easy.

The second is the principle that the integration gaps cultivated by adversaries are themselves the attack surface, and closing them is therefore a cognitive defence priority rather than a social policy externality. Latvia's lesson is not the specific policy mix, the school reform, regional development, the public-space restrictions, or the channel bans, which are too specific to Latvia's circumstances to travel directly, but the framing. The condition for adoption is the willingness to identify, within other democracies, the structural gaps where adversary access exists, whether linguistic, communal, regional, or institutional, and to treat closing them as a cognitive defence investment in its own right. The third element, the incident-response strategic communications system built around the first-informer principle, travels conditionally. The institutional design is exportable; the political authority required to operationalise it at speed is the variable that needs to come with it. Coordinating machinery can be transplanted; what cannot easily be transplanted is the political will to grant the machinery the authority to act in real time.[16]

Latvia's partner landscape

Latvia organises its external security relationships through three pillars: NATO, bilateral relationships, and the Joint Expeditionary Force (JEF). NATO is the structural backbone, with the Multinational Brigade in Latvia the central operational expression. Bilateral relationships carry the deepest defence cooperation, particularly with the United States, the United Kingdom, Canada, Germany, Sweden, and Denmark, each contributing through different combinations of brigade presence, industrial cooperation, intelligence sharing, and capacity-building. JEF, the UK-led format that includes all NB8 members plus the Netherlands, is a recent and expanding contributor to hybrid threat and disinformation work, and gives Latvia an operational framework outside NATO's formal command architecture. The Nordic-Baltic Eight remains a valuable platform for experience sharing among the eight, even if it is a diplomatic alignment forum rather than an operational coordination structure. Alongside these defence pillars, Latvia coordinates with the European Union on countering disinformation through joint initiatives on strategic communications, cybersecurity, media resilience, and foreign information manipulation and interference (FIMI), participating in work coordinated through the European External Action Service and other EU institutions, and

strengthening cooperation with European partners following Russia's 2022 full-scale invasion of Ukraine.[17]

Two operational realities sit alongside the three pillars. The first is the tightening of Baltic and Polish cooperation since 2022. Estonia, Latvia, and Lithuania coordinate on threat assessment, public attribution, and regional fact-checking through the Baltic Engagement Centre for Combating Information Disorders (BECID), the cross-Baltic consortium that is the largest in the European Digital Media Observatory network. Poland is increasingly an operational partner on the shared Russian threat picture: Foreign Minister Baiba Braže's 20 June 2024 joint statement with Polish Foreign Minister Radosław Sikorski named hybrid threats from Russia, the instrumentalisation of migration, and intensive sabotage as the common threats both countries are managing, with a commitment to information exchange for more rapid response. The second operational reality is Nordic partner contribution, which operates through brigade presence (Sweden and Denmark in the Canadian-led NATO Multinational Brigade) and through JEF and dense bilateral relationships rather than through the NB8 frame.[18]

The Canada-Latvia relationship rests on a foundation older than the current security partnership. From the end of the Second World War through Latvia's restoration of independence in 1991, Canada maintained a de jure non-recognition policy toward the Soviet occupation and annexation of Latvia, alongside the United States, the United Kingdom, the Federal Republic of Germany, France, and others. The current Canadian-led NATO Multinational Brigade (expanded from the original eFP battlegroup) is the latest expression of a relationship that has spanned more than seven decades. The Canadian Armed Forces presence in Latvia has been extended to 2029, confirmed in the Foreign Minister's Annual Report tabled in January 2026 and reiterated by Foreign Minister Braže in her address to the Saeima at the time. The extension prolongs the political answer to the question of Allied durability rather than permanently resolving it: the structural ambiguity of rotational presence is itself a Russian narrative resource Latvia reads as cognitively consequential. Latvia reads physical Allied presence as cognitive reassurance, visible in everyday life: exercises in Daugavpils, Allied troops staying in local hotels rather than military camps, soldiers recognisable on the street,

and what Latvian practitioners describe as the hairdresser test, the moment when ordinary residents tell their neighbours that they have Allied clients at the bar or the salon. The question of whether and how the rotational presence should be converted into permanent infrastructure is the most consequential cognitive defence question in the bilateral relationship. More broadly, Latvia situates its bilateral relationships within the regional context: the United Kingdom leads the NATO Brigade in Estonia, Germany has committed a permanently stationed brigade to Lithuania, and the German Rheinmetall investment in the 155mm ammunition factory at Iecava in southern Latvia is the concrete example of how cooperation moves beyond the military domain. Latvia's hosting of the StratCom COE is the Alliance-level institutional contribution Latvia makes to the cluster.[19]

Latvia is not a benchmark and does not present itself as one. It is the operationally-tested case for what closing integration gaps and building cognitive defence architecture cost when both are undertaken simultaneously and under live pressure; at submission, Latvia is in caretaker government, four months before national elections, with the architecture absorbing operational pressure that the political accountability layer above it has not survived. What Latvia does next, particularly on the integration project the 2025 reforms are designed to complete on a generational timeline, will shape how the architecture continues to operate under conditions Latvia has not previously been asked to navigate.

Endnotes

1 Latvian Central Statistical Bureau, stat.gov.lv.

2 Latvian Occupation Museum panels "*Sovietisation, Russification, Colonisation* 1944 to 1988" and "Erasing National Identity," observed January 2026.

3 Field research, Riga, January 2026.

4 Māris Andžāns, Director, Centre for Geopolitical Studies Riga, field research, Riga, January 2026, attributed by name with permission.

5 Field research, Riga; NEPLP institutional record, neplp.lv; EU DisinfoLab (2025) & Christopher Paul and Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model," RAND Corporation, 2016.

6 EU DisinfoLab (2025), "Emblematic Cases" section (Note 4); Radio Free Europe / Radio Liberty, "Express Your Loyalty," September 2024, rferl.org; & Atlantic Council, "What's the best way to deal with Russian information manipulation? Latvia has answers," 14 May 2025, atlanticcouncil.org.

7 Field research, Riga, January 2026. & Latvian Ministry of Defence, "Russia carries out information operation against Baltics," 27 March 2026, mod.gov.lv.

8 Latvian Ministry of Defence, Comprehensive Defence System policy framework, mod.gov.lv.

9 Latvian State Chancellery, mk.gov.lv.

10 LSM, “Deepfake use to influence elections will be criminalised in Latvia,” 9 May 2024, eng.lsm.lv

11 Feld research, Riga, January 2026.

12 Latvian Ministry of Education and Research, izm.gov.lv; & Latvian Ministry of Defence, White Book on Defence Spending 2026 (Baltā Grāmata), December 2025, mod.gov.lv.

13 Field research, Riga, January 2026. Cross-case comparison with Estonia and Lithuania developed in Chapter 29.

14 Meduza analytical piece by Sergey Potapkin (Latvian Institute of International Affairs), 12 May 2026; & coverage on the 14 May 2026 of the resignation of Prime Minister Siliņa, BBC News, 14 May 2026, news.bbc.co.uk.

15 Latvian Central Statistical Bureau, “Latvian exports were on the up in 2025,” provisional data, 19 February 2026, eng.lsm.lv.

16 Field research, Riga, January 2026; with reference to Latvian Constitutional Court institutional documentation.

17 Field research, Riga, January 2026 & UK Ministry of Defence, gov.uk.

18 Latvian Ministry of Foreign Affairs, “Baiba Braže and Radosław Sikorski: Joint action by Latvia and Poland,” 20 June 2024, mfa.gov.lv. And regarding Nordic 5 contributions through brigade presence: Latvian Foreign Minister’s Annual Report on Foreign Policy and EU Affairs (2025-2026), 13 January 2026, mfa.gov.lv.

19 Foreign Minister’s Annual Report (2025-2026), with field research, Riga, January 2026.

Chapter 25: Lithuania

Lithuania does not use “cognitive warfare” as a formal term, instead working under “hybrid threats,” with disinformation and information operations as practical categories. It also has early experience with combined cyber and information attacks, shaping its integrated approach.

At the same time, Lithuania is one of the clearest examples of a democracy that learned early, adapted under pressure, and then formalised that learning into a working system. Its strength is not technological sophistication or scale. It is disciplined coordination and calibrated response. Lithuania shows that cognitive resilience can be built through ever evolving method: shared assessment, threshold-based action, and whole-of-government and whole-of-society approaches.

The transferable lesson is not a single tool, but the system behind it. It is the decision to treat the information environment as a governed space with rules, thresholds, and institutional ownership.

Opening Argument

Lithuania sits on the alliance’s eastern edge, with direct exposure to Russia and Belarus, a history shaped by Soviet occupation, and a political environment that should make it vulnerable to external manipulation. It experienced the shocks of 2014 not as distant events but as a direct warning. This is a country that should struggle with cognitive resilience, instead, it is one of the most systematically organised.

How did Lithuania turn early exposure into structured advantage, and which elements of that system can be reproduced elsewhere? The answer is not a single reform or moment. It is the gradual construction of a coordination model that treats information threats as continuous, measurable, and governable.

This model has developed in parallel with deeper integration into EU and NATO structures, which provide both the external framework for deterrence and the regulatory and financial backbone for resilience.

Threat Actors and Methods

Lithuania sees threats as persistent, not episodic. Its official threat picture combines disinformation, cyberattacks, sabotage, coercive pressure on critical infrastructure, election interference, and border pressure. Russia is the dominant actor, with Belarus operating alongside it in closely aligned ways, including through instrumentalised migration, border provocations and, recently, air balloons.

From a military perspective there is no meaningful difference between Russian and Belarusian armed forces.

Russia's objective is not persuasion toward a single narrative but erosion of coherence. Lithuanian assessments consistently describe efforts to spread fear, disrupt institutions, weaken support for Ukraine, and erode trust in democratic systems. Increasingly, these activities combine information operations with cyber activity, electronic interference, and physical sabotage.

Critical infrastructure is a central vulnerability. Energy systems, transport links, and communications networks are frequent targets of hybrid pressure. Lithuania's long effort to reduce dependence on Russian energy reflects this understanding: strategic dependence was itself a vector of influence.

A major structural shift came with the Baltic states' synchronisation to the Continental European electricity grid in 2025, ending reliance on the Russia–Belarus system. This EU-supported project removed a long-standing hybrid vulnerability.

Russia accounts for approximately 80 percent of the operational threat. Belarus approximately 18 percent. China approximately 2 percent.

This operational allocation reflects the formal threat picture established in Lithuania's 2021 National Security Strategy (Resolution XIV-795), which identifies Russia, Belarus, and China as the primary hostile state actors and calls for the development of state capacities to monitor, assess, and respond to information threats in coordination with NATO and the EU. Lithuania's institutional architecture is the operational expression of that strategic doctrine.

China indeed is a secondary but relevant actor, particularly in cyber espionage, economic pressure, and influence attempts in strategic sectors. Its operations are less effective and increasingly routed through Russian information ecosystems. China also attempted infrastructure investment in Lithuanian critical infrastructure including the Klaipeda seaport and 5G networks. These were blocked.

The pattern of Russian activity is consistent: it amplifies existing tensions rather than creating them. Examples include:

- Opposition to energy transitions;
- Resistance to foreign investment projects;
- Anti-NATO narratives;
- Environmental protests near strategic military areas.

The mechanism is stable. A real issue emerges, external actors scale it, and narratives are layered onto it.

A concrete illustration came during the 2024 Lithuanian presidential election. Belarusian actors, including state structures and the state broadcaster Belarus-1, ran a coordinated foreign information manipulation and interference operation against several presidential candidates, using fabricated journalist personas impersonating the Latvia-based outlet Meduza to secure interviews that were then heavily edited and distributed across multiple platforms. In the week before the May 12 vote, approximately thirty pieces of derivative disinformation circulated from these manipulated interviews. The operation was detected and publicly attributed by Debunk.org, demonstrating both the speed of Lithuania’s detection capability and the closely aligned Russian-Belarusian operational pattern described above.

A key distinction in Lithuania is that effectiveness is limited. Long-term exposure has produced societal awareness. Operations gain traction only when they attach to genuine domestic grievances.

At the same time, the main challenge is growing geopolitical uncertainty. Unpredictability in the US, the war in Ukraine, and doubts about alliance reliability are creating more instability than any single Russian operation.

What Makes Lithuania Distinctive: Three Pillars

Pillar One: Coordination as method

The National Crisis Management Centre, established in 2023 under the Prime Minister's office, is the core invention. It replaced fragmented coordination with a single, legally grounded structure. Its method is disciplined:

- Eleven institutions monitor the information space;
- A shared methodology is applied;
- Low-impact narratives are ignored to avoid amplification.

Responses are calibrated according to reach, credibility, and potential impact rather than the sheer volume of incidents or online activity. This helps prevent overreaction, preserves institutional credibility, and allows resources to be concentrated on genuinely harmful threats.

The system is designed to function across a broad spectrum of crises, including hybrid attacks, cyber incidents, disinformation campaigns, critical infrastructure disruptions, natural disasters, and border-related security incidents. In practice, it enables rapid information sharing, coordinated decision-making, and unified public communication between civilian authorities, emergency services, the military, and intelligence institutions.

Recent incidents, including repeated cases of unidentified air balloons crossing from Belarusian territory and disrupting air traffic near Vilnius Airport, have demonstrated the importance of integrated monitoring and rapid interagency coordination. Such events are treated not only as aviation or border-security issues, but also as potential elements of hybrid pressure designed to test institutional responsiveness and public resilience.

Lithuania's national framework operates alongside wider EU and NATO mechanisms. It is supported by EU regulatory instruments such as the European Union's Digital Services Act and benefits from coordination with NATO structures focused on hybrid threats and strategic resilience. This ensures that domestic crisis responses remain aligned with broader allied practices and collective security standards.

