

EUROPE'S NEXT AWAKENING

China – the Enabler and Hybrid Actor

A Close-Up on Northern and Western Europe

Editor: Anna Rennéus Guthrie

**Authors: Dr Una Aleksandra Bērziņa-Čerenkova,
Ferdinand A. Gehringer, Patrik Oksanen, Luke de Pulford,
Jeanette Serritzlev**



Contents

Foreword from Stockholm Free World Forum (Frivärld)	5
Why Getting China's European Story Right Matters	8
Beyond an Alliance: The Sino-Russian Relationship	19
Murky Waters: Latvia's Strategic Communications on Kinetic Maritime Threats	32
Access as Influence: China's Strategic Embeddedness in Germany	42
Beyond the Mirage: A Decade of UK-China Relations and the Price of Asymmetry	60
Chinese Influence and Espionage Activities in Denmark	67
Conclusion & Recommendations	79
Afterword from Konrad-Adenauer-Stiftung	82

Copyright: Stockholm Free World Forum (Frivärld)
& Konrad-Adenauer-Stiftung
ISBN: 978-91-988500-5-5
Publisher: Frivärld, 2026



Foreword from Stockholm Free World Forum (Frivärld)

The Russian threat for Europe is not only evident but also more or less immediate. Extensive warfare is already being conducted in the shadows of the grey zone, in the form of what is commonly referred to as hybrid warfare.

Russia, however, does not stand alone. Only weeks before the invasion, Moscow and Beijing proclaimed a partnership ‘without limits’, and China has since become the decisive enabler of Russia’s war.

In 2024, Stockholm Free World Forum (Frivärld) published the report *Tracking the Russian Hybrid Warfare – Cases From Nordic-Baltic Countries* which in 2025 was developed into the anthology *Russia’s Hybrid War: The Northern Front* (Stockholm Free World Forum, Konrad Adenauer-Stiftung 2025).

The writings demonstrated the mechanisms and methods of Russia’s hybrid war in the Nordic Baltic region. One of the principal objectives of Russian hybrid warfare is to undermine support for Ukraine and to promote a narrative in which the war is attributed to a wide range of supposed causes for which Ukraine itself is held responsible.

The methods used are however not unique for Russia. The same grey-zone toolkit of disinformation, elite capture, and the deliberate creation of economic and technological dependencies is employed by China on a global scale and with far greater resources. Though China usually acts in quieter and more patient forms. Where Russia confronts, China cul-

tivates. The two increasingly operate in parallel, and at times in concert, against the same target of open and democratic societies.

There is now widespread awareness both of the Russian threat to Europe and of the forms of warfare through which it is being pursued. For the foreseeable future, this will remain one of the defining issues of European politics. It is China, as the following chapters show, that stands increasingly behind Russia, and increasingly above it.

China poses a global threat and aspires to global dominance. Since Russia's full-scale invasion of Ukraine, China has become an increasingly important partner for Russia and, in practice, by far the stronger of the two. Over the past fifteen years, the Russian economy has largely stagnated, while China's GDP has almost tripled.

China seeks to achieve global dominance through its economic strength and military capabilities. By 2027, China aims to possess armed forces sufficiently powerful and modernised to give it full freedom of action regarding the seizure of Taiwan. By 2035, it intends to have the world's most modern military, and by 2049 it seeks to be the world's leading global power. In the longer term, China represents the principal threat to free nations and democracy, and its ambitions extend far beyond regional dominance. While Russia's stagnant economy is steadily weakening the country, China's economic strength provides the foundation for imposing totalitarian demands on other parts of the world.

In this anthology, Stockholm Free World Forum, in cooperation with the Konrad Adenauer Foundation, brings together leading experts on hybrid warfare to examine how China is already projecting this threat in the grey zone. They show how a totalitarian state governed by the logic of dictatorship mobilises all sectors of society behind its ambitions: Chinese companies and researchers ultimately operate as extensions of the Communist Party's global aims.

This threat is already real and present. China deliberately exploits the openness of democratic societies and market economies. Unlike Rus-

sia, however, it generally does so through non-confrontational means. It seeks instead to cooperate with institutions in democratic societies and to use the openness of their economies to create growing dependencies and accumulate political influence.

In response, Europe must develop the necessary strength, together with other free nations, to compel China to respect the sovereignty and integrity of democracies. This is a challenge that must be confronted today. And that is what this anthology is about.

Gunnar Hökmark

Chairman Stockholm Free World Forum (Frivärld).

Why Getting China's European Story Right Matters

Anna Rennéus Guthrie

The inability to foresee the future is truly both a gift and a curse humans have been aware of since our early self-reflective days on earth. With regards to modern security policy one can arguably say that cultivating a mindset on foreseeing a darker future has paid off, especially during most recent years. Those who expected Russia to come back in the pejorative meaning, were obviously right. And those who thought that Russia would turn into an ordinary European state were fundamentally wrong.

Since Russia launched a full-scale invasion of Ukraine in 2022, the grimness of war has been one of the major focal points for Europe. The shock and 'awakening' that followed accelerated a rearmament that had begun hesitantly after the annexation of Crimea in 2014, ending decades of post-Cold War downsizing.

Poland and the Baltic states have led the way, with defence budgets approaching or exceeding 5 per cent of GDP, and the Nordic countries close behind. Finland and Sweden joining the defensive alliance NATO in 2023 and 2024 respectively, was metaphorically speaking the icing on the cake in the process of taking charge of the worsening security situation.

2024 was also the year when China was directly linked to the war in Ukraine called out as *a decisive enabler*.¹

The way in which a mindset of expecting the worst has developed, has been questioned by progressive opportunists. Prophetic statements from security experts on that worse times are awaiting risks overshadowing positive potential, i.e. if we focus overly intently on growing risks and threats we might lose sight of developments that are demonstrating another truth, and hence also the chance of stimulating the constructive direction of the order of things.

Nonetheless, as history has made blatantly clear, it tends not to repeat, but rather appear in a similar disguise, uncannily rhyming with the past. Facts have, in this regard, a way of gaining the upper hand. And the facts – or the cards, to continue an analogy that recent events in the transatlantic sphere have stretched close to distortion – point to a few central truths with immense impact on the larger global geopolitical and related security landscape.

These facts however include additional truths to those which the larger European political consensus have established during the 2020's.