Pillar Two: Whole-of-society defence

Lithuania's total defence model extends beyond the military and is rooted in the idea that resilience is societal, not institutional. It includes:

- Professional armed forces and conscription. Lithuania maintains a combination of professional military personnel and compulsory military service to ensure both operational readiness and a trained national reserve. Conscription also strengthens public awareness of national defence and reinforces the connection between society and the armed forces.
- The Riflemen's Union and National Defence Volunteer Forces (KASP) structures. The Lithuanian Riflemen's Union and the National Defence Volunteer Forces are central to Lithuania's whole-of-society defence model, linking civilian engagement with territorial defence capabilities. Both organisations strengthen local resilience, support rapid mobilisation, and help ensure continuity during crises, hybrid attacks, or wartime situations. The Riflemen's Union focuses on civic resistance, preparedness, and community resilience through training and support to public authorities during emergencies. KASP, as part of the Lithuanian Armed Forces, provides regionally based volunteer reservists who reinforce military units and support territorial defence and critical infrastructure protection.
  Commandant Units addressing wartime personnel gaps. Newly established Commandant Units are designed to support territorial defence, maintain public order, and protect critical infrastructure during wartime or national emergencies. They help address personnel shortages by integrating trained reservists and civilians into local defence and continuity structures.
  Civilian training across public and private sectors. Lithuania increasingly involves municipalities, schools, businesses, healthcare preparedness exercises. Training programmes focus on emergency response, continuity of operations, disinformation awareness, and practical preparedness for hybrid threats or natural disasters.

Public engagement in national defence has strengthened steadily since Russia's aggression against Ukraine began in 2014 and accelerated significantly after the full-scale invasion in 2022. Public support for defence preparedness, military service, and civic resilience initiatives has increased alongside rising defence spending and broad backing for an enhanced allied military presence in Lithuania. NATO deployments, including the German-led brigade, reinforce this model by linking national preparedness with collective defence.

Reference models vary by domain: Denmark for early frameworks; the US and UK for later development; Finland, Sweden, and Norway for total defence and societal resilience; and Israel for whole-of-society defence under constant threat.

The flexible "Elves" model demonstrates how organised citizen participation can reinforce state capacity in the information domain. Originating in Lithuania, the "Elves" are volunteer networks of digitally active citizens who identify, expose, and counter disinformation, hostile propaganda, and coordinated online manipulation. Rather than operating as formal state institutions, they function as civic resilience communities that complement official strategic communication efforts.

Its replication across countries, including through decentralised online communities such as NAFO, demonstrates that this form of civic participation is transferable and adaptable. These networks rely on rapid online engagement, fact-checking, humour, and community mobilisation to challenge hostile narratives and strengthen public awareness.

Beyond volunteer networks, Lithuania has produced specialised institutions that combine research, fact-checking, and capacity building. Debunk.org, founded in Vilnius, runs applied disinformation analysis, structured methodologies including the DISARM framework, and media literacy programming, and operates across the Baltic states, Poland, and several other partner countries. It illustrates how small-state civil society institutions can function as exportable resilience infrastructure.

Education and skills development are increasingly integrated into resilience, including practical training relevant to modern conflict environments. Decision-makers need to

build competence in the information domain alongside their core expertise and be prepared for a long-term effort.

At the same time, the effectiveness of Lithuania's coordinated information response has created certain vulnerabilities. Some experts underline that public trust in state institutions has become so strong that many citizens increasingly expect authorities to identify and debunk false information on their behalf, reducing incentives for independent fact-checking and individual cognitive resilience. Survey data suggests that Lithuanians are among the least likely in the EU to verify online information themselves. In response, public communication efforts are increasingly encouraging emotional self-awareness as a first-line defence, promoting the idea that highly emotional or shocking content should itself be treated as a warning sign of possible manipulation or disinformation.

Pillar Three: Calibrated communication

Lithuania does not attempt to counter every false narrative. The guiding principle is reach and potential impact. Small-scale disinformation is often ignored to avoid amplification, while larger narratives are addressed quickly and visibly. The Ministry of Defence model of "identify, label, respond early" is designed to prevent escalation before hostile narratives gain wider traction.

Responses are calibrated through a structured rating system. Low-level narratives are often addressed indirectly through academics, journalists, or independent experts, whose interventions are viewed as more credible because they appear objective rather than government-led. Mid-level narratives trigger factual responses from relevant ministries and institutional experts.

A notable example was Lithuania's energy desynchronisation from the Russian-Belarus electricity grid BRELL. Russian-linked actors promoted claims that electricity prices would rise sharply, exploiting public sensitivities linked to the closure of the Ignalina nuclear power plant. Ministry of Energy experts responded early with technical explanations and factual corrections.

Higher-rated narratives prompt responses from senior officials, while the highest escalation tier would involve statements by the president or prime minister, particularly in scenarios such as deepfake-driven disinformation campaigns.

This approach combines structured monitoring with disciplined communication and avoids turning the state into an amplifier of hostile narratives. The horizontally coordinated model based on narrative assessment and calibrated response is widely viewed as one of the most transferable elements of Lithuania's system, although its close trust-based cooperation between government and media is harder to replicate in larger and more polarised democracies.

The Russian-Speaking Minority, Soviet nostalgia and the Information Environment

Lithuania's Russian-speaking population is relatively small and largely integrated. The more significant vulnerability is cultural rather than linguistic.

Indeed, Soviet nostalgia remains present among parts of Lithuanian society, particularly within some older generations and socially or economically marginalised groups who associate the Soviet period with greater social stability, guaranteed employment, or lower living costs. While support for Soviet rule itself is limited, these sentiments can create vulnerability to Russian disinformation narratives that portray the Soviet era more positively or question Lithuania's post-independence political and economic trajectory.

This creates an entry point for influence operations focused on historical memory, economic comparison, and perceived stability. For example, Belarus adds more distinct cultural dimension through Litvinism, a narrative portraying Belarusians as closely tied to Lithuanians. This creates an influence vector that cannot be countered with standard Russia-focused responses and requires tailored approaches.

Indeed, in the case of hostile narratives linked to Belarus, Litvinism represents an important cultural dimension of the cognitive security environment. The narrative portrays Belarusians as the primary heirs of the Grand Duchy of Lithuania and seeks to blur distinctions between Lithuanian and Belarusian historical identity and statehood. In Lithuania, more radical forms of Litvinism are increasingly viewed not simply as

historical revisionism, but as part of a broader influence environment that can be used to undermine national identity, create symbolic tensions, and support hostile geopolitical narratives.

The information environment is further complicated by:

- Belarusian arrivals since 2020 and Russian arrivals since 2022;
- Ukrainian refugees with different perspectives.

These are distinct groups requiring different approaches.

A structural side effect of success is the passive citizen problem. High trust in institutions reduces individual verification behaviour. This creates a dependency risk: resilience shifts from society to the state.

Social media is the main vector of concern in Lithuania, with Facebook dominant across all age groups and TikTok and Instagram shaping younger audiences. The bigger issue is not AI itself, but platform design and policies. Recent cuts to content moderation and disinformation research, especially by Meta, have weakened the information environment and are already having a noticeable impact.

In the case of sensitive informational environments, special attention is given to the Suwałki Gap, the strategically critical corridor connecting the Baltic states with the rest of NATO territory between Kaliningrad and Belarus. Due to its geopolitical significance, defence-related projects in the region frequently become targets for hostile narratives and political contestation.

A recent example was the proposed Kapčiamiestis military training range near the Suwałki corridor. Although presented by Lithuanian authorities as necessary for territorial defence, military readiness, and allied interoperability, the project became a focus of anti-NATO and pro-Russian narratives portraying Lithuania as being militarised or turned into a frontline zone. The debate illustrated how strategically important infrastructure projects can become part of the broader cognitive defence environment, where public opinion, local concerns, and hostile information operations intersect.

Despite sustained opposition campaigns and disinformation narratives, the Lithuanian parliament approved the establishment of the training ground in May 2026, reaffirming the country's long-term commitment to strengthening defence infrastructure in the region.

Coordination Architecture

The placement of the National Crisis Management Centre within the Prime Minister's Office gives Lithuania's crisis coordination system strong political authority and ensures that interagency coordination functions at the highest level of government. The Centre does not replace ministries, but organises their cooperation through shared situational awareness, common assessment standards, and coordinated decision-making.

Responsibilities remain distributed according to institutional competence:

- The Ministry of the Interior leads border and internal security crises;
- The Ministry of National Defence leads military, cyber and hybrid security issues;
- The Ministry of Foreign Affairs coordinates external communication and international engagement;
- The Ministry of Culture contributes to strategic communication and counter-disinformation efforts;
- The Ministry of Transport and the Ministry of Energy are responsible for critical infrastructure resilience and continuity;
- The Ministry of Agriculture oversees food security and resilience planning in the agricultural sector;
- The Ministry of Health leads public health preparedness, disease response, and health system resilience.

Academic institutions are increasingly integrated into this architecture. The Centre for Communication Influences and Propaganda Research, established at Vilnius University's Faculty of Communication in October 2024, conducts research on strategic narratives, propaganda, and disinformation in the public sphere, and provides expertise

to decision-makers. This formalises a research-policy bridge that previously relied on individual academic relationships, embedding analytical capacity within an institution that can sustain it over time.

The structure evolved gradually through several stages:

- Early awareness of hybrid and information threats emerged in the mid-2000s;
- Russia's aggression against Ukraine in 2014 became a major strategic shock that accelerated preparedness and interagency coordination;
- The COVID-19 pandemic acted as a catalyst for permanent horizontal coordination across government institutions.

As a result, the system now functions continuously rather than only during emergencies, enabling constant monitoring, preparedness, and rapid response.

The architecture is also embedded within wider EU and NATO frameworks:

- EU mechanisms support infrastructure resilience, cybersecurity, civil preparedness, and regulatory responses;
- NATO provides intelligence sharing, operational coordination, deterrence measures, and hybrid threat support teams.

The architecture is reinforced by a developing legal toolkit. In February 2024, Lithuania enacted Article 118 of its Criminal Code, which establishes criminal liability for the manipulation of accounts or the artificial amplification of information on social media when directed against the constitutional order, sovereignty, territorial integrity, defence, or economic power of the state. The provision allows penalties up to five years of imprisonment. It sits alongside Article 285, which addresses false information likely to cause public panic or disrupt critical infrastructure operations. Together, these provisions give Lithuania the capacity to act against coordinated information operations without relying solely on broader speech restrictions.

How does the Centre operate in practice? Institutions involved contribute to a shared monitoring and assessment process. Each institution monitors the information

environment from its professional perspective using a common methodology. Narratives are assessed on a scale from zero to ten according to reach, credibility, and potential impact. Ratings below two are deliberately ignored. This threshold discipline emerged from earlier experience, when institutions sometimes reacted to marginal narratives and unintentionally amplified them through official responses. The current system is designed to avoid doing the adversary's work for them. Approximately three to ten narratives are formally assessed each week, with continuous tracking of how narratives evolve and how public engagement changes over time.

A practical example involved Lithuania's synchronisation and desynchronisation from the Russian electricity grid. Russian-linked actors circulated claims that the process would cause dramatic electricity price increases, using seemingly credible economic arguments and exploiting public sensitivities linked to the closure of the Ignalina nuclear power plant. Rather than escalating the issue politically, the response was calibrated to the narrative's assessed impact. Experts from the Ministry of Energy provided technical explanations and factual corrections before the claims gained wider traction.

Honest Limitations

Lithuania's system is effective but not complete. Passive citizen risk remains a concern. High trust in institutions has made Lithuanian citizens less likely to verify information themselves, weakening individual cognitive resilience.

Indeed, as already stressed, the effectiveness of Lithuania's coordinated information response has also produced certain unintended side effects, as strong public trust in state institutions has reduced incentives for independent fact-checking and weakened individual cognitive resilience. While precise figures on trust in counter-disinformation institutions remain limited, broader surveys indicate comparatively high trust in Lithuanian state institutions involved in security and public order, including around 69% trust in the police and 55% trust in the Special Investigation Service (STT)

Small-scale trust networks do not scale easily to larger societies.

Geopolitical uncertainty, including questions about alliance cohesion, creates a more complex environment than any single adversary operation.

The threat landscape is evolving. AI-driven manipulation and deepfakes are likely to increase pressure on response systems.

Measurement remains limited. It is easier to map operations than to assess their real-world effects.

What Lithuania Models for Others

What makes Lithuania's model transferable is not its scale but its structure. Central coordination under political authority ensures that responses remain coherent rather than fragmented. Shared methodologies for monitoring and assessing threats create a common operating picture across institutions, while disciplined communication thresholds prevent overreaction and avoid amplifying hostile narratives. Civil society is treated not as separate from the state, but as part of the resilience system itself.

The broader lesson is that cognitive resilience depends less on isolated technological tools and more on governance discipline, coordination, and societal preparedness. Lithuania did not eliminate uncertainty or hybrid threats. Instead, it built a system capable of managing them continuously while anchoring national resilience within wider EU and NATO frameworks.

At the same time, some elements are less transferable. Informal trust networks between institutions, close working relationships with major media outlets, and the cohesion of a relatively small society are difficult to replicate in larger and more politically fragmented democracies. These characteristics enable rapid coordination and alignment in Lithuania, but cannot simply be copied elsewhere.

Partner Landscape

Lithuania's resilience model is not purely national. It is built on domestic coordination, but sustained and reinforced through deep integration with regional, EU, and NATO frameworks. These partnerships are not secondary additions but core components that extend Lithuania's capacity, reduce vulnerabilities, and embed national resilience within a wider collective security architecture.

Regional cooperation among the Baltic states remains particularly important. Lithuania works closely with Latvia and Estonia on strategic communication, counter-disinformation, cybersecurity, and hybrid threat monitoring, reflecting shared threat perceptions and similar institutional approaches. Baltic-Polish cooperation has also intensified, especially in countering Russian disinformation, protecting critical infrastructure, and coordinating responses to hybrid pressure along NATO's eastern flank.