As true as it still is, when speaking of foreign states, Russia is the largest direct, closest, and most well-known threat to European democratic societies. Equally true is that Russia is not the sole destabilizing actor for our continent. In addition to other long-term threats (which this anthology will not address), the Chinese state occupies a unique position – both globally and for our region – because it is a state actor we have invited into our societies and engaged with extensively over centuries, and which has become even more active since the golden age of globalisation in the late 1990s and early 21st century.²

China's Rise and Growing Relevance

China has during recent decades undergone distinctive processes of changes with regards to its economy and technology, bolstering innovation, making the leap from factory facility onwards to a frontline production hub, and now innovation lab which has transformed not just the country's self identity but also its relevance on the global stage.³ This

story is often told, sold, and reproduced not merely by Chinese voices but also by global and European experts and media. The storytelling has a certain value and impact which China has invested heavily in.

And, the story is at the same time to a large extent also true. Yet it is decorated and developed with projections about the future which stem from antidemocratic impulses and ambitions of world leadership modelled in a system which stands in sharp conflict with a liberal rules-based order and outlook on humanity.⁴

What is even more striking is that parts of the storytelling, related directly to the sheer interpretation of China, is also so commonly echoed in interpersonal conversations about China. *To truly understand China is a life-long and still impossible quest.* If you have heard or possibly even yourself uttered this, or similar versions of the same, alluding to the impossibility to grasp the vastness and complexity of an ancient superpower and civilization, you probably have thought it sounds reasonable. For sure, on the one hand it certainly does. Any attempt to assess and make sense of a nation rich in not mere geographical materia, in people, history, tradition, culture and community-building, would, in a reputational manner, be potentially self-harming. Who am I (disregarding who the individual I at the moment happens to be) to make assumptions about such an old civilization, grand nation, economy, and geopolitical master player? What knowledge do I possess, or rather how much do I lack in order to be able to actually say anything of relevance about China? The task is probably daunting for those who do set out.

Irrespective of background, occupation and political alignment, it is essential not to let a multitude of intellectual courses remain in the backwaters when it comes to figuring out our part of the relationship with China. Letting the relationship be dominated by inferiority and smallness, or lack of certain expertise risks making it become specialised to a degree that only very few individuals are qualified to speak about China or even issues related to China, consequently making the task too daunting.

The ambition with this anthology is not to ‘unpuzzle’ or shed new light on China as such, nor does the writing in this book cover aspects related to China’s intentions and motivations on the world stage, or reasoning from its own ideological and historical context. Instead it will focus on how China has been able to use and in fact even weaponise and monetise the above mentioned perspective of that China is ‘ungraspable’, in order to shield itself from criticism and questions as well as build its own mastery over western democracies and thinking through cognitive warfare.⁵

The following writing and thinking has a foundation in favour of the democratic system and societies formed by this thinking and seeing the reality through this lens. It will investigate the clashes between the democratic society and the authoritarian, as well as analyse the effect that China, as a great power, has on the security landscape in individual democracies, Europe, and the West at large. As such, the anthology discusses the questions, which in our current era are more urgent to try to find answers and policy responses to.

Our Response Needs to Be More Ambitious Than the Challenge

As we shall see throughout this anthology, which has contributions from renowned China scholars, seasoned security policy thinkers, liberal human rights professionals, military analysts, and researchers specialised in cyber and technology, the way to ‘deal’ with China can never be less ambitious than the challenge posed against us. As China uses its *whole of society* to control, dominate, and influence our societies developments, often aiming to deconstruct larger alliances forming individual local, regional or national relations to disempower the other in the bilateral relation, we, as the we in European democracies together with democratic allies at large, should be able to make use of *the whole of all our societies* and combined competencies and forces, in order to preserve

and protect the long term interest and the very foundations of liberal democracy.

Fast Tracking Threat Assessments

In the European public context we are by now used to openly discuss and deal with growing Russian hybrid warfare, yet we are still in the starting blocks of understanding China being itself an actor in the hybrid realm. When the NATO declaration 2024 rightly named China, or in fact in the document PRC, as a ‘decisive enabler’ of the war in Ukraine, it was the result of years of process of sharpening understanding of the challenges posed by China (nuclear build-up, military cooperations with Russia, disinformation, cyber, space, technology transfer etc) and meant breaking with years of more cautious language.⁶

Speaking more locally from the national level in Sweden, during the years prior to the pandemic there was a sharp increase in disrupting events that affected Sweden-China relations. The complicated interplay between business, security, and human-rights risk surfaced, the abduction of Swedish citizen Gui Minhai, ‘wolf warrior diplomacy’ became recognised as a phenomenon and the cultural clash between freedom of expression and authoritarian interpretations of individual and nation became tangible – causing public debate about China’s influence on domestic issues to spark.⁷ Media started to report more extensively on subjects related to censorship and attempts to control the narrative on topics and issues that are sensitive to China.⁸ China’s role in the changing information landscape is a challenge that has become more visible with platforms such as Tiktok that are replacing other communication channels.⁹

Post-Pandemic ‘Peak Awareness’

The understanding that China is becoming increasingly important to assess spiked during the years following the pandemic. The pandemic itself was an exceptional global situation where China did not level

down but rather enhanced its power play and made it more difficult to deal with the Covid outbreak.¹⁰

In 2020/2021 Sweden founded the Swedish National China Centre, (Nationellt Kunskapscentrum om Kina, NKK) engaging expertise in China studies and associated competencies, offering research, expertise and advice for both decision-makers and the Swedish public as well an international audience.¹¹

China has under its current leadership distinctively heightened its ambitions on the global scene. The multitude of masterplans, five-year plans, and agendas for different prioritised industries and areas all aim at world dominance in various dimensions: Made in China 2025, China 2030, China Standards 2035, China 2050, the Belt and Road Initiative, Health Silk Road and Polar Silk Road, to mention a few.

Being an actor in the forefront, driving cutting edge technologies within green-transition industries, quantum computing and AI, to mention some, increasing its influence over critical European infrastructure, and holding a more essential role in the development of international standards, and at the same time being part of, and sometimes the very centre of, research communities in the West, has given China an upper hand. Yet, the stability that China wishes to project is itself questionable.¹²

The strategic thinking and approach of a non-democratic country, where the political, business, and military direction are aligned and basically one and the same, leads to an unfair playing field, with rising subsidy levels demonstrating this.¹³ Between 2005–2024, Chinese firms received three to eight times more government support than firms in OECD countries.¹⁴

Parallel to investing in the Global South and increasing international acceptance of China's growing influence, increased strategic coordination between China and Russia constitutes a growing security dilemma for the Euro-Atlantic and Arctic regions.¹⁵ Being dependent on that which is critical to our economy and security has become more wor-

risome both individually as well as enhanced by the Russian add-on risk.¹⁶

Among international experts who follow hybrid threats, near-consensus is that while Russia may be the present challenge, China will be a larger and more difficult threat for Europe and Western democracies to defend themselves against in the long term.¹⁷ In addition to the economical and technological dependencies we have with China, even when they are changing to some extent, there are a multitude of expressions of the hybrid landscape; extensive cyber espionage and transnational repression, undermining academic freedom and freedom of expression through pressure, surveillance, and influence directed at research institutions and diaspora communities in the West. Most of these phenomena are difficult to assess in terms of their impact, yet they are crucial to our resilience and security.

Opinion: Shaping and Changing

The public opinion in Sweden, as well as in Europe, has for a long time been critical when it comes to China. Swedes hold a particular critical view, as large opinion polls from Pew Research has tracked. This is still very much the case, however, in most recent data there has been a minor shift, especially in relation to how one views the current American leadership.¹⁸

Despite the public sentiment, the severe security situation in Europe and the rising awareness of China as a hostile actor (stated by Swedish Security Service in official reports during the last decade) we are still not collectively as national societies, nor the EU at large, yet recognising China's agency and strategic thinking, including on the political level,¹⁹ at the appropriate level in our own region.²⁰ This is partly due to a lack of a comprehensive understanding of China beneath the transactional relationship as well as what could best be described as a psychological *existential default mode*. When any professional community (ranging from research to business to tech and entertainment) start to discuss

security and China, the leap of thought often instantly jumps to ‘end-game’ scenarios, i.e. the resolution being cutting of ties similar to those large parts of the West have cut with Russia. Envisioning China outside of the global ecosystem is near impossible considering its role in the ecosystem of trade, a range of crude dependencies, raw earth substances, aspects of technological and innovative character, including AI, as well as production and supply.²¹

But also, which is the key point: ‘We’ are hindered in recognising China’s darker agency since we, to some extent, also risk becoming confined by *their* strategic objectives and narration, or at least narratives that are sufficient for China (regardless of origin of these narratives).

Europe is weak, China is strong. Europe is lagging behind, China is running ahead. The West cannot afford to decouple from China.

The reality, however, is obviously never this black or white. Even if China is driving innovation to a much larger scale today than previously, even when the Chinese economy is pushing ahead and challenging the US in incomparable ways, it urges us to think more thoroughly. What does it mean for us as Europeans or Westerners and democratic players if we substitute our own narration and storytelling with other actors’ stories?

The stories untold in the above context are in fact those which would be more of an advantage for Europe to foster. And as is the case with the ‘decoupling threat’, it is typically cast as Europe holds the active choice to break up the relation whereas China is not responsible for decoupling measures.²²

The Next Awakening for Europe is Yet to Happen

At this point in time we might be able to find consensus that dependencies come with risks and together identify vile diplomatic language when we hear it, as well as politically understand that large scale threats directed towards Taiwan are more than abstractions.²³ A wide range of events that affect our societies, related to cybercriminality, data collec-

tion, disinformation, maritime sea security, the future of Russia's war in Ukraine, economic and political leverage on our continent (and the list continues), is still to great degree underexplored and under-reported when outside of security and policy circles.

In the current geopolitical era – where strains are growing inside the West even as the determination to confront rivalry from hostile states and their leaderships also grows – it has never been more important to get China right, and even more so to get our own history, present, and future, right.

This anthology aims to bring analysis from thinkers of different fields and nations together in order to demonstrate differences and similarities in the current assessment of the emerging hybrid enabler and actor. Being both an enabler and an independently capable actor makes the threat, to some extent, two-layered.

The next awakening for Europe is yet to happen. We are being nudged by the awakening brought on by the Russian invasion of Ukraine and even more so by what it revealed about alliances and partners globally. This makes the next awakening possible to be more mature when it comes, but it will nevertheless be uncomfortable as all wake-up calls brought on by urgency are.

References

- 1 NATO, "Washington Summit Declaration," July 10, 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration>.
- 2 Säkerhetspolisen, "Ryssland, Kina och Iran" [Russia, China and Iran], *Säkerhetspolisen 2025/2026* (annual threat assessment), March 18, 2026, <https://www.sakerhetspolisen.se/om-sakerhetspolisen/publikationer/sakerhetspolisens-lagesbilder/sakerhetspolis-en-2025-2026/ryssland-kina-och-iran.html>.
- 3 Kaiser Kuo, "Made in China 2.0: The Future of Global Manufacturing?," *World Economic Forum*, June 26, 2025, <https://www.weforum.org/stories/manufacturing-and-value-chains/how-china-is-reinventing-the-future-of-global-manufacturing/>.
- 4 Justyna Szczudlik, "'Tell China's Stories Well': Implications for the Western Narrative," PISM Policy Paper no. 9 (169) (Warsaw: Polish Institute of International Affairs, September 2018), https://pism.pl/publications/Tell_Chinas_Stories_Well_Implications_for_the_Western_Narrative.