Lithuania is also active within the Joint Expeditionary Force (JEF), where Northern European states cooperate on hybrid threats, maritime security, and rapid crisis coordination below the threshold of conventional conflict. These frameworks strengthen information sharing, situational awareness, and coordinated response planning across the Baltic Sea region.

At the EU level, cooperation is most visible in infrastructure resilience, regulation, and strategic coordination. Energy synchronisation with Continental Europe reduced dependence on Russia and Belarus and removed a major hybrid vulnerability. EU mechanisms support cybersecurity, military mobility, defence financing, and regulatory responses related to digital platforms and critical infrastructure protection. Lithuania also contributes to and benefits from structures such as the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) and the EU Hybrid Fusion Cell, which support threat analysis, information exchange, and coordinated responses to hybrid activity.

NATO provides the operational and deterrence dimension of this architecture. Forward deployments, including the German-led brigade, demonstrate that Lithuania's defence is collective from the outset. NATO air policing, intelligence sharing, hybrid threat support teams, and operations such as Baltic Sentry strengthen Lithuania's ability to detect and respond to hybrid activity before escalation. NATO's increasing recognition of hybrid threats as part of collective defence has also narrowed the grey zone adversaries seek to exploit.

Lithuania additionally uses the Organisation for Economic Co-operation and Development as an external platform for exporting elements of its resilience model,

including support for disinformation resilience initiatives and training programmes involving around twenty countries.

Chapter 26: France

France has become one of the genuine leaders on cognitive defence within Europe and the broader democratic world. This is itself a significant shift. In the years before 2022, France was widely viewed in Eastern Europe as one of the EU countries most sympathetic to Russia and most supportive of accommodating Moscow's position. The journey from there to here is part of what makes the leadership project consequential. VIGINUM is the strongest dedicated detection institution in the European Union, French Response is the most fully developed active defence model among European democracies, and President Macron's personal championing of European cognitive sovereignty has built coalition support for the project across the EU and beyond. The architecture is real, the leadership is real; the French model is now actively being adapted by Germany and studied by others, and its analytical methodology has become the foundation of the European Union's FIMI work through the European External Action Service. The institutional architecture rests on an increasingly shaky foundation. France built one of the most generous social welfare states in the democratic world, and over recent decades did not defend it well enough to keep it whole. A threshold has now been crossed in public trust in the political class, the parliament, and the government, with trust in each measured at between 17 and 22 percent in early 2026.[1] The attachment to democracy as a system remains strong; the willingness to defend France remains higher than in most major European democracies.[2] What has fractured is faith in the current institutional arrangement that delivers democracy, and that fracture is what foreign information manipulation exploits. France is therefore the cautionary case for the six-layer cognitive defence framework. The best detection and active defence architecture in the democratic world is not enough on its own to defend against a social infrastructure that has given way and democratic institutions that have lost the public's trust.

Security culture and France's approach to information sovereignty

France approaches security and defence as files of unusually concentrated national sovereignty. Few democracies place coordination of security and defence as tightly under the head of government as France does. The institutional reflex is to treat questions of state security as French matters first and European or multilateral matters second, a

disposition that runs through the Fifth Republic's political-cultural inheritance and through the Élysée's structural primacy over the foreign and defence portfolios. This is the disposition the cognitive defence file has been built within, and the disposition that explains both what France has built and how France has chosen to lead.

The institutional through-line on FIMI runs across roughly a decade. The 2017 attempt by Russia to disrupt Emmanuel Macron's presidential campaign through the release of stolen emails on the eve of the legal silence period gave France its first direct experience of an adversarial state operation aimed at the country's democratic decision-making process. Unlike many democracies, France started to learn from this experience immediately. The 2018 *loi relative à la lutte contre la manipulation de l'information* (Law 2018-1202) made France the first major Western democracy to legislate specifically against information manipulation during election periods. Task Force Honfleur was stood up under the Secrétariat général de la défense et de la sécurité nationale (SGDSN) in 2020. VIGINUM was established by a decree of the French government of July 2021, issued by the Prime Minister, placing VIGINUM under the authority of the Secretariat-General for National Defence and Security (SGDSN). Its functions were consolidated and expanded by the decree in February 2026.[3] The 2026-2030 National Strategy against Foreign Digital Interference, adopted by the SGDSN in February 2026, codifies the doctrinal frame under which the architecture now operates.[4] The candidate whose campaign was attacked in 2017 became the European leader who has now articulated European cognitive sovereignty as a continental project.

Two elements of French political-cultural inheritance shape what has been built. The first is administrative centralisation. SGDSN sits under the Prime Minister and coordinates security and defence across ministries on the President's authority, the institutional design that has allowed France to place VIGINUM where it sits and to coordinate the cognitive defence architecture horizontally across the state in a way federalised systems would struggle to match. The second is the political-will articulation at the head-of-government level. President Macron's three major interventions on the file, the Sorbonne II "Europe is mortal" speech of 25 April 2024, the Saarbrücken German Unity Day address of 3 October 2025, and the Berlin Digital Sovereignty Summit with Chancellor Merz on 18 November

2025, have built the case for European cognitive sovereignty as a strategic project across an EU-wide political coalition rather than only within France.[5] The Sorbonne speech of April 2024 framed Europe's risk of mortality as a strategic-sovereignty problem of which information sovereignty was a load-bearing element, calling for European cybersecurity and cyberdefence capacity adequate to defend the continent's democratic life. The Saarbrücken speech named the twin threats with rare clarity: authoritarian propaganda from outside and democratic doubt from within. The Berlin summit framed digital sovereignty as a refusal to be a vassal of either American or Chinese platforms, and pushed directly at the platform-algorithm question that European leaders have largely avoided. Macron has reclaimed the freedom-of-expression argument from the platforms themselves, framing the issue not as state restriction of speech but as the refusal to let private algorithmic systems determine the conditions of democratic discourse without democratic accountability. The 2026-2030 Strategy is the institutional codification of what those speeches have argued.

That political-will articulation has produced real operational results. The G7 Rapid Response Mechanism, which Canada has chaired since 2018, was the institutional vehicle through which G7 coordination on FIMI had operated for seven years; the G7 Leaders' declaration of January 2025 under the French presidency elevated FIMI to a leaders-level commitment at the moment the United States was withdrawing from this work, an explicit French-led codification at the highest political level. The European Democracy Shield communication by the European Commission and the High Representative from November 2025 established a European Centre for Democratic Resilience as the coordination hub for Member State capability rather than a centralised EU-level detection agency, a design that matches the French preference for sovereign Member State capability coordinated through EU architecture rather than substituted by it.[6] The Information Manipulation Spectrum (IMS) analytical model VIGINUM developed has been adopted by the European External Action Service as the methodological standard, and the January 2026 *Building a Common Operational Picture of FIMI* report, co-authored by VIGINUM, the Auswärtiges Amt, the EEAS, and four independent civil-society and analytical organisations (EU DisinfoLab, CheckFirst, Cassini, and the Atlantic Council's DFRLab), is the operational expression of that adoption.[7] The void left by the

closure of the United States Global Engagement Centre in December 2024 has been the space France has stepped into, and the academic record now treats this as deliberate role-claiming rather than reactive opportunism.[8]

The empirical picture of where the foundation beneath the architecture stands now is sharper than is comfortable. The Centre de recherches politiques de Sciences Po (CEVIPOF) *Baromètre de la confiance politique* Vague 17, fielded in February 2026 with a sample of 3,166 respondents by OpinionWay for Sciences Po, recorded 22 percent trust in politics (down four points year-on-year), 17 percent trust in the government, 20 percent trust in the National Assembly (matching the December 2018 *gilets jaunes* historical low), 18 percent trust in the President of the Republic, and 15 percent trust in political parties. Eighty-seven percent of respondents said political leaders do not care about citizens. Seventy-four percent said they are corrupt. Sixty percent reported that they "cohabit" rather than live in a united nation. Seventy-nine percent want more frequent referenda; 77 percent want citizens' conventions.[9] France's trust collapse is among the steepest in Western Europe, and the CEVIPOF data shows continued decline from an already-low OECD baseline.[10] The picture is not uniformly negative. Eighty-two percent of respondents remain attached to democracy as a political system. The willingness to defend France in the event of war, measured by the Riga Stradins University autumn 2025 survey across NATO members, sits at 42 percent, in the upper half of the Alliance and above Canada (39 percent), the United States (37 percent), Germany (27 percent), and Italy (25 percent).[11] This is the picture: an attachment to democracy that holds, a willingness to defend the country that exceeds most major European democracies, and a collapse of confidence in the political-institutional arrangement that delivers democracy in practice.

The threat environment

French intelligence assessments name Russia, China, Türkiye, and Iran as the four states of most concern, in the public-record framing of the November 2023 annual report of the Délégation parlementaire au renseignement (DPR), the foundational French public-record analysis of the foreign interference threat picture.[12] Azerbaijan has been added to the public attribution record through VIGINUM's December 2024 investigation. The

intelligence assessment that has gained the most analytical traction in Paris is that the threat actors are not always operating in coordination but produce ad hoc alignments of interest, particularly around French vulnerabilities in the overseas territories, in Corsica, and in Africa.[13]

Russia is the primary acute threat. The DPR characterises Russia as the only state to have made information manipulation an official doctrine of foreign policy. The 2017 operation against the Macron campaign remains the foundational French case, attributed to GRU Unit 26165, the same Russian military intelligence unit responsible for the 2016 DNC hack in the United States. The Doppelganger operation, exposed by VIGINUM in June 2023, established the working pattern: cloned versions of legitimate Western media sites seeded with disinformation designed to be shared as if from the originals.[14] The Portal Kombat network, exposed by VIGINUM in February 2024, mapped at least 193 interlinked websites spreading pro-Kremlin narratives across Europe.[15] Storm-1516, the operation involving John Mark Dougan and an extensive AI-generated content programme, targeted France with five major narratives between December 2024 and March 2025 that reached close to 56 million social media views.[16] The red hands case of June 2024, when the Shoah Memorial in Paris and the Mur des Justes were daubed with red hands, was attributed by VIGINUM in its Matryoshka investigation to a Russia-linked operation.[17] The Matryoshka operation continued through 2025 and 2026, including a coordinated campaign in February 2026 that weaponised the release of the United States Justice Department's Epstein files to attack President Macron directly, using forged content branded as France 24, *Libération*, *Le Parisien*, *La Croix*, and Reuters to spread fabricated allegations across X, Telegram, and Bluesky.[18] The 2024 Romanian presidential election, where Russian information operations contributed to the conditions that produced the Călin Georgescu first-round victory and the constitutional court annulment that followed, is the European case that has most shaped French thinking about what FIMI can do when it lands on a foundation that has already given way.

China is the medium-term systemic threat in the DPR's framing, operating through longer time horizons and across academic, economic, and diaspora-influence vectors. VIGINUM has publicly documented Chinese-attributable digital interference using the Spamouflage

operating method, including text content generated by AI and seeded across X and Tumblr by inauthentic-account ecosystems during the Paris 2024 Olympic and Paralympic Games.[19] The Front uni, or United Front strategy, that France's parliamentary intelligence committee describes is the longer-term institutional vector: a Chinese state framework using diaspora networks, academic exchange, and economic relationships to shape French public discourse on issues including Taiwan, Hong Kong, and Xinjiang.

Azerbaijan has been the precedent-setting non-traditional attribution. VIGINUM's December 2024 *Un-notorious BIG* report named the Baku Initiative Group as the principal actor behind disinformation operations targeting France in connection with New Caledonia, Corsica, and the COP 29 climate conference Azerbaijan hosted.[20] Azerbaijan's information operations against France are widely seen as being linked to France's close political and security ties with Armenia, as well as Paris's strong criticism of Azerbaijani actions in Nagorno-Karabakh. This is the public attribution that established the principle France has carried forward: that public attribution of a non-Russia, non-China state actor on the basis of OSINT investigation is doable, defensible, and one element in a broader cost-imposition response that includes diplomatic denunciation, EU advocacy, and the eventual adoption of restrictive measures. EU sanctions adopted in May 2025 expanded the restrictive measures regime to cover FIMI actors and were applied to several individuals and entities VIGINUM had previously named, including ones connected to Doppelganger and Portal Kombat.

Türkiye is associated with political entryism through religious financing, mosque networks, and the New Caledonia case, where Kanak representatives were invited to a March 2024 decolonisation conference in Ankara and where disinformation around a French ministerial visit to Nouméa was suspected by French intelligence of having Türkiye-based origins. Iran appears across the French threat picture as one of the four states of concern, less developed in VIGINUM's public attribution record than Russia or Azerbaijan to date. The European External Action Service's third FIMI Threats Report (March 2025) recorded 505 FIMI incidents globally in 2024 across 90 countries, with France the second most-targeted state after Ukraine and the subject of 152 cases attributable to Russian and Chinese FIMI ecosystems.[21]

What France has built: VIGINUM, French Response, and the 2026-2030 Strategy

VIGINUM operates as a horizontal coordination service within SGDSN under the Prime Minister, with approximately 65 staff, of which 35 to 40 are analysts in the operational division. The agency's mandate, set by Decree 2021-922 of 13 July 2021 and consolidated by the decree of 11 February 2026, is to detect and characterise foreign digital interference operations meeting four cumulative criteria: a content that is manifestly false or deliberately misleading, an inauthentic and artificial mode of dissemination, foreign actor involvement, and harm to France's fundamental national interests or to the integrity of public debate during electoral periods.[22] The criteria are deliberately tight. VIGINUM does not look at domestic political speech and is barred by its founding decree from doing so. It looks at foreign-actor inauthentic operations using France's information space, which is the distinction that has allowed the agency to operate publicly without producing the censorship-and-overreach criticism that has dogged similar projects in other democracies.