- 5 NATO Science and Technology Organization (STO), 2025, *NATO Chief Scientist Research Report on Cognitive Warfare*, <https://www.nato.int/content/dam/nato/webready/documents/sto/chief-scientist-report-cognitive-warfare.pdf>.
- 6 NATO, "Washington Summit Declaration," July 10, 2024, <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration>.
- 7 Bloomberg News, "China Canceled H&M. Every Other Brand Needs to Understand Why," *Bloomberg*, March 13, 2022, <https://www.bloomberg.com/graphics/2022-china-canceled-hm/>; Patrik Oksanen and Jesper Lehto, "Draken som bytte taktik: Kinesiska ambasadens arbete för att tysta kritiker" [The dragon that changed tactics: The Chinese embassy's efforts to silence critics] (Stockholm: Frivärld, August 30, 2021), <https://frivarld.se/rapporter/draken-som-bytte-taktik/>; Frivärld, "En Kinastrategi för Sverige och den fria världen" [A China strategy for Sweden and the free world] (Stockholm: Frivärld, December 2021), <https://frivarld.se/wp-content/uploads/2021/12/Kina-Rapport-.pdf>; Gustav Sundqvist and Erik Mo Welin, "Forskning med förbehåll? Auktoritär påverkan i svensk-kinesiska forskningsrelationer" [Research with reservations? Authoritarian influence in Swedish-Chinese research relations] (Stockholm: Swedish National China Centre and Mälardalen University, November 2025), <https://kinacentrum.se/publikationer/forskning-med-forbehall-auktoritar-paverkan-i-svensk-kinesiska-forskningsrelationer/>.
- 8 Lydia Farran-Lee, "Jesper Rönndahl om Kinainslaget: 'Det var korkat att lägga ut det på kinesisk sajt'" [Jesper Rönndahl on the China segment: "It was stupid to post it on a Chinese site"], *SVT Nyheter*, October 3, 2018, <https://www.svt.se/kultur/jesper-ronndahl-om-kinainslaget-det-var-korkat-att-lagga-ut-det-pa-kinesisk-sajt>; SVT Nyheter, "SVT om kinesiska kallarmötet: 'Borde inte ägt rum'" [SVT on the Chinese basement meeting: "Should not have taken place"], March 7, 2025, <https://www.svt.se/kultur/svt-om-kinesiska-kallarmotet-borde-inte-agt-rum>; TT, "Svenska nyheter frias för Kina-inslag" [Svenska nyheter cleared over China segment], *Svenska Dagbladet*, April 1, 2019, <https://www.svd.se/a/dO4zBw/svenska-nyheter-frias-for-kina-inslag>.
- 9 Patrik Oksanen and Anna Rennéus Guthrie, "TikTok: The Children's Entertainment App That Became a Security Problem" (Stockholm: Stockholm Free World Forum, December 19, 2024), <https://frivarld.se/rapporter/tiktok-the-childrens-entertainment-app-that-became-a-security-problem/>.
- 10 Jojje Olsson, "Kinas propaganda är i sig ett hot mot den globala hälsan" [China's propaganda is itself a threat to global health], *Vi*, March 19, 2020, <https://www.vi.se/artikel/jojje-olsson-kinas-propaganda-ar-i-sig-ett-hot-mot-den-globala-halsan>.
- 11 Swedish National China Centre, "About," Swedish Institute of International Affairs, accessed August 26, 2026, <https://kinacentrum.se/en/about/>.
- 12 DN Debatt, "Kina inte så stabilt som många vill tro" [China not as stable as many want to believe], *Dagens Nyheter*, 7 October 2025, <https://www.dn.se/debatt/kina-inte-sa-stabilt-som-manga-vill-tro/>.
- 13 Kristina Sandklef, "Temperaturmätare: Kinas näringsliv och statens inflytande över företagen" [Temperature gauge: China's business sector and the state's influence over companies] (Stockholm: Frivärld, November 2025), <https://frivarld.se/wp-content/uploads/2025/11/Temperaturmatare-Kinas-naringsliv-Frivarld.pdf>.

- 14 OECD, "Industrial Subsidies Reach Highest Levels Since the Global Financial Crisis, Says OECD," press release, June 1, 2026, <https://www.oecd.org/en/about/news/press-releases/2026/06/industrial-subsidies-reach-highest-levels-since-the-global-financial-crisis-says-oecd.html>.
- 15 Arctic Centre, University of Lapland, "The Polar Silk Road", <https://arcticcentre.org/en/arctic-region/maps/polar-silk-road/>.
- 16 NATO, "NATO 2022 Strategic Concept", June 29, 2022, <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>.
- 17 Chris Kremidas-Courtney, "Hybrid Storm Rising: Russia and China's Axis against Democracy" (Brussels: European Policy Centre, May 2, 2025), <https://www.epc.eu/publication/Hybrid-storm-rising-Russia-and-Chinas-axis-against-democracy-64b158/>.
- 18 Laura Silver, Jonathan Schulman, Laura Clancy, and William Miner, "Views of China and Xi Are Improving Globally" (Washington, D.C.: Pew Research Center, July 15, 2026), <https://www.pewresearch.org/global/2026/07/15/views-of-china-and-xi-are-improving-globally/>; Pew Research Center, "People in Many Countries Now View China More Positively Than the U.S.," July 15, 2026, <https://www.pewresearch.org/global/2026/07/15/people-in-many-countries-now-view-china-more-positively-than-the-u-s/>.
- 19 Malin Oud, "En seger för Kinas narrativ" [A victory for China's narrative], *Kvartal*, October 29, 2025, <https://kvartal.se/olawong/artiklar/en-seger-for-kinas-narrativ/cG9zdDoyMzk3MQ>.
- 20 Hélène de Rengervé and Maya Wang, "Europe's China Strategy Is Ready for a Refresh", *The Diplomat*, July 2026, <https://thediplomat.com/2026/07/europes-china-strategy-is-ready-for-a-refresh/>; Ulf Kristersson and Hans Wallmark, "M: Ett offensivt Kina kräver tydlig strategi" [M: An offensive China requires a clear strategy], *Svenska Dagbladet* 3 juni 2019, <https://www.svd.se/a/op1nwm/m-ett-offensivt-kina-kraver-tydlig-strategi>; Anna Rennéus Guthrie, "Världen får inte göra samma misstag med Kina som med Ryssland" [The world must not make the same mistake with China as with Russia], *Altinget*, October 20, 2023, <https://www.altinget.se/sakerhet/artikel/varlden-faar-inte-gora-samma-misstag-med-kina-som-med-ryssland>; Claus Soong and Niklas Hintermayer, "MERICS China Forecast 2026: High Expectations for Chinese Innovation, Low Expectations for Relations with US and EU" (Berlin: Mercator Institute for China Studies, December 2025), <https://merics.org/en/comment/merics-china-forecast-2026-high-expectations-chinese-innovation-low-expectations-relations>.
- 21 Karl Lallerstedt, "The China Challenge: The Inherent Difficulty in Balancing Security Concerns against Economic Interests," FOI Memo 8440 (Stockholm: Swedish Defence Research Agency, February 5, 2024), <https://www.foi.se/en/foi/reports/report-summary.html?reportNo=FOI%20Memo%208440>.
- 22 Johannes Stenlund, "Kinas taktik får hård kritik av OECD: 'Industrifall doping'" [China's tactics draw harsh criticism from the OECD: "Industrial doping"], *Dagens PS*, June 2, 2026, <https://www.dagensps.se/bors-finans/kinas-taktik-far-hard-kritik-av-oecd-industriell-doping/>.
- 23 Totalförsvarets forskningsinstitut (FOI), "Så försöker Kina isolera Taiwan" [How China is trying to isolate Taiwan], June 14, 2022, <https://www.foi.se/nyheter-och-press/nyheter/2022-06-14-sa-forsoker-kina-isolera-taiwan.html>.