VIGINUM's published evidentiary record is built on open-source intelligence. The service is officially the State's open-source investigation arm, established to detect and characterise foreign digital interference operations by analysing publicly accessible content on online platforms. The 2026 decree expanded VIGINUM's data-collection authorities while maintaining the open-source posture of its published reports. The methodological choice is strategically significant. By basing its public attributions on open-source evidence, VIGINUM produces analytical product that can move across institutional boundaries without the secondary-distribution problems classified material creates, and the European Union has been able to use that product as the basis for restrictive measures under the FIMI sanctions regime. The choice does not isolate VIGINUM from the wider French intelligence community. The Direction générale de la sécurité extérieure (DGSE), France's foreign intelligence service, and the Direction générale de la sécurité intérieure (DGSI), the domestic intelligence service, contribute to the broader French threat picture and to the inter-ministerial decision-making process that underlies attribution choices, including which operations to investigate and how to characterise them. The Direction du renseignement militaire is reported to play a role in the offensive

counter-interference function that sits outside VIGINUM's published mandate.[23] What the open-source posture creates is a public-facing evidentiary record that does not depend on disclosing intelligence sources. This is what allows attribution to function as a diplomatic and sanctions-grounded instrument; it is also what allows attribution to function as a public-trust instrument, demonstrating to citizens that the state can name foreign interference with evidence rather than asking the public to take attribution on faith.

The active defence layer that sits alongside VIGINUM detection is the responsibility of two separate centres of operation. The first is the Ministry for Europe and Foreign Affairs (MEAE) counter-FIMI unit, a small team operating across analyst, communications, and policy functions that produces public denunciations of detected operations, projects French strategic communication into contested information spaces abroad, and coordinates with embassies and partner foreign ministries to share lines and aligned response. The MEAE's French Response model is the most fully developed European active defence framework currently in operation: a structured doctrine that combines public attribution of inauthentic operations, denunciation of red-line crossings, and projection of France's own positive narrative in spaces where adversary operations are most active. The second is the Ministry of Armed Forces, which carries the military active defence function in operational theatres abroad, including in the Sahel and in support of French deployments to NATO Forward Land Forces. Administrative-technical response, including direct engagement with platform providers and service providers on infrastructure vulnerabilities identified through VIGINUM detection work, sits as a third register coordinated through SGDSN and operates without public profile.

The 2026-2030 National Strategy codifies what the architecture has now become and where it commits to going next. Pillar 1 commits France to building societal resilience through media literacy expansion, civic engagement instruments, and a VIGINUM Academy designed to extend analytical capability across the French state and partner administrations. Pillar 2 commits to consolidating the detection and response architecture, including the recent decree's expansion of VIGINUM's mandate. Pillar 3 commits to platform accountability and to the implementation of the Digital Services Act at national level under ARCOM oversight. Pillar 4 commits to structuring a European community of

FIMI services and to projecting French doctrine through the European Union, the G7, NATO, the OECD, the United Nations, and the Francophonie.[24]

Honest limitations

The central honest limitation is the foundation the architecture sits on. The Centre de recherches politiques de Sciences Po (CEVIPOF) picture and the *gilets jaunes* through pension reform through 2024 dissolution through Bayrou and Lecornu government instability arc are the picture of a social-infrastructure foundation that has been allowed to crack while the upper-foundation architecture has been built on top of it. Pillar 1 of the 2026-2030 Strategy is the explicit recognition of this gap, and it is also at commitment stage rather than at operational reality. The VIGINUM Academy is being built. The civic engagement instruments, including the new-generation format of the Defence and Citizenship Day being rolled out from September 2025, civic service, the voluntary military service Macron announced on 27 November 2025 to begin in 2026, and the reserves, are being scaled rather than reimagined. Pillar 1 is also not the totality of a reinvestment in France's social infrastructure, nor is it designed to be. The broader work, the work that the budget plans of the Bayrou and Lecornu governments have cut against rather than supported, sits outside the cognitive defence architecture entirely. The €5 billion healthcare spending cap, the cut of 3,000 civil service jobs, the proposed elimination of two national holidays, the unemployment-insurance reform, and the ongoing fiscal compression of social spending under the pressure of defence-budget expansion, all continue to erode the foundation while Pillar 1 builds counter-FIMI resilience adjacent to but not substituting for that work. The relational work of restoring trust between the political class and the populations who have lost faith in it is hard and slow, but not impossible. It is the work of a generation, not an electoral cycle, and it is not work the cognitive defence architecture can do on its own. The architecture's central exposure is at the foundation it was built to protect.

The April 2027 presidential election sits inside this picture. What the election will test is whether the political-will articulation that has produced France's leadership project on cognitive defence survives the polarisation that has reshaped French politics and the rise of the *Rassemblement national*, France's far-right national party, currently polling above

33 percent for legislative voting intention. A change of presidential direction in France would not immediately dismantle VIGINUM, French Response, or the 2026-2030 Strategy, though it could very well do so over time, if dismantlement became the political mandate of a new government. The institutional architecture is law and ministerial structure; law can be amended and ministerial structures can be restructured. The more immediate threat is the loss of the political articulation that has made France's leadership of the European project possible, and the resulting uncertainty about whether France continues to lead the European cognitive defence project or whether the project loses its leading articulator at the moment EU institutions are starting to build around it. That is the foundation-architecture exposure the chapter's argument turns on.

Three supplementary limitations warrant being named. The first is that France's societal resilience capability remains at commitment stage. The Nordic and Baltic comparator chapters describe operational reality on Layer 1 work; France's 2026-2030 Strategy Pillar 1 is a credible roadmap rather than a comparable operational record. The second is the intelligence-to-strategic-communications coordination pattern across the French state, which field research suggests remains less fluid than the public-facing architecture implies. The third is the algorithm-knowledge gap: VIGINUM analyses platform outputs but does not have full visibility into the upstream algorithmic and amplification dynamics that shape what the public encounters. This is a limitation shared across European democracies and acknowledged in the 2026-2030 Strategy's Pillar 3 commitments around platform accountability. An additional outside-view qualification comes from EU DisinfoLab's May 2025 France factsheet, which observed that France has a dense ecosystem of fact-checking, media literacy, and legal frameworks against disinformation, but that coordination across that ecosystem remains a challenge that leads to fragmented responses.[25]

What travels from France

France's model is harder to copy than it looks. The visible elements, an OSINT-based detection methodology and a structured doctrine for public attribution, are publicly documented and methodologically transferable. What makes the French model work is not those visible elements alone. It is the alignment of five institutional conditions that very

few democracies have achieved at the same time: dedicated analytical capacity at scale (35 to 40 French-language FIMI analysts and a serious Datalab), legal authority for automated collection across major online platforms, institutional placement that allows inter-ministerial coordination on the President's authority, sustained political will at head-of-government level willing to defend the architecture against domestic political attack, and integration with the broader intelligence community that does not require the published evidentiary record to depend on classified intelligence. Each condition is independently demanding. The combination is what produces VIGINUM's capability, and the combination is rare.

Three elements of France's experience travel, with different adoption conditions.

The IMS analytical methodology as a shared European standard. The Information Manipulation Spectrum framework VIGINUM developed has been adopted by the EEAS and applied across the January 2026 common operational picture work. The model gives partner agencies a common analytical language for assessing inauthenticity and impact, and it gives the European Union a methodological standard in which the FIMI sanctions regime can be evidentially grounded. This is the most transferable element of France's experience. Smaller European democracies can adopt the methodology through EEAS partnership and through the VIGINUM Academy without needing to build VIGINUM-scale detection capacity of their own. The adoption condition is institutional capacity at the three analytical tiers IMS uses (signal detection, manipulation characterisation, and impact assessment), and willingness to work with the OSINT evidentiary standard that allows analytical product to move across institutional boundaries.

The doctrinal shift from monitoring to occupying the information space. The combination of VIGINUM detection and the MEAE French Response active defence model is the most fully developed European answer to the question of how a democracy can defend itself against FIMI without sliding into the censorship-and-counter-propaganda posture that erodes democratic norms. The doctrine treats public attribution as defence, projects French strategic communication into contested spaces rather than retreating from them, and accepts that effective cognitive defence requires the state to be present in the information environment rather than only watching it. The doctrine has been

studied by Germany and is being adapted with German institutional features. The UK Parliament's Joint Committee on the National Security Strategy has also drawn on the French model in its recent study of malign actors and democratic resilience.[26] The adoption condition is sustained political will at the head-of-government level. The doctrine is significantly aided by presidential or prime ministerial championing, sustained over multiple years, to defend the architecture against the inevitable domestic political attack on counter-FIMI activity as censorship or partisan use of state communication. France has had this championing in unusually concentrated form. Most other European democracies have not.

The institutional model as a partial template. The fuller VIGINUM-and-MEAE institutional architecture transfers in pieces rather than as a whole. Germany's adaptation is the closest example of partial adoption: a new dedicated detection agency built on the French model, but placed under the Ministry of the Interior rather than under the Chancellery, with seconded MFA officers and aspiration to import French-style inter-ministerial coordination. The placement difference matters. Germany's federal structure and post-Weimar constitutional design make placement under the Chancellor difficult; the Ministry of the Interior is the available institutional home but it does not produce the same horizontal coordination reach VIGINUM has under SGDSN. The adoption conditions are legal authority for collection at scale, willingness to invest in dedicated analytical capacity, and a clear institutional home that can credibly coordinate across ministries. Each democracy's design is responsive to its own institutional inheritance. France's design is the most fully developed European answer because France purposefully aligned the five conditions over a sustained institutional effort that began with the 2018 information manipulation law and has been built on at every step since.

The cautionary observation that travels across the broader Alliance. France is the case that demonstrates the framework's central interdependence claim. A democracy can build the strongest detection and active defence architecture within the European Union, can articulate a coherent doctrine at the highest political level, can lead the European project on the file, and can still find the architecture exposed at the foundation it was built to protect when the social-infrastructure foundation underneath is allowed to crack.

Canada, Germany, the United Kingdom, and most major democracies with generous social contracts now under fiscal pressure and populations that read the contract as being rewritten without their consent sit closer to the French trajectory than to the Finnish steady state. The lesson is that detection and active defence are necessary but not sufficient. The foundation work, the patient, multi-decade investment in social infrastructure and democratic-institutional trust that Chapter 6 develops in detail, must run alongside it, or the architecture above ends up exposed at exactly the layer it was built to protect. France did not build the cognitive defence architecture ahead of its social-infrastructure foundation. France built the social-infrastructure foundation first, decades before VIGINUM existed. What France did was allow that foundation to erode over time, and then, when the FIMI problem became visible in 2017, built the cognitive defence architecture without adequately reckoning with the cracks that were already opening in the ground beneath its feet. France is the case that shows what happens when a country builds sophisticated architecture on top of a foundation it has stopped tending to. The architecture is necessary. It is not sufficient.

France's partner landscape

Germany is France's lead European bilateral on cognitive defence. The Weimar Triangle format with Poland operates as a small, trust-based, operationally focused coordination forum with frequent engagement at analyst, political-director, and strategic-director levels. The format's strength is precisely its smallness and its informality: no secretariat, no bureaucratic overhead, a coordination tempo that allows for rapid alignment on common communication lines. Joint communication campaigns including the recent coordinated effort on Russia's shadow fleet are the operational expression of the trilateral working format. The Weimar Triangle has been extended on a more limited basis to include the EEAS and the United Kingdom in a "Weimar Plus" framing, though the core operational coordination remains trilateral. President Macron's joint appearance with Chancellor Merz at the Berlin Digital Sovereignty Summit in November 2025 is the most recent high-level political expression of the Franco-German operational partnership in this domain.

Poland is the third member of the Weimar core and has built its own counter-FIMI capability from the cyber side through NASK (Naukowa i Akademicka Sieć Komputerowa,

the national research institute), ABW (Agencja Bezpieczeństwa Wewnętrznego, the domestic intelligence service), and SKW (Służba Kontrwywiadu Wojskowego, military counterintelligence) rather than as a dedicated agency-and-active-defence pairing on the French model, which combines VIGINUM detection with the MEAE French Response active defence unit and the Ministry of Armed Forces military function. The cooperation across the three Weimar partners is operationally close, particularly in the run-up to elections and around historical-memory contests where Russia's narrative operations on the Second World War commemoration have produced coordinated trilateral response.

The European Union is the institutional pillar France has invested most in shaping. The European External Action Service has adopted VIGINUM's IMS model as the methodological standard. The European Democracy Shield, published as a Commission and High Representative communication on 12 November 2025, establishes a European Centre for Democratic Resilience that matches France's preference for a Member State-led architecture coordinated through EU institutions rather than substituted by them. The May 2025 expansion of the EU restrictive measures regime to cover FIMI actors has been built on VIGINUM's OSINT evidentiary record. The G7 Leaders' declaration of January 2025 under the French presidency is the multilateral parallel track.

The United Kingdom is the intelligence-StratCom model France has studied most closely. The UK Government Communications Headquarters posture on attribution and the 77th Brigade as the dedicated information-environment unit are the two elements that have informed French thinking, though the French architectural choice has been to build the equivalent capability within civilian agencies (VIGINUM, MEAE) rather than within military structures. The UK is significant for France's cognitive defence project because it combines intelligence-led attribution with public strategic communication in a way few European democracies do, and because UK-France intelligence-sharing on Russian operations has been one of the most productive bilateral channels of the post-2022 period.

Canada is an operational partner France has been working with closely since at least 2024. The Rapid Response Mechanism Canada has chaired through the G7 since 2018 is recognised in Paris as the conceptual antecedent of VIGINUM, and bilateral exchanges

have included analytical methodology and operational practice. VIGINUM's weekly electoral-bulletin methodology was developed in dialogue with the Canadian Privacy Commissioner, an early example of bilateral cooperation shaping French operational design. Field research with both VIGINUM and MEAE counter-FIMI staff confirms Canada as one of the countries that has actively approached France for deeper cooperation since the United States withdrew from the field in late 2024. The bilateral relationship is operationally close and methodologically aligned, and represents one of the most active non-EU partnerships in France's cognitive defence partner landscape.