Beyond an Alliance: The Sino-Russian Relationship

Patrik Oksanen

Deeper than Nazi Germany and Japan during World War II. But nowhere near Anglo-American War-cooperation, yet something that reminds about The United States and the Soviet Union in the same conflict. The three historical models from WWII help us to frame the problem on how to understand the Russian Chinese partnership.

Since Russia's annexation of Crimea in 2014, the strategic relationship between Moscow and Beijing has deepened markedly with acceleration after 2022, and it is moving from a strategic partnership into something more consequential and closer. With no limitations according to the February 2022 Xi–Putin joint statement.

The central question is no longer whether Moscow and Beijing co-operate militarily. They clearly do. The question is what kind of alliance, or coalition, this cooperation is creating – and how we in the West should understand it. Here history can guide us into an interpretation that could be intuitively understood by European decision makers that are facing many tough decisions in the coming years.

So let us first return to history: Nazi Germany and Imperial Japan fought many of the same enemies during the Second World War, and were formally in an alliance since the Tripartite pact in 1940, but conducted largely separate wars, with only limited operational coordination, that started at separate times. One can call the start of the wars an

organic, intertwined series of events rather than a strategic coordination of forces. The second Sino-Japan war started already in 1937, and could be viewed as the starting point of World War II in Asia. Nazi-Germany attacked Poland and went to war with the United Kingdom and France in 1939 and attacked the Soviet Union in 1941. Japan attacked Pearl Harbour later that year and Nazi-Germany declared war on the US, but Japan never declared war on the Soviet Union (even if the USSR declared war on Japan after Nazi-Germany defeat in 1945). Geography also hindered more concrete cooperation around military technology, lessons learned and resources.

The United States and Britain represented the opposite end of the spectrum: combined staffs, deep intelligence sharing, interoperable forces, integrated logistics, and genuinely joint operational planning.

The United States and the Soviet Union remained politically distant and operated under separate commands and operations, yet coordinated grand strategy against Nazi-Germany, exchanged material support (i.e. US supplied USSR), and forced Germany to fight on multiple fronts.

So where do China and Russia today fit into these three historical models?

The evidence since 2014 suggests that they have moved well beyond the German-Japanese model, but remain far short of the Anglo-American one. So closest is a version that leads the thought to the US and the Soviet Union during World War II.

The best description of the cooperation is probably something like an informal strategic alignment for potential conflict: two autonomous nuclear powers increasingly building the political, institutional, and military capacity to act in mutually reinforcing ways against the same adversarial system, while avoiding the formal obligations and command integration of a traditional alliance.¹

Xi Jinping and Vladimir Putin have met more than forty times since Xi assumed China's presidency in 2013, an exceptional frequency of leader-level contact among major powers.

The volume of high-level contact is the first reason to take this development seriously. Xi Jinping and Vladimir Putin have met more than forty times since Xi assumed China's presidency in 2013, an exceptional frequency of leader-level contact among major powers. This includes formal visits and bilateral meetings on the margins of BRICS, the Shanghai Cooperation Organisation (SCO), G20, APEC, and other summits. The precise number depends on whether separate sessions during the same visit are counted individually, and the COVID-19 years temporarily shifted the relationship to telephone and video diplomacy. What can be said more confidently is that, among leaders of major independent powers, the Xi–Putin relationship is exceptional in its sustained intensity.²

The latest Xi–Putin meeting was on the sidelines of the SCO summit in Bishkek on 31 August 2026. Xi explicitly referred back to the agreements reached during Putin's May state visit to China, noting that the two leaders had set the direction of the relationship 'from a strategic height and with a long-term perspective' and, crucially, that the relevant authorities in both countries were already implementing those understandings. Putin likewise described cooperation as developing successfully 'on all fronts' and highlighted new opportunities in digital innovation and artificial intelligence.

The significance lies not merely in personal diplomacy or the number of meetings between the top leaders. Beneath the presidents is a layered institutional architecture. Foreign ministers Sergei Lavrov and Wang Yi, and their predecessors, have held dozens of physical meetings since 2014. The bilateral strategic-security consultation mechanism had reached its twentieth formal round in Moscow in December 2025. Co-chaired in recent years by Wang Yi and the secretary of the Russian Security Council, the mechanism is officially described as a channel

for coordinating positions on major issues affecting the two countries' strategic security interests and for implementing the understandings reached by Xi Jinping and Vladimir Putin.

One should note that Wang Yi is not merely China's foreign minister. As a member of the Communist Party's Politburo and director of the Office of the Central Commission for Foreign Affairs, he is one of Xi Jinping's principal foreign-policy coordinators. His recurring strategic-security consultations with the secretary of Russia's Security Council therefore operate at a level between conventional diplomacy and military planning, translating presidential direction into broader security coordination.

At the defence-minister and the Chinese senior Central Military Commission (CMC) level, open-source records identify approximately twenty major encounters since 2014.

Most revealing of all is the staff-to-staff channel. Formal military consultations between China and Russia date back to 1997, while the recurring numbered strategic military consultation mechanism appears to have been established in the late 1990s. By November 2014, it had already reached its seventeenth round and had reached its twenty-second round by December 2023. Subsequent high-level military contacts have continued through the defence-minister and Central Military Commission channels, although a publicly documented twenty-third round has not yet been identified.³

Level	Documented volume	Primary significance
Xi Jinping–Vladimir Putin	~40 physical encounters since 2014	Strategic direction and political authorization
Foreign-minister level	Several dozen meetings	Diplomatic coordination and international positioning
Political/Strategic Security Consultation (Wang Yi–Russian Security Council)	18 formal rounds by 2023	Broad security, political and strategic coordination
Defence minister / senior CMC	~20 major documented encounters	Military programmes, technology, exercises and implementation
Armed-Forces Strategic Consultation (CMC Joint Staff–Russian General Staff).	22 formal rounds by Dec. 2023	Staff-to-staff strategic dialogue and exercise coordination

Table 1. Approximate open-source meeting volume. Counts are deliberately conservative and exclude routine telephone calls, video conferences, ordinary deputy-minister contacts, and mere co-attendance at multilateral events.