The institutional architecture France has built is sophisticated. The leadership project France has articulated has produced the European centre of gravity for cognitive defence cooperation in the absence of American leadership on this file. What the architecture and the leadership cannot do is repair the foundation underneath. The 2026-2030 Strategy's Pillar 1 makes a partial contribution to that work through media literacy and civic engagement, but Pillar 1 is not, and is not designed to be, the totality of a reinvestment in France's social infrastructure. The broader work sits outside the cognitive defence architecture entirely, and the political class will or will not be allowed to continue it depending on what April 2027 produces.

The April 2027 presidential election will be extraordinarily consequential, and not only for France. The European cognitive defence project France has built rests on French leadership at the head-of-government level, leadership the architecture cannot replicate from below. A change of presidential direction in France would not immediately dismantle VIGINUM, French Response, or the 2026-2030 Strategy. It would end the political articulation that has made France's leadership of the European project possible, at the precise moment the EU is building institutional structures designed around the French model, and at the moment the broader democratic world most needs the project to continue. What April 2027 produces will shape not only France's own cognitive defence trajectory but the cognitive defence trajectory of European democracy, and, given the absence of American leadership on this file, of the democratic world as a whole.

Endnotes

1. Centre de recherches politiques de Sciences Po (CEVIPOF), *Baromètre de la confiance politique, Vague 17*, fieldwork by OpinionWay, sample of 3,166 respondents, published 9 February 2026, at sciencespo.fr/cevipof.

2. Center for Geopolitical Studies Riga and Riga Stradins University, "Willingness to Fight Across NATO,", available at geopolitics.center.

3. On VIGINUM's founding and consolidation: Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé "service de vigilance et de protection contre les ingérences numériques étrangères," *Journal officiel de la République française*, 14 July 2021.

4. Secrétariat général de la défense et de la sécurité nationale, *Stratégie nationale de lutte contre les ingérences numériques étrangères 2026-2030* (Paris: SGDSN, 11 February 2026).

5. Emmanuel Macron, "L'Europe peut mourir," speech at the Sorbonne, 25 April 2024, transcript available at elysee.fr; Emmanuel Macron, speech for German Unity Day, Saarbrücken, 3 October 2025, transcript at elysee.fr; Emmanuel Macron and Friedrich Merz, joint statements at the Berlin Digital Sovereignty Summit, 18 November 2025.

6. European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *European Democratic Shield: Empowering Strong and Resilient Democracies*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2025) 791 final, 12 November 2025.

7. VIGINUM, Auswärtiges Amt, European External Action Service, EU DisinfoLab, CheckFirst, Cassini, and Atlantic Council's Digital Forensic Research Lab (DFRLab), *Building a Common Operational Picture of FIMI: Russian Operations Doppelganger, Media Brands/RRN, Undercut, Storm-1516, and Overload* (Paris, Berlin, Brussels, January 2026).

8. A. K. Cianciara, "How Has France Established Itself as a Champion of the European Fight Against Foreign Information Manipulation and Interference (FIMI)?" *JCMS: Journal of Common Market Studies* (2026), DOI 10.1111/jcms.70114.

9. CEVIPOF, *Baromètre de la confiance politique, Vague 17*, *op. cit.*

10. Organisation for Economic Co-operation and Development, *OECD Survey on Drivers of Trust in Public Institutions, 2024 Results, Country Notes: France* (Paris: OECD, 2024).

11. Center for Geopolitical Studies Riga and Riga Stradins University, "Public Trust in NATO Across Alliance Countries" and "Willingness to Fight Across NATO," surveys & Māris Andžāns, "Would You Fight For Your Country? The Most and Least Willing Among NATO Allies," *Foreign Policy Research Institute*, 20 March 2026.

12. Délégation parlementaire au renseignement, *Rapport relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2022-2023*, Assemblée nationale and Sénat, November 2023.

13. Inès Gentil, *Disinformation Landscape in France* (Brussels: EU DisinfoLab, May 2025).

14. VIGINUM, *Rapport technique RRN: une campagne numérique de manipulation de l'information complexe et persistante* (Paris: SGDSN, June 2023).

15. VIGINUM, *Portal Kombat: un réseau structuré et coordonné de propagande prorusse* (Paris: SGDSN, February 2024)..

16. VIGINUM, *Storm-1516, l'écho des opérations de manipulation de l'information du Kremlin* (Paris: SGDSN, May 2025).

17. VIGINUM, *Matriochka: une opération de manipulation de l'information dirigée contre les médias et la communauté de l'information* (Paris: SGDSN, 2024).

18. Bot Blocker / *The Insider*, investigation published 4 February 2026,.

19. VIGINUM, *Rapport sur la menace informationnelle liée à l'intelligence artificielle* (Paris: SGDSN, February 2025).

20. VIGINUM, *Un-Notorious BIG: les opérations d'influence numérique du Baku Initiative Group* (Paris: SGDSN, December 2024).

21. European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (Brussels: EEAS, March 2025).

22. Décret n° 2021-922; consolidating Décret of 11 February 2026.

23. *Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères* (Institut des Hautes Études du Ministère de l'Intérieur, May 2024).

24. Stratégie nationale 2026-2030, *op. cit.*.

25. Gentil, *Disinformation Landscape in France*, *op. cit.*

26. UK Parliament, Joint Committee on the National Security Strategy, *How Malign Actors Are Seeking to Undermine Democracy*, report available at committees.parliament.uk.

Chapter 27: The United Kingdom

The UK recognises the evolving nature of hybrid and cognitive threats, but its response remains somehow conceptually fragmented and operationally misaligned.

While adversaries integrate influence, cyber, economic, and even kinetic tools to achieve cognitive effects, the UK still treats these domains separately - both in terminology and in practice. This results in a system that is strong in crisis response but insufficiently integrated, too slow, and overly reactive in the grey zone where these threats primarily operate.

At its core, the UK's challenge is not understanding the threat, but translating that understanding into a coherent, whole-of-system response that matches the speed, integration, and persistence of its adversaries.

Terminology and Framing

UK does not operate with a single unified conceptual framework. The terminology varies by community and function. "Hybrid threats" and FIMI (Foreign Information Manipulation and Interference) are the dominant operational terms, while "cognitive warfare" is recognised but not consistently applied.

There is also a notable analytical gap. Cognitive warfare is still largely understood as an information-domain activity rather than a strategic objective that can be pursued through multiple instruments. This is beginning to shift. The recognition that kinetic actions, such as attacks on Ukrainian energy infrastructure, are intended to degrade morale and social cohesion has broadened understanding. These are increasingly seen as cognitive effects achieved through physical means.

A competing conceptual framing is "political warfare," which some practitioners consider more useful. This approach captures the full spectrum: disinformation, sabotage, covert finance, organised crime networks, and proxy actors. Under this model, cognitive warfare and FIMI are components within a wider system rather than standalone categories.

Threat Actors

Russia is assessed as the primary threat in both intent and capability. Its methods range from traditional influence operations to more direct and less subtle forms of interference. Historical examples include political outreach networks and attempts to build influence within elite circles. Since 2022, many of these overt cultural and diaspora-linked channels have diminished, but Russia has adapted.

Recently the new head of Britain's foreign intelligence service MI6 warned that the UK faces an unprecedented convergence of threats from hostile states, cyber actors, and disinformation networks, arguing that the scale, speed, and complexity of today's security environment surpass anything seen in recent decades.[1]

A key shift is the use of AI-enabled targeting. What was previously broad segmentation is now precise micro-targeting, deployable rapidly and at scale. This, combined with a fragmented information environment, has significantly increased operational effectiveness.

Russian operations in the UK have consistently sought to exploit existing societal divisions rather than create entirely new ones. Their objective has generally been less about directly determining political outcomes and more about amplifying distrust, polarisation, and fragmentation within democratic debate. In this sense, influence operations are often assessed not by whether they changed votes directly, but by whether they intensified an already divided information environment.

This debate became particularly prominent during and after the Brexit referendum. Russian-linked media outlets and online amplification networks promoted divisive narratives around sovereignty, migration, elites, and distrust of institutions. However, the precise extent of Russian influence on the referendum outcome remains contested. Indeed, the UK Intelligence and Security Committee's Russia Report acknowledged evidence of Russian information activity and broader influence operations, but did not reach a definitive conclusion on whether these materially affected the Brexit result. It also criticised the lack of a systematic government assessment of possible interference at the time.[2]

As a result, the question remains active in UK practitioner and analytical debates. Many experts argue that the significance of Russian influence lies less in proving direct causality and more in understanding how hostile actors can exploit polarisation and open media ecosystems to deepen societal divisions over time.

China is assessed as a more sophisticated and restrained actor. Rather than overt disinformation, it relies on:

- Academic and institutional pressure;
- Transnational repression targeting diaspora communities;
- Narrative control through state-linked media.

Chinese operations tend to avoid visibility, though when they are heavy-handed, they can backfire and generate greater attention - Chinese heavy-handedness sometimes amplifies the attention it is trying to suppress.

Iran operates at a smaller scale but uses similar tactics to Russia, including bot networks, influence operations targeting trust and identity fractures, and potential links to illicit financial or smuggling networks that sustain activity.

The US is an increasingly sensitive dimension. While still structurally an ally, there is growing concern about:

- Political unpredictability;
- Influence from US-based oligarchs or platform owners;
- The ability to shape narratives through media, funding, and digital infrastructure

The US is now seen simultaneously as ally and potential source of cognitive risk. This reflects broader uncertainty about alliance reliability.

Institutional Architecture: Strength and Weakness

Crisis management system of the UK operates a distributed, whole-of-government structure, coordinated from the centre:

- The National Security Council sets strategic direction;

- The Cabinet Office ensures cross-government coordination;
- The National Security Secretariat integrates policy, intelligence, and crisis response.

Operational work is spread across intelligence agencies, departments, and specialised units. Key operational components:

- **Intelligence & Crisis Coordination:** MI5, MI6, GCHQ, COBRA: detection, attribution, and high-level crisis coordination (rapid, centralised, political decision-making); Electoral Commission (on election-specific disinformation);
- **Information Domain:** National Security Communications Team; Government Communication Service; Counter Disinformation Unit (strategic communication and disinformation monitoring); OFCOM (broadcast and social media regulation); the Department for Culture Media and Sport (legislation, broadcast, newspaper, and media disinformation);
- **External:** hybrid directorate in the Foreign Office (upstream identification and disruption of foreign state actors);
- **Cyber and Infrastructure:** National Cyber Security Centre; Centre for the Protection of National Infrastructure (cyber defence and critical infrastructure protection);
- **Domestic Response:** Counter Terrorism Policing; Home Office (disinformation action team, internal security and operational response);
- **Military:** 77th Brigade (information operations, mainly external).

Strengths of the UK system:

- Strong central coordination culture (Cabinet Office + NSC);
- High-quality intelligence integration;
- Ability to escalate quickly through COBRA;
- Experience in crisis management (terrorism, cyber, pandemics).

At the same time, this produces several systemic weaknesses (especially for hybrid/cognitive threats):

- **Fragmentation in day-to-day operations**: Coordination works better in crisis than in steady-state competition;
- **COBRA is reactive, not preventive:** It activates after escalation, not during slow-burn influence campaigns;
- **Lack of integration:** Each body operates within its mandate, leaving gaps between domains.
- **Limited integration of societal dimension:** No fully operationalised “whole-of-society” model like Finland.
- **Information domain still treated as secondary:** Compared to kinetic or cyber threats. The Security Service looks at discrete intelligence targets rather than social media campaigns. Previous practice impose caution on government use of intelligence assessments in public communications. This has made attribution slow.
- **Some units are chronically under-resourced:** For example, a disinformation action team in the Home Office.
- **Ineffective regulation:** Regulators have been reactive rather than proactive, particularly in dealing with state-backed media and platforms. For example, OFCOM is described as broadly ineffective, having issued repeated warnings to RT before eventually banning it only as part of the post-invasion sanctions package. On the other hand, the Online Safety Act is noted as a work in progress whose current focus has been on protection of minors and vulnerable groups rather than cognitive defence. Whether it will serve as an effective instrument against foreign information operations is an open question.
- **Capability mismatch:** Some departments lack the expertise or clearance to treat information operations as security threats rather than media issues. For example, the Department for Science, Innovation and Technology a structural

conflict of interest between attracting AI and platform investment and regulating the same platforms;

- **Bureaucratic and legal constraints:** Slow down real-time responses, especially domestically. Processes shaped by past intelligence failures prioritise caution, resulting in delays of months or years

Whole-of-Society Defence Gap

While recognised at the strategic level, whole-of-society defence is not operationalized, UK lacks:

- Institutionalised crisis roles for citizens;
- Regular interaction between government, industry, and society on security issues;
- Embedded elite socialisation around national security;
- Societal roles are not clear, and preparedness is not normalised.

Civic education is identified as the most critical missing layer. Without understanding how institutions function, citizens are more vulnerable to manipulation and conspiracy narratives.

The Princess of Wales's May 2026 visit to Italy, undertaken through the Royal Foundation Centre for Early Childhood, reflected a recognition by Buckingham Palace that early childhood is a foundation for healthier societies and, by extension, for societies better able to withstand cognitive pressure. Speaking after the visit, the Princess described the task of early childhood work as one of protecting and nurturing "the connections that form the foundations of life-long wellbeing." While this sits below the level of formal cognitive defence policy, it speaks to the same underlying logic: resilience is built across generations, not only in institutions.

At the same time, there were innovative proposals to build UK structure around civil society first, then governments. The logic is that civil society cooperation is harder for the US to object to on sovereignty grounds, and it paves the way for government-to-

government cooperation. The vehicle would be something like a democracy shield format, operating by qualified majority and purely voluntary, with Canada, UK, France, Germany, Sweden, Norway, Finland, and like-minded others as core members. Whether such a proposal will gain traction remains to be seen.

Best practice models are drawn from Finland and Estonia, particularly in digital literacy across all age groups.