This density underlines the analytical picture. If Sino-Russian cooperation rested principally on Xi and Putin's personal relationship, it would be politically important but institutionally shallow. But China and Russia have built a structure that goes further. The relationship has multiple levels that can transmit strategic direction downward from the presidents; further down to foreign-policy and security institutions; defence ministers and senior CMC leaders; and the Russian General Staff and Chinese CMC Joint Staff Department. The question is therefore not whether an architecture exists, but what that architecture is capable of producing.

The strongest evidence of production of results comes from correlating meetings with subsequent changes in military behaviour. Such correlations must be handled cautiously: major exercises are planned long in advance, so a meeting weeks before an exercise is not the beginning

of planning. But repeated sequences can reveal an implementation cycle in which political leaders authorize a direction, defence institutions program cooperation, staff coordinate it, and operational forces execute it.

Here the following pattern can be noticed:

2014–2016: Building the Staff Relationship

In August 2014, Russian Chief of the General Staff Valery Gerasimov met his Chinese counterpart Fang Fenghui in Beijing. In November, the two sides held the seventeenth strategic consultation between their armed forces. Within the same broader meeting cycle, the defence ministers agreed on a Joint Sea exercise in the Mediterranean, which was conducted in May 2015. The sequence demonstrates that staff consultation, ministerial authorization, and operational activity were linked within the same institutional process.⁴

The May 2016 sequence is more diagnostically valuable. On 24 May, Admiral Sun Jianguo of the CMC Joint Staff Department and Lieutenant General Sergei Rudskoy of the Russian General Staff chaired the eighteenth strategic military consultation in Beijing. In connection to the consultation China and Russia began Aerospace Security 2016, their first joint computer-assisted command-post exercise focused on air and missile defence. Because such an exercise requires prior work on command procedures, threat identification, sensor information, and task allocation, its proximity to the staff consultation strongly suggests that both belonged to the same planning cycle and one can note a possible symbolic timing.⁵

2017–2020: From Exercises to Strategic Operations

The next major step was the 2017–2020 military cooperation roadmap signed in June 2017. As it was phrased at the time by the Chinese defense ministry spokesperson, it was a top-level plan that *‘...shows the high level mutual trust and strategic cooperation; it is conducive for both sides*

*to face new threats and challenges in the security field and to jointly safeguard regional peace and stability.*⁶

This led to China entering Russia's national strategic exercise cycle by participating in Vostok 2018 and Tsentr 2019. In July 2019 the two countries conducted their first joint strategic bomber patrol, establishing a practice that later became recurrent. Russia also publicly acknowledged helping China develop a ballistic-missile early-warning system—cooperation in a strategically sensitive field linked to nuclear deterrence.⁷

The twentieth strategic military consultation, held in Beijing on 30 May 2018, illustrates the pattern. Chinese official reporting stated that the two sides reached broad consensus on further deepening military cooperation. Three months later, Chinese forces participated in Vostok 2018. Vostok obviously had been planned earlier; the value of the consultation lies instead in showing that senior staff dialogue was embedded in the programme-management process that brought the PLA into an increasingly sensitive Russian operational training environment.⁸

2021–2024: Institutionalising Patrols and Geographic Reach

A second multi-year roadmap, covering 2021–2025, coincided with another qualitative expansion. Joint naval exercises were followed by recurring combined patrols, strategic bomber patrols became routine, Chinese forces continued to participate in major Russian exercises, and cooperation spread geographically. By July 2024, the two militaries had conducted their eighth joint strategic air patrol, this time over the Ber- ing Sea and into the Alaska Air Defense Identification Zone. The US Department of Defense subsequently assessed that Sino-Russian military activities had increased in frequency, geographic reach, and complexity.⁹

After the pandemic the visible General Staff-to-Joint Staff contact returned. In June 2023 Gerasimov spoke directly with Liu Zhenli, head

of the CMC Joint Staff Department, with both sides explicitly linking their dialogue to implementing the presidents' consensus and expanding military cooperation. In December 2023 the armed forces held their twenty-second strategic military consultation in Beijing. The following year brought further expansion in combined air and maritime activity.¹⁰

So what Kind of Alliance is Emerging?

Let us go back to the World War II-analogies. The meeting architecture and its observable outputs make the Germany–Japan analogy totally inadequate. Berlin and Tokyo shared enemies but never developed a comparable peacetime network of recurring leader-level, security, defence, and general-staff mechanisms. China and Russia now exercise together, conduct recurring strategic patrols, share selected military technology, and maintain formal multi-year cooperation programmes. Yet the Anglo-American analogy remains equally misleading. RAND's examination of possible future Sino-Russian coalition warfare identifies continuing limitations in interoperability, command-and-control integration, procedures, logistics, and shared systems. There is no publicly known equivalent of the Anglo-American Combined Chiefs of Staff, no permanent combined theatre command, no mutual-defence treaty, no routine integrated targeting process, and no public evidence has been identified of shared nuclear targeting or release authority.¹¹

The middle model is therefore the most plausible, even if we are seeing something that goes beyond the cooperation between the United States and the Soviet Union during WW2. Russia and China are increasingly capable of operating as distant coalition partners: maintaining separate national commands and primarily separate theatres while coordinating strategic timing, reducing friction between their forces, exchanging selected capabilities, and imposing simultaneous burdens on the United States and its allies. RAND describes a plausible form of such cooperation as deconflicted operations—geographically separate campaigns with limited joint planning and strategic coordination rather than fully integrated tactical warfare.¹²

This model could be strategically powerful without a single Russian regiment serving under Chinese command, and vice versa. In a Taiwan conflict, Russia could raise military pressure in Europe and the Arctic, forcing Washington to retain scarce assets outside the Pacific while providing political, economic, technological, or intelligence support to China. In a NATO–Russia conflict, China could help sustain Russia’s industrial base, complicate US force allocation in Asia, and preserve Moscow’s strategic endurance without formally entering the European war. The essential effect is not integrated battlefield command but strategic simultaneity.