Operational Capability Gaps

Attribution and response speed are major weaknesses. The current system cannot operate at the tempo required in the information environment.

Military capability, particularly the 77th Brigade, is not seen as a solution:

- Primarily offensive in orientation;
- Constrained by legal and bureaucratic approval chains;
- Too slow for real-time response;
- Limited in its ability to operate domestically.

Outsourcing to private contractors has introduced additional risks, including lack of accountability and unclear oversight.

Platform dependency is another vulnerability. Regulatory hesitation, combined with economic reliance on major tech platforms, limits the state's willingness to act decisively (the UK has a large enough advertising market and audience that it should be willing to use regulatory leverage against the platforms, including at the risk of friction with the US administration).[3]

Intelligence gaps exist in specific environments, notably platforms like Telegram, which are avoided for political or reputational reasons despite their operational relevance.

Reform Agenda (Emerging Thinking)

A reform direction is visible but not yet implemented. Key elements include:

- Building a true whole-of-society model tailored to national context;

- Developing rapid, real-time detection and response capabilities;
- Shifting government communication toward proactive exposure of hostile activity;
- Creating scalable civil resilience networks across regions;
- Strengthening legal and financial tools to disrupt hostile actors;
- Imposing stronger obligations on platforms, including enforcement mechanisms;
- Expanding research into the psychological effects of digital environments.

The UK House of Commons Foreign Affairs Committee report of 27 March 2026 ("Foreign Disinformation: The New Warfare," HC 703) recommends the UK establish a dedicated Disinformation Centre modelled explicitly on Swedish Psychological Defence Agency, French VIGINUM and Ukrainian Center for Countering Disinformation. The Committee Chair Emily Thornberry's "sitting ducks" framing and the report's assessment that the UK is in a "state of war" with Russia are both useful framings.

Allied Cooperation and External Dimension

Current alliance structures are seen as insufficient:

- **NATO** is constrained by political and structural limitations in the cognitive domain;
- **The EU** is more active but limited by internal divisions among member states. Despite no longer being an EU member, the UK is building strong and increasingly close relations with European partners on countering hybrid threats and on disinformation,
- **JEF** is noted as attractive but currently too military-focused and with internal resistance to expansion.[4]

As a result, there is growing interest in **coalitions of the willing**, potentially built through:

- Despite Brexit, the UK and the EU have expanded cooperation on countering hybrid threats and disinformation through joint initiatives on cybersecurity, foreign

information manipulation, election interference, and broader European security coordination frameworks;[5]

- The UK, together with France, has also taken a leading role in building the “Coalition of the Willing” in support of Ukraine;[6]
- Civil society-led cooperation as a precursor to government alignment;
- Platforms such as the Hybrid CoE in Helsinki;
- Expanded formats including non-EU partners (UK, Canada, Norway, etc.);

The preferred model is operational rather than declaratory: joint attribution, shared data, and coordinated responses.

Points of Convergence

Across sources, several conclusions are consistent:

- The institutional system is not fit for true purpose;
- Existing military capabilities are not an effective solution;
- Whole-of-society defence exists in rhetoric but not in infrastructure;
- Civic and digital education are the most critical missing elements;
- Geopolitical uncertainty, particularly around the US, is a growing destabilising factor;
- Cooperation with like-minded partners is essential, but current formats are inadequate;
- UK understands the threat but has not yet built the system to match it. The challenge is not awareness. It is integration, speed, and coherence.

Endnotes

1 Caitlin Danaher and Nick Paton Walsh, "UK's new spy chief warns the 'front line is everywhere' amid growing threat from Russia," CNN, 15 December 2025.

2 Intelligence and Security Committee of Parliament, Russia (HC 632, 21 July 2020).

3 "UK urged to break dependence on US technology giants," The Times, 19 April 2026.
4 Foreign Affairs Committee, House of Commons, "Foreign disinformation: 'the new warfare and open liberal democracies are sitting ducks,'" 27 March 2026.

5 Foreign Affairs Committee, House of Commons, From a Common Understanding to Common Ground: Building a UK-EU Strategic Partnership fit for the future, Third Report of Session 2024–26, HC 857 (4 March 2026).

6 House of Commons Library, "Proposals for a Coalition of the Willing in Ukraine," Research Briefing (8 January 2026).

Chapter 28: Poland

Poland demonstrates that democratic backsliding - politicisation of public media, erosion of judicial independence, and weakening of institutional checks and balances - does not irreversibly destroy cognitive defence capacity. Even after the rule of Law and Justice (PiS; a conservative-nationalist party) governing Poland from 2015 to 2023 that reshaped state institutions and increased political control over public broadcasting - the country retained sufficient operational capability, institutional depth, and civil society resilience.

The Polish case is therefore not one of uninterrupted resilience, but of **recoverability under pressure**. The decisive factor enabling this recovery has been sustained external threat awareness - primarily driven by Russia's actions since 2014 - which ensured that core analytical and operational functions continued even when the broader political environment deteriorated. While not fully repaired, Polish system is moving in a strategically coherent direction.

Threat Actors

Russia is the principal threat actor, responsible for sustained, large-scale campaigns aimed at undermining trust in institutions, weakening support for Ukraine, and exploiting domestic societal, ethical etc divisions. A notable example is the **instrumentalisation of the 2021–2022 Belarus migration crisis**, where Russian-linked narratives amplified fears of migrants, framed Poland as violating human rights, and simultaneously targeted EU cohesion.

A defining feature of the Russian operational pattern in Poland is the reuse of pre-existing information infrastructure rather than the creation of new networks. Analyses by NASK, the Polish Press Agency, the Polish-Japanese Academy of Information Technology, and FakeNews.pl have documented how the social media accounts and conspiracy networks built around anti-vaccine and anti-COVID narratives pivoted almost overnight to anti-Ukrainian content following Russia's full-scale invasion in February 2022. This pipeline effect illustrates the chapter's broader argument that hostile actors

exploit existing vulnerabilities rather than persuade, repurposing networks built around one grievance to amplify another.

Belarus acts as a secondary but closely aligned actor, particularly in the context of regional destabilization and operationalization of Russian narratives in politically sensitive contexts.

China plays a more limited but non-negligible role, primarily through **strategic narratives on technology, economic cooperation, and global governance**, rather than direct interference campaigns.

The effectiveness of hostile actors lies less in persuasion than in **exploitation of existing vulnerabilities** - polarisation, emotional narratives (migration, Ukraine, public health), and declining trust in media. Increasingly, these campaigns are augmented by AI-generated content, bot networks, and hybrid tactics linking information operations with cyber and physical disruption.

A concrete illustration came in June 2025, when a forged document attributed to the Ukrainian Ministry of Culture and an AI-generated video of Professor Andrzej Ossowski, head of the Volhynia exhumation works, were circulated through a fake account created nearly a year earlier. The content falsely claimed Ukraine had suspended exhumation rights in retaliation for Poland's establishment of a National Day of Remembrance. The fabrication was rapidly attributed and denied by both governments, but not before it amplified anti-Ukrainian sentiment online. The case demonstrates the fusion of AI-generated content, historical memory exploitation, and likely Russian opportunism around an emotionally loaded bilateral issue.

Polish societal resilience to Russian narratives has followed a clear temporal arc. In the early phase of the full-scale invasion, Poles demonstrated high resistance to Russian propaganda and broad willingness to shelter Ukrainian refugees. Resilience eroded as the war continued. Economic tensions in late 2023, particularly around Ukrainian grain transit and disputes affecting Polish farmers, alongside fatigue and shifting domestic politics, contributed to a measurable decline. By 2025, surveys indicated that negative attitudes toward Ukrainians outnumbered positive ones for the first time. The current

President is also less supportive of Ukraine than his predecessor. Support for Ukraine remains substantial in policy terms, but the societal foundation is no longer the uniform consensus of 2022.

What Makes Poland Distinctive

Poland's distinctiveness lies in the fact that its cognitive defence capabilities were **forged under real operational pressure rather than built as a purely policy-driven response**. Since 2014, Poland has continuously monitored and analysed hostile information activity, developing practical detection and attribution capabilities - most notably within the Research and Academic Computer Network (NASK, Naukowa i Akademicka Sieć Komputerowa), a state-supervised research institute operating under the Ministry of Digital Affairs and serving as the leading civilian analytical hub for disinformation monitoring.

A second distinguishing feature is that **operational continuity survived political disruption**. While the PiS period significantly politicised the media space, it did not fully dismantle the technical and analytical core of Poland's counter-disinformation system. Civil society remained active.

Third, Poland benefits from a **high level of threat awareness embedded in strategic culture**. Proximity to Russia, Belarus, and the war in Ukraine have anchored cognitive warfare firmly within national security thinking, rather than treating it as a secondary communications issue.

Coordination Architecture

Poland has developed a relatively dense and functional coordination architecture, combining civil, security, and crisis-management components.

At its centre stands NASK, particularly its Disinformation Analysis Center, functioning as the lead civilian body for monitoring, detection, and attribution. The **Internal Security Agency (ABW)** leads on counterintelligence, while the **Military Counterintelligence Service (SKW)** operates in the defence domain. The **Government Centre for Security (RCB)** coordinates crisis response and integrates threat information across institutions.

The **Ministry of Foreign Affairs** manages external strategic communication, while the **Ministry of Digital Affairs** has taken a leading role in election protection, notably through the 2025 presidential election protection programme “Parasol Wyborczy.” The Prime Minister’s Chancellery plays a coordinating role at the political level, while the President’s office contributes more selectively.

The Ministry of Foreign Affairs also established the Consultative Council for Resilience to International Disinformation in 2024, a 22-member advisory body drawing on NGOs, universities, local governments, and business, which held its first meeting in April 2025.

This system is **networked rather than centralised**, integrating state institutions with non-state actors.

Poland’s societal fight against disinformation is therefore a key component of this architecture. Organisations such as the INFO OPS Polska Foundation provide operational analysis of FIMI, while the Demagog Association focuses on fact-checking and public education. This is reinforced by actors like the Kościuszko Institute and media initiatives such as OKO.press and Konkret24, forming a pluralised societal layer that strengthens resilience.

The legal toolkit has also developed, though unevenly. Amendments to the Criminal Code in August 2023 introduced penalties for the spread of disinformation as part of espionage activity, providing prosecutors with a more targeted instrument than general defamation provisions. Poland is also implementing the EU Digital Services Act, with the head of the Office of Electronic Communications designated as Digital Services Coordinator, although the pace of implementation has lagged expectations.

Honest Limitations

Despite clear progress, Poland’s cognitive defence system faces several structural limitations.

First, the media environment remains partially politicised, and trust deficits persist. For example, public media reforms remain contested, and segments of the population

continue to perceive major outlets as politically biased, creating openings for disinformation.

Second, **political polarisation continues to act as a force multiplier**, including tensions between the President and the current government, which can slow decision-making and create inconsistent strategic messaging.

Third, Poland remains dependent on large technology platforms, whose cooperation is inconsistent. Even during the relatively successful **2025 presidential election**, not all flagged disinformation content was removed, highlighting a gap between national detection capacity and platform enforcement.

Fourth, **future threats are becoming more complex**, particularly with the rise of AI-generated content, deepfakes, and hybrid operations linking information, cyber, and physical domains.

Institutional Architecture

Poland's cognitive defence operates as a **multi-layered system integrating both state and societal efforts**.

At the analytical layer, NASK and expert NGOs such as the INFO OPS Polska Foundation monitor, detect, and analyse hostile information activity.

At the security layer, the Internal Security Agency (ABW, Agencja Bezpieczeństwa Wewnętrznego) and the Military Counterintelligence Service (SKW, Służba Kontrwywiadu Wojskowego) translate these insights into counterintelligence and protective measures.

At the coordination layer, the Government Centre for Security (RCB, Rządowe Centrum Bezpieczeństwa) and central government structures integrate responses across institutions.

At the policy and strategic communication layer, the MFA and other ministries shape narratives and engage internationally.

Crucially, at the societal layer, organisations such as the Demagog Association, independent media, and think tanks actively expose disinformation, educate the public, and sustain democratic resilience.

This distributed model is a key strength: resilience does not depend on a single institution but on **interaction between state capacity and societal engagement**. It is conceptually close to what is known as the whole-of-society concept. Mapped onto the report's six-layer architecture set out in Figure 1, these functional layers correspond principally to Layers 4 through 6, detection and attribution, active defence, and sovereign response capacity, while the societal layer reaches down into the foundational Layers 1 and 2, societal cognitive capacity and the integrity of the information environment.

Partner Landscape

Within the Weimar Triangle (Poland–France–Germany), there is renewed focus on disinformation and resilience. Poland is widely seen as the most proactive actor, though the format still struggles to translate political intent into sustained operational output, with France often viewed as a more reliable partner than Germany.

Regionally, Poland operates within a **frontline cooperation network** with Lithuania, Ukraine, and other Eastern flank states, where threat perceptions are aligned and practical experience is shared.

At the EU level, Poland is integrated into regulatory and coordination frameworks, particularly regarding platform governance, though effectiveness depends on enforcement.

Within NATO, cognitive warfare and resilience are increasingly recognised as core security challenges, and Poland actively contributes to this agenda.

Overall, partnerships reinforce Poland's capabilities but do not substitute for strong national systems -especially given the speed, scale, and specificity of the threats it faces.

Cross-Cutting Analysis

Chapter 29: Lessons Across Cases

This chapter sits at the close of the country evidence base. Its job is the analytical work that cannot be done from any single chapter, the work that only becomes possible once thirteen cases have been read alongside one another. Restating the country chapters is not the point. Surfacing the cross-case insights that emerge only from the comparison is.

The thirteen country cases of this report constitute the cluster from which this synthesis works. One case carries a particular evidentiary weight inside that cluster and should be named at the outset. The Ukrainian operational experience is the foundational evidence base from which several of the framework's core claims are derived: that adversary cognitive operations succeed by amplifying existing fractures at population scale rather than by introducing new ones, that kinetic and cognitive operations operate as a single integrated campaign in adversary doctrine, that civil society functions as the load-bearing substrate of cognitive defence under sustained pressure rather than as a supplement to state capacity, and that cultural production operates as foundational infrastructure rather than as adjacent enrichment. The other cases corroborate, complicate, or extend those claims. This synthesis chapter holds them together.

Foundations precede architecture

The single most consistent finding across the cluster is that the strongest cognitive defence architectures sit on foundations that were not built for security. The deepest of these foundations is one no democracy in the cluster names as cognitive defence infrastructure at all. The operational mechanism by which adversary cognitive operations succeed runs through acute emotional arousal: fear, outrage, or moral disgust takes the prefrontal cortex offline, and access to logic, reasoning, empathy, and forward thinking degrades. The framework chapters develop this through Kruglanski's seizing-and-freezing mechanism and the neuroscience documented by C. Sue Carter on the oxytocin and threat-physiology relationship. Adversaries design operations to trigger this state because reaction forecloses reflection. The defensive answer is the

capacity to notice the spike of arousal, pause before acting on it, and ask whether the response was engineered to produce exactly the reaction the citizen was about to have. This is not therapy dressed as policy. It reflects the recognition that adversaries exploit an emotional rather than purely informational attack surface, and that the population-level capacity to regulate emotional responses under deliberate cognitive pressure forms the foundation of the broader resilience architecture.

Denmark operationalises this capacity through Klassens Tid, which is the cluster's most worked operational example of emotional regulation as foundational cognitive defence infrastructure. Klassens Tid is embedded in the Folkeskole (the Danish public school system from year one through year ten) and is therefore government policy, even though Denmark does not name the work as security policy. No other government in the cluster recognises emotional regulation as cognitive defence infrastructure. No national architecture invests in it as such. Civil society programmes in the cluster's countries do related developmental work, including Roots of Empathy, a Canadian civil society organisation founded by Mary Gordon in 1996 that operates in more than 3,000 classrooms across Canada and internationally, but these are civil society practices rather than recognised components of national cognitive defence architectures, and they are not resourced or framed as security infrastructure by the governments under which they operate. The Sapien Labs Global Mind Health Report, drawing on survey data from more than one million respondents across 84 countries, documents measurable decline in emotional regulation capacity among adults under 35 across the preceding five years, with the trend concentrated in high-income democracies.[1] The reason this matters is that adversary cognitive operations target perception of reality, and perception is shaped by emotional state: a population whose capacity to regulate emotional response is declining is a population whose perception of reality is increasingly available to manipulation. This decline expands the cognitive vulnerabilities that adversary operations exploit most effectively, while the architectures democracies have built remain poorly suited to counter them. This is the cluster's deepest finding: the foundation everyone is defending is the foundation no one has named.

Beyond emotional regulation, four cases lead on different aspects of the visible foundation, each on a different aspect of what the framework calls the dual foundations: Denmark on social infrastructure, Finland on the framework as a whole, France on the doctrinal articulation of cognitive defence as strategic priority, and Ukraine on cultural-resistance foundation and head-of-state communication under sustained operational pressure. Each lesson is different, and the differences matter.

Denmark leads on societal resilience among its citizens, the foundation layer beneath everything else the architecture rests on. Denmark is a leader within a regional Nordic cluster that already does this well, with the folk high school tradition, the associational tradition, and the broad-social-trust outcome regionally distributed across the Nordics rather than uniquely Danish. What is particularly Danish, against this regional baseline, is *almene boliger* (decommodified housing organised through non-profit associations) at scale, *bofællesskab* (the cohousing tradition that produced the world's first modern intentional cohousing communities), Klassens Tid as the operational expression of emotional regulation already discussed, and the deliberate redesign of public space through Cities for People. The 2022 wave of the Integrated Values Survey records 74 percent of Danes agreeing that most people can be trusted, the highest figure in the world, ahead of Norway at 72 percent and Finland at 68 percent, the cumulative outcome of design choices made over generations to address Danish problems, none of them adversarial cognitive operations.[2] Denmark does not name any of this as security infrastructure. The country that has done the most to build the societal resilience foundation has the least developed institutional vocabulary for recognising what that foundation is and what threatens it. Standardisation pressure on the Folkeskole, financialisation pressure on housing, privatisation pressure on public space, and bureaucratisation pressure on associational life are pressures from outside the security frame, and the cognitive defence consequence is that the architecture protecting Denmark's foundation is not engaged when the foundation is under threat, because the threat is not framed as security-relevant. The non-recognition pattern is universal across the cluster. Failure to recognise existing government investments and societal structures as part of the broader collective security architecture is a failure almost every democracy in the cluster shares. That the leading case carries this failure most acutely

is the cluster's clearest warning to every other democracy investing in cognitive defence architecture. Denmark already does the most, and Denmark does not see it.

Finland leads on the framework as a whole. Where Denmark holds the social infrastructure foundation, France holds the doctrinal articulation, and Ukraine holds the operational architecture under sustained pressure, Finland is the case where both foundations hold up together and the architecture above performs accordingly. *Kokonaisturvallisuus*, the Finnish comprehensive security concept, organises Finnish societal preparedness across seven vital functions of society (leadership, international and European Union activities, defence capability, internal security, economy and infrastructure, functional capacity of the population, and psychological resilience) and is the cluster's most fully institutionalised whole-of-society framework. Its operational backbone is the Security Committee under the Ministry of Defence, which brings together ministries, security agencies, business actors, critical infrastructure operators, and civil society to coordinate preparedness, crisis response, hybrid threat resilience, and societal continuity across sectors. The Committee functions less as a command structure and more as a permanent coordination and planning mechanism for whole-of-society resilience. Alongside it, the Diamond model of cross-party convening on national security, the National Defence Courses that have socialised over 10,000 senior decision-makers across politics, civil service, business, media, and civil society into a shared threat assessment, the Foreign Affairs Committee meeting on dates established by law rather than by political convenience, and the Intelligence Oversight Committee with statutory cross-party access produce the kind of elite coherence across electoral cycles that the framework's political-will foundation requires. Finnish civic-duty culture, the embedded media literacy that is the cumulative outcome of a thirty-year political commitment, and the Finnish disposition itself, calm under pressure, with a level of trust in institutions that is unusual by Western standards, together produce a society in which adversary operations have less to attach to than they would in any other case in the cluster. Finland is the reference case for the framework overall.

France leads on the doctrinal articulation of cognitive defence as a strategic priority and on the institutional architecture that backs it. President Macron's Berlin speech

advancing European cognitive sovereignty as a continental project, the 2026-2030 National Strategy, VIGINUM as the cluster's reference detection institution, the *Riposte française* doctrine, and the Information Manipulation Spectrum methodology now adopted as the European Union's analytical standard through European External Action Service partnership together constitute the cluster's most fully developed articulation of cognitive defence as a strategic priority, with the institutional architecture to match. France is also the cautionary inverse: the architecture is built and the doctrine is articulated, and yet the architecture does not reach the foundation underneath it. The CEVIPOF *Baromètre de la confiance politique*, fielded in February 2026, recorded 22 percent trust in politics, 17 percent trust in government, 20 percent trust in the National Assembly (matching the December 2018 *gilets jaunes* historical low), 18 percent trust in the President, and 15 percent trust in political parties; 87 percent said political leaders do not care about citizens; 60 percent reported that they cohabit rather than live in a united nation.[3] The 2026-2030 National Strategy's Pillar 1 commits France to building societal resilience through media literacy, civic engagement, and the VIGINUM Academy. Pillar 1 reaches only a component of the social infrastructure foundation and of the layer-one work the framework requires. The broader work that would repair France's fracturing social safety net sits entirely outside the cognitive defence architecture. Pillar 1 is not the fix. France is the case that proves the architecture and tools, however well built, do not on their own restore the foundation they were built to protect.

Ukraine leads on cultural-resistance foundation and on head-of-state communication under sustained operational pressure. The cultural-resistance foundation is the deepest layer of Ukrainian cognitive defence, and it is a different kind of foundation from the social-infrastructure foundation Denmark exemplifies. A population sustained by cultural production, moral integrity, language, and everyday-life continuity under sustained kinetic threat is structurally harder to manipulate than a population without that substrate, because the population's underlying identity is anchored in a cultural inheritance adversary operations cannot reach. The institutional architecture sustaining this work is substantial: the Office of the First Lady's Global Coalition of Ukrainian Studies across sixty institutions in twenty-three countries, the Ukrainian Bookshelf

project at over two hundred universities, Books Without Borders distributing more than a quarter of a million Ukrainian books to displaced children across twenty countries, and the active decolonisation work disentangling Ukrainian studies from inherited Slavic and Russia studies frameworks. The transferability finding is that cultural investment is security commitment, and democracies that have under-invested in cultural production, arts funding, and the institutional infrastructure of cultural and civic life have left a foundational attack surface that no operational architecture built on top of it can close. Other democracies should aspire to comparable investment, adapted to their own conditions and historical inheritance. Ukraine also leads on head-of-state communication under operational pressure. The Zelenskyy architecture during the war's first years integrated three communicative registers (pragmatic interest, ethical values, and emotional connection) calibrated continuously to evolving audiences in the United States, the European Union, and the Global South. This is a different category of head-of-state work from France's. France's lesson is about doctrine and institutional architecture sustained across the political cycle. Ukraine's is about communication discipline under pressure and continuous calibration to audiences whose attention and political will cannot be assumed. The cluster has both. The synthesis holds them distinct.

The four lessons combine into the chapter's central observation on transferability. The Nordic-Baltic cases share family resemblance through their whole-of-society security doctrines, but they are not the same model. Each has been adapted to its own constitutional structure, institutional history, threat geography, and political culture. The transferability question is therefore not which configuration travels, because no single configuration is on offer. The question is which elements work for the country in question, given its cultural, geographic, economic, and societal mix.

Sweden warrants separate development on this point. The Swedish Psychological Defence Agency is built around an empowerment doctrine: better democratic citizens in the digital age, not better digital citizens. The citizen is the cognitive defence unit and the agency's job is to equip the citizen, not to do the defence on the citizen's behalf. MPF integrates analysis and outreach inside a single civilian body precisely because

the empowerment doctrine treats the two as inseparable: detection and attribution exist to feed the public-facing work that equips Swedish citizens, not as an independent end. The doctrinal commitment is what shapes the institutional design, not the other way around. The comparison with France is the analytical key. France protects democracy by attributing and exposing adversary operations through state institutional capacity; Sweden protects democracy by equipping citizens to recognise adversary operations themselves. These are two different theories of cognitive defence, not two equivalent institutional choices. VIGINUM specifically is purpose-built for detection and active defence, with population-facing work distributed across other parts of the French architecture (Pillar 1's media literacy commitments, the VIGINUM Academy as the educational outreach arm, the broader public communication work of SGDSN and ARCOM). Sweden built MPF to integrate analysis and outreach in one body because empowerment requires both functions to work together; France built VIGINUM to do detection and active defence at depth and distributed the empowerment work to other vehicles. Both are legitimate; the difference is doctrinal, and the institutional form follows from the doctrinal choice.

Other transferable elements travel differently. Lithuania's calibrated rating system is a procedural design any democracy can adopt. Lithuania's Elves could also serve as a model for other countries in defending against cognitive attacks by demonstrating how organised civic networks can rapidly identify, expose, and counter disinformation while strengthening societal resilience from the bottom up. Latvia's legal architecture for active defence travels conditionally with the procedural democratic legitimacy that makes it work as the binding adoption condition. Estonia's citizen-as-owner constitutional foundation and transparency-as-strategic-posture doctrine are political-decision-level commitments any democracy can, in principle, adopt. Norway's household preparedness architecture, with civil-defence materials reaching every home annually, the 2026 Total Defence Year programme running across approximately 400 municipalities, and the *Egenberedskap* tradition treating citizen self-preparedness as part of national defence, travels as a commitment to preparedness at population scale. Finland's thirty-year integration of media literacy into mother-tongue education does not travel as an integration, though media literacy itself does. Some elements do not travel

as institutional forms at all and travel only as diagnostics: the high-trust substrate the Nordic models rest on, the existential-threat conditioning that produced Ukrainian civil society capacity, the 180-year accumulation that produced Danish interpersonal trust at 74 percent.[4]

Adversaries do not start fires

The cluster's second most consistent empirical finding is that adversary cognitive operations succeed at population scale by exploiting existing fractures rather than by introducing new ones. The Ukrainian chapter states this most directly. At population scale, Russia does not start the fires it exploits; it identifies fires already burning inside target societies and amplifies them. The distinction between population scale and kinetic operations matters: Russia conducts kinetic ignition where it serves operational objectives, including the documented arson and sabotage campaign across European Union member states since 2023. The amplification-rather-than-ignition pattern is specifically the population-scale finding. The pattern is corroborated across the cluster. Polish anti-vaccine and anti-COVID networks pivoted almost overnight to anti-Ukrainian content after February 2022, repurposing networks built around one grievance to amplify another.[5] Russian operations in Lithuania attached to Soviet nostalgia among older, economically marginalised, and Russian-speaking constituencies and to the Litvinist narrative emanating from Belarus, which adds a cultural-historical dimension the standard Russia-focused responses cannot address. Operations against Latvia have shifted since 2022 from the Russian-speaking community to the Latvian-language audience, disseminated through local Latvian-language intermediaries because the direct Russian state-broadcast vector was closed by the National Electronic Mass Media Council's 2022 channel bans.[6] Operations against Norway concentrate on Finnmark, where distance from Oslo makes national coherence hardest. Operations against the United Kingdom attached to genuine divisions around sovereignty, illegal migration, elites, and distrust of institutions during and after the Brexit referendum. Operations against Canada have attached to the Alberta convergence, which exists because of grievances domestic to Canadian political life that information operations did not create.