The February 2022 Xi–Putin joint statement is revealing in this respect. The two governments portrayed their relationship as exceeding traditional Cold War-era alliances while deliberately avoiding a formal mutual-defence commitment. That formulation is not merely rhetoric; it fits the institutional design visible in practice: intimacy without treaty obligation, coordination without merged command, and increasingly routinised military interaction without publicly demonstrated joint war plans.¹³

The increasingly asymmetric character of the relationship is perhaps most clearly reflected in Russia’s material dependence on China. If the diplomatic and military architecture described above shows how closely the two states have institutionalised their cooperation, current trade figures illustrate how uneven that partnership has become. According to the Kiel Institute’s 2026 assessment of the Russian economy, China now accounts for approximately 35 percent of Russia’s total foreign trade and 76 percent of the increase in its supply of banned critical military components.

The dependence is even more pronounced in strategically important dual-use goods: China’s share of Russian dual-use imports has risen from roughly 25 percent before the full-scale invasion of Ukraine to more than 80 percent by 2025, concentrated in electronic components, CNC machine tools, computing and telecommunications hardware, and advanced optical and aerospace components.

Detailed customs data also show that China supplies 62 percent of all sanctioned critical components imported by Russia, compared with only 13.5 percent supplied collectively by the other non-sanctioning countries among the ten largest suppliers.¹⁴

This suggests that the relationship is not developing as a coalition of equals. Russia retains major military capabilities, strategic technology and combat experience of considerable value to China, but its ability to sustain its military-industrial base has become increasingly dependent on Chinese trade, technology and access to supply chains.

For Europe, with the growing Russian threat and the dilemma of economical dependencies on China, the headache is growing – especially for the simultaneous scenario. Imagine Russia and China acting with strategic coordination on separate theaters in order for once and all to break unity and capacity of the Western alliances.

So what to do for Europe, which is also struggling amid renewed uncertainty about the durability and scope of US security commitments?

Here are some urgent priorities for Europe

- 1. Enhanced intelligence warning.** Build a fused Russia–China strategic warning picture. European intelligence and defence planning should systematically correlate Xi–Putin summits, CMC–General Staff contacts, exercises, patrols, defence-industrial flows, cyber activity, critical-infrastructure incidents, and Chinese military pressure in the Indo-Pacific. The decisive warning indicator may be a cluster across both theatres rather than a single dramatic event. Staff-to-staff contacts deserve particular attention because they are closer to actual implementation than summit rhetoric.
- 2. Increase deterrence through sanctions.** Raise the cost to China of enabling Russia's war effort. Europe should systematically expand the sanctions policy it has already begun to apply to Chinese actors by targeting companies, financial institutions, and individuals demonstrably facilitating Russia's military-industrial production, sanctions circumvention, or access to critical dual-use technologies.

The EU has already sanctioned Chinese companies and banks under its Russia sanctions regime; this should become a more systematic instrument of deterrence.¹⁵ Given China's increasingly central role in supplying Russia's military-industrial base, Europe should make clear that continuing (and deepened) material support for Russian aggression will bring progressively higher economic costs. In parallel, the EU should prepare credible sanctions packages in advance for use if China attempts to alter the status quo in the Indo-Pacific by force. Words must be backed by action.

3. **Plan for the worst.** The strategic simultaneity, not merely a Russian contingency, should be the serious crisis European NATO members plan for. Europe must assume that Russian action in the West will coincide with a Chinese crisis in the East. In such circumstances the United States could remain politically committed to Europe while facing acute constraints in submarines, air and missile defence, long-range strike, ISR, strategic lift, and munitions. Europe therefore needs the logistics, industrial capacity, air defence, ammunition stocks, command resilience and will to manage a Russian contingency while substantial US combat power remains committed elsewhere. And it is urgent.
4. **Shield the infrastructure.** Infrastructure that makes European reinforcement possible must be protected. Ports, railways, energy systems, telecommunications, satellite links, data centres, and undersea cables are part of NATO's operational architecture. Cyber defence, redundancy, maritime domain awareness, counter-sabotage, and rapid attribution must therefore be integrated into defence planning rather than treated as separate civilian security issues. The objective should be resilience against parallel Russian and Chinese pressure even when there is no evidence of a single jointly commanded attack. This will have consequences for how Europe views for example Chinese vehicles that could be shut down remotely or collect data from Europe and send it to China.

The strategic challenge is subtler than the emergence of a formal alliance. China and Russia may not need integrated commands or a mutual-defence treaty to generate many of the strategic effects of an alliance. By coordinating pressure across separate theatres and domains, they can impose simultaneous challenges on the United States and European allies while retaining operational autonomy. For Europe, the key challenge is therefore not whether they become formal allies, but whether they can act in increasingly mutually reinforcing ways.

Moscow and Beijing may never need to formalise such an alliance in order to achieve their goals on Western behalf. Their emerging model already offers many benefits of coalition warfare without its political and organisational costs.

For Europe, the practical requirement is to prepare not for Russian and Chinese forces necessarily fighting shoulder-to-shoulder, but for two increasingly coordinated great powers capable of forcing the West to manage multiple theatres, multiple domains, and multiple forms of pressure at the same time.

References

- 1 Mark Cozad et al., *Future Scenarios for Sino-Russian Military Cooperation: Possibilities, Limitations, and Consequences* (Santa Monica, CA: RAND Corporation, 2024), especially the discussion of coalition models and deconflicted operations, https://www.rand.org/pubs/research_reports/RRA2061-5.html.
- 2 The figure of roughly forty Xi–Putin physical encounters since 2014 is an open-source reconstruction and varies slightly according to counting rules.
- 3 Yu Bin, China–Russia chronology, *Comparative Connections* (Pacific Forum), various issues, 2014–2024; Ministry of National Defense of the People’s Republic of China, official reporting on bilateral strategic military consultations.
- 4 Yu Bin, “Russia’s Pride and China’s Power,” *Comparative Connections* 16, no. 3 (January 2015), <https://cc.pacforum.org/2015/01/russias-pride-chinas-power/>.
- 5 Yu Bin, “Politics of ‘Reluctant Allies,’” *Comparative Connections* 18, no. 2 (September 2016), <https://cc.pacforum.org/2016/09/politics-reluctant-allies/>.
- 6 D. D. Wu, “China and Russia Sign Military Cooperation Roadmap,” *The Diplomat*, June 30, 2017, <https://thediplomat.com/2017/06/china-and-russia-sign-military-cooperation-roadmap>. The quote comes from a regular news briefing on June 29, 2017, when the Chinese Defense Ministry spokesman Wu Qian confirmed that Chang Wanquan did sign the roadmap on June 7 in the meeting with Shoigu.

- 7 U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2025* (Washington, D.C.: Department of Defense, 2025), <https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/annual-report-to-congress-military-and-security-developments-involving-the-peoples-republic-of-china-2025.pdf>; President of Russia, public statements on Russian assistance to China's missile early-warning capability, 2019.
- 8 Xinhua, "China, Russia Armed Forces Hold Strategic Consultation," May 30, 2018, https://www.xinhuanet.com/english/2018-05/30/c_137218061.htm.
- 9 Ministry of National Defense of the People's Republic of China, official reporting on the eighth China–Russia joint strategic air patrol, 2024; U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2025*.
- 10 Ministry of Veterans Affairs of the People's Republic of China, "中央军委联合参谋部参谋长同俄罗斯武装力量总参谋长举行视频通话" [Chief of the CMC Joint Staff Department Holds Video Call with Chief of the Russian Armed Forces General Staff], June 9, 2023, originally published by the Ministry of National Defense of the People's Republic of China, https://www.mva.gov.cn/sy/xx/gfxx/202306/t20230612_80796.html; TASS, "Chief of Russian General Staff Holds Video Call with Chinese Counterpart," June 9, 2023, <https://tass.com/defense/1629987>; Ministry of National Defense of the People's Republic of China, "Chinese, Russian Militaries Hold 22nd Round of Strategic Consultation," December 21, 2023, https://eng.mod.gov.cn/xb/News_213114/TopStories/16275271.html.
- 11 Cozad et al., *Future Scenarios for Sino-Russian Military Cooperation*.
- 12 Ibid.
- 13 President of Russia, "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development," February 4, 2022, <https://en.kremlin.ru/supplement/5770>.
- 14 Torbjörn Becker and Moritz Schularick, eds., *Endgame: The State of the Russian Economy*, Kiel Report no. 9 (Kiel: Kiel Institute for the World Economy, June 2026), 3, 6–7, https://www.kielinstitut.de/fileadmin/Dateiverwaltung/IfW-Publications/fis-import/3d87c36f-c2f7-46a6-aedb-8c03627a224a-Endgame_The-State-of-the-Russian-Economy-Kiel_Report_No_9-english-Version.pdf; Alicia García-Herrero, Elina Ribakova, and Lucas Risinger, "The China-Russia Asymmetric Partnership: Implications for Europe," in *Endgame: The State of the Russian Economy*, 34–47, esp. 36–37; Konstantin Egorov, "China's Role in Supplying Russia with Sanctioned Products," in *Endgame: The State of the Russian Economy*, 48–65, esp. 50–52.
- 15 Council of the European Union, "Russia's War of Aggression against Ukraine: EU Adopts 18th Package of Economic and Individual Measures," press release, July 18, 2025, <https://www.consilium.europa.eu/en/press/press-releases/2025/07/18/russia-s-war-of-aggression-against-ukraine-eu-adopts-18th-package-of-economic-and-individual-measures/>.



Murky Waters: Latvia's Strategic Communications on Kinetic Maritime Threats

Dr. Una Aleksandra Bērziņa-Čerenkova

Abstract

Latvia has a distinctive position in the European hybrid threat landscape: exposed geographically, experienced institutionally, and increasingly subject to pressure from two actors – Russia and China – whose hybrid activities, while not operationally coordinated, produce compounding effects. This paper examines how Latvia's strategic communications architecture has evolved to address threats and where its adaptation remains incomplete. It argues that Latvia's resilience framework was designed primarily for countering information operations and is now being stress-tested by ambiguous greyzone events in the Baltic Sea that have both a kinetic and an informational component. Given the traces of China-Russia cooperation in the emerging maritime-information nexus flagged in the Nordic-Baltic neighbourhood, Latvia should be ready for similar “murky” challenges to its stratcom and decide whether it will stick to its policy of clear attribution and calling out adversarial intent, or will opt for keeping a lower profile, as neighbours have done.¹

Introduction

Latvia is, by many assessments, among the better-prepared EU member states in countering hybrid threats in the information domain.² The nation initiated the resolution for fighting the spread of disinformation and misinformation that the UN adopted in 2021.³ Alongside its Baltic neighbours Lithuania and Estonia, the standing of information high performers is not unearned. Years of institutional investment, early adoption of the FIMI (Foreign Information Manipulation and Interference) analytical framework, and the presence of NATO's Strategic Communications Centre of Excellence in Riga have produced a resilience architecture that is more mature and coherent than that of many larger European counterparts. Some of the approaches were controversial at the time of adoption, including bans on 20 Russian TV channels in Latvia after Russia's full scale invasion of Ukraine in 2022. Ultimately Latvia's ban on RT was found by the European Commission to comply with EU law "due to its incitement to hatred."⁴

And yet, the threat environment is shifting in ways that outpace even the best-prepared responses.⁵ Russia's hybrid operations against Latvia are not new, but their delivery infrastructure has been substantially strengthened via AI-assisted content generation. Russia's long-term goal to cultivate cynicism in the Latvian society is now being supported by an elaborate network of online and offline coordination, in which information attacks form but one prong. More significantly, Russia is not the only state actor of concern. China, a relative newcomer to the Latvian information space, is primarily centered on fostering an image of itself as a guardian of the UN and international norms, as a business opportunities provider, and as a leader in addressing climate change. But it has also developed a distinct set of influence instruments that existing frameworks are poorly equipped to address, including information suppression and stakeholder cultivation.⁶

Furthermore, several cases have emerged where kinetic events are clearly followed by informational contestation. The continuing pres-

asures of weaponised migration,⁷ and Latvia's recent political challenges following a drone incident on Latvian territory,⁸ are both testaments to the argument that a nation that knows how to safeguard its information space well does not always bring its top game when physical activities precede the information phase. In this, the maritime domain has emerged as a new theatre, in which kinetic hybrid events carry information consequences, and