What this implies for what cognitive defence can and cannot do is the more important point. Cognitive defence does not stop adversary operations. It reduces the surfaces those operations can attach to, the depth to which they penetrate, and the speed at which they propagate once attached. The architecture is therefore inseparable from the conditions of the receiving society. Detection and attribution close the propagation gap. Legal architecture raises the cost of operating on the platform side. Active defence imposes consequences on the adversary. None of these tools reduce the surface area itself. Reducing surface area is the work the foundation layer does, slowly, over generations, through housing, education, civic infrastructure, local media, social trust, cultural production, emotional regulation capacity, and the political will to invest in these things at the right horizon. The essence of cognitive defence, in this reading, is upstream work on societal, economic, and other structural vulnerabilities before hostile actors can exploit them.

Two framework findings the cluster surfaces

The cluster confirms the framework Volume I develops at the level of functions and dual foundations. The six functional layers are recognisable in every case. The horizontal foundations of social infrastructure beneath and political will above are the binding variables across the cluster. Two findings the cluster surfaces deserve explicit treatment because they are framework-shaping rather than complications inside the framework, and the Ukrainian case is the foundational evidence for both.

The first is civil society as the load-bearing substrate of cognitive defence rather than as a supplement to state capacity. From 2014 through 2021, Ukrainian civil society carried the cognitive defence function alone, with no Centre for Countering Disinformation, no Centre for Strategic Communication, and no operational architecture inside the National Security and Defence Council with responsibility for the cognitive domain. StopFake was founded in March 2014 at the Mohyla School of Journalism in the immediate aftermath of the Russian annexation of Crimea; the Ukraine Crisis Media Centre was founded in February 2014 in response to the institutional vacuum following Yanukovych's departure; the Hybrid Warfare Analytical Group was established within the Centre in 2017, four years before any Ukrainian state institution formally assumed

responsibility for cognitive defence work. The state institutional architecture that has emerged since 2021 has not displaced the civil society substrate. It sits on top of it. The operational integrity of the civil society function depends on its institutional separation from the state apparatus, which is why the Ukrainian funding architecture is structured around international, commercial services, and philanthropic funding rather than direct state funding. The Polish case demonstrates the same load-bearing role from a different angle: civil society analytical capacity sustained democratic resilience independent of the political environment, with INFO OPS Polska, Demagog, the Kościuszko Institute, OKO.press, and Konkret24 continuing to carry the function through the 2015 to 2023 period when state institutions were politicised. The Lithuanian Elves volunteer network, scaled internationally including through the North Atlantic Fellas Organisation, demonstrates civil society architecture that operates beyond national borders. The Estonian case shows civil society playing the role state institutions cannot, with Propastop functioning as the credible counter-disinformation voice in Russian-language space because it is operationally independent of the Estonian state. The implication is operational: the Ukrainian civil society architecture from which much of the cluster's evidence is derived is currently degrading, with United States withdrawal of counter-disinformation funding decimating significant portions of the ecosystem. StopFake survives through a commercial services funding model that subsidises its public-interest work; most Ukrainian counter-disinformation organisations cannot build comparable models and are scaling down, with some closing entirely. The capacity democracies might learn from is being lost in real time.

The second is kinetic-cognitive integration. For democracies under sustained operational pressure, the layers integrate into a single fused architecture rather than remaining analytically separable. The Ukrainian case is the foundational evidence. The civic-digital infrastructure (Diia, eVorog, Brave1), the kinetic operations infrastructure, and the cognitive defence infrastructure are no longer separate domains administered through separate ministries; the January 2026 appointment of Mykhailo Fedorov, architect of Ukraine's civic-digital infrastructure, as Minister of Defence, with Mstyslav Banik, the launch lead for Diia, appointed Deputy Minister of Defence in March 2026, formalises at the cabinet level what was already happening operationally. The

integration is not a Ukrainian institutional quirk to be admired. It is the recognition that Russian operational doctrine integrates kinetic and cognitive operations against adversary decision-making as a single problem, and that democracies maintaining the inherited Western institutional separations between civilian and military, kinetic and cognitive, digital and physical are operating inside frameworks adversary operations have been designed to defeat. The Ukrainian case also produces two methodological contributions that the cluster surfaces as framework-shaping rather than country-specific: the application of kill-chain methodology to adversary information-operations infrastructure rather than to discrete narratives, and the development of narrative intelligence as an emerging analytical discipline analogous to signals intelligence or human intelligence, producing operational indicators of adversary intent and capability through systematic tracking of narrative volume, intensity, and pattern over time. The transferable finding is not the specific Ukrainian wartime cabinet fusion. It is the underlying recognition that kinetic and cognitive operations are not separate domains administered by separate institutions, and that the institutional separations Western democracies have inherited are themselves the operational vulnerability adversary doctrine has been designed to exploit.

Three universal institutional gaps the cluster surfaces

Three institutional gaps recur across every case in the cluster with sufficient regularity to warrant naming as universal rather than national.

The first is reactive strategic communications. Lithuania carries the cluster's most disciplined work on this question and the most honest reckoning with the trade-offs the discipline creates. Lithuania's National Crisis Management Centre, established in 2023 under the Prime Minister's Office, is the cluster's clearest case of central coordination paired with head-of-government authority. The Lithuanian rating scale that ignores narratives below the two-of-ten threshold avoids amplifying adversary content through official response and is the cluster's mature example of communication discipline as the operational corollary of detection capacity. The Lithuanian chapter also highlights a trade-off that no other case in the cluster addresses as explicitly: the more effective institutions become at countering disinformation, the weaker individual incentives may

become to verify information independently, creating what the chapter terms the "passive citizen" problem. Latvia names the broader pattern most directly. The Latvian Military Intelligence and Security Service's first detailed public threat assessment appeared in 2025, years after comparable Estonian and Lithuanian publications, because the intelligence culture had historically prioritised operational security over public threat communication. Estonia's Narva People's Republic amplification paradox in March 2026 demonstrated that detection paired with calibrated response doctrine, what gets named, at what threshold, in what framing, to what end, is the next generation of architecture the cluster's strongest cases must now develop. France's Matryoshka case in February 2026 demonstrates that even the cluster's strongest detection-and-attribution apparatus is operating reactively against the cadence of operations now running. The United Kingdom case identifies forward narrative capability as a missing layer. Germany operates an extensive analytical and counter-narrative ecosystem that remains, in operational terms, reactive against the AfD's parliamentary capacity to inject adversary frames into the legitimate political conversation. No country in the cluster has built proactive forward narrative capability at the speed and scale required, and most have not begun to try.

The second is the measurement problem. No democracy examined has solved the problem of measuring cognitive defence effectiveness. What can be assessed is readiness, and what can be compared is relative capability. This is sufficient basis for learning across cases even without validated outcome metrics. The cluster contains four kinds of measurement evidence, each useful but each limited. Input metrics document that institutional capacity exists. Process metrics document detection speed, attribution accuracy, coordination effectiveness, and public communication reach. Resilience proxies document the social-infrastructure and trust indicators adversary operations target. Comparative benchmarking documents how architectures perform relative to each other. What no country has is validated metrics proving its cognitive defence investments prevented specific adversary successes. Norway can point to the failure of the pro-Russia party formation in the September 2025 election, which the Norwegian chapter attributes to visibility-as-defence rather than to the full architecture's operational performance. France can point to diplomatic and sanctions costs imposed on

adversaries through public attribution. None of these is causal proof. The counterfactual question, what would have happened if the architecture were not in place, cannot be answered by any country in the cluster. The measurement gap is not a methodological irritation. It is a structural feature of the domain, and democracies that pretend otherwise are setting themselves up for a credibility crisis when the architecture meets its first serious failure.

The third is terminological fragmentation. Every country in the cluster uses different working vocabulary for the same problem. Finland prefers societal security and information influence; Sweden centres psychological defence; Norway works under *sammensatte trusler* (composite threats); Denmark mixes cognitive resilience, FIMI, and information warfare across institutions; Estonia works under *Lai Riigikaitse* (broad national defence) without using cognitive warfare institutionally; Latvia operates under influence operations countered by strategic communications; Lithuania uses hybrid threats with disinformation and information operations as practical categories; France uses *ingérences numériques étrangères* (foreign digital interference); the United Kingdom operates without a single unified conceptual framework; Poland uses cognitive warfare with greater institutional comfort than most; Ukraine uses kinetic-cognitive integration as the operational frame; Germany uses *Desinformation* and *hybride Bedrohungen* (hybrid threats), with the Federal Ministry of the Interior and the Federal Ministry of Defence operating different working vocabularies; and Canada uses foreign interference and disinformation as its primary lexicon, with the term cognitive warfare not yet officially institutionalised. EU DisinfoLab's comparative analysis of disinformation across twenty European Union member states identified the absence of standard terminology as a structural impediment to coordinated policy monitoring, recommending that cooperation start from shared definitions.[7] Nevertheless, at the EU and NATO levels there is an institutional consensus around the use of the term "hybrid threats," even if the term is not always used consistently at the national level, which in turn also creates terminological confusion. The fragmentation itself is a coordination cost: practitioners need to translate continuously across vocabularies even when they share threat assessments and operational practices. The terminological consolidation for cognitive defence will not arrive through institutional fiat at the European level, because

each country's vocabulary is grounded in its own legal frame and operational culture. It is more likely to arrive through NATO doctrinal recognition. NATO's work to recognise cognitive warfare as a doctrinal term unlocks the funding streams, institutional adaptation, and alignment incentives that drive terminological consolidation in practice rather than in declaration. Once recognised at NATO, member states adapt to access the funding and shared analytical product the recognition makes available. The methodological consolidation underway through the European External Action Service, with the Information Manipulation Spectrum framework adopted as the analytical standard and the January 2026 *Building a Common Operational Picture of FIMI* report establishing shared method, is the operating workaround for terminological consolidation while NATO's doctrinal work continues.

Conclusion

The cluster's findings, read together, point to cognitive defence as a layered architecture resting on foundations no democracy yet recognises as security infrastructure. The deepest of these foundations, the population-level capacity for emotional regulation, is the most universally absent and the most operationally consequential, and is the foundation on which every other layer above depends. The visible foundations of social infrastructure, cultural production, civic association, and the political will to sustain investment in them across electoral cycles are the work generations of democratic development have already produced in some cases and have hollowed out in others. The architecture described across these two volumes is buildable, and the cluster contains the institutional templates and operational doctrines through which to build it. The foundation is the harder problem, and the recognition that the foundation is what is being defended is the first step every democracy in this cluster and beyond has yet to take.

Endnotes

1 Sapien Labs, *Global Mind Project Annual Reports*, at sapienlabs.org.

2 Gert Tinggaard Svendsen, *Trust* (Aarhus University Press, 2014), drawing on Integrated Values Survey data.

3 Centre de recherches politiques de Sciences Po (CEVIPOF), *Baromètre de la confiance politique, Vague 17*, published 9 February 2026, at sciencespo.fr/cevipof.

4 Gert Tinggaard Svendsen, *Trust* (Aarhus University Press, 2014)

5 NASK, the Polish Press Agency, the Polish-Japanese Academy of Information Technology, and FakeNews.pl, documented in the Polish chapter of this volume.

6 Field research, Riga, January 2026, as documented in the Latvia chapter of this volume; NEPLP institutional record at neplp.lv; & Monika Hanley, *The Disinformation Landscape in Latvia*, version 2, EU DisinfoLab, August 2025, at disinfo.eu.

7 Maria Giovanna Sessa, *Connecting the disinformation dots: insights, lessons, and guidance from 20 EU Member States* (EU DisinfoLab, 5 December 2023), at disinfo.eu.

About the Author



Elizabeth Anderson is a Canadian researcher in cognitive warfare and democratic defence. Her research examines how authoritarian actors employ grey-zone and cognitive warfare to subvert democratic cohesion and political will, developing whole-of-society frameworks for democratic resilience grounded in comparative field research across thirteen countries and over one hundred interviews with senior government, military, and civil society officials. Her work spans transatlantic security, Ukraine's defence, Canada's strategic partnerships in an era of shifting alliances, and the intersection of emerging technologies with national security.

She previously served as Director of Operations and Senior Advisor for International Security to Canada's Minister of Foreign Affairs, where she was among those leading Canada's policy response to Russia's full-scale invasion of Ukraine. She brings over seven years of experience across multiple Government of Canada portfolios. As a Fulbright Scholar, she was a visiting associate fellow with the Transatlantic Security Program at the Center for a New American Security. She holds an MA in Global Risk from Johns Hopkins School of Advanced International Studies.

She served as contracted Research Director for the project Cognitive Warfare: A Democratic Defence, produced with Konrad-Adenauer-Stiftung Canada, and is a Fellow at the Montreal Institute for Global Security.

About the Distinguished Advisor



Ambassador Eitvydas Bajarūnas is a Lithuanian diplomat and international security expert with more than three decades of experience in foreign policy, NATO and EU affairs, hybrid threats, and Baltic-Nordic security. He served as Lithuania's Ambassador to the United Kingdom, the Russian Federation, and Sweden, as non-resident Ambassador to Portugal, Oman, and Uzbekistan, and earlier as Consul General in Saint Petersburg and Deputy Head of Mission at Lithuania's Representation to NATO.

Within Lithuania's Ministry of Foreign Affairs he served as Political Director, leading EU foreign and security policy, and as Ambassador-at-Large for Hybrid Threats, where he coordinated Lithuania's pioneering work on non-conventional threats. He was Diplomatic Adviser to the President of Lithuania and served on the Steering Board of the European Centre of Excellence for Countering Hybrid Threats in Helsinki. He is a Senior Fellow with the Democratic Resilience program at the Center for European Policy Analysis (CEPA) and the author of numerous articles on Russia's foreign and security policy, hybrid threats, and Baltic and Nordic security.

He holds an MA in War Studies from King's College London and a Diploma in Applied Mathematics from Vilnius University. He has received state honours from Lithuania, Sweden, Estonia, and Portugal, including the Knight's Cross of the Order of Merit for Lithuania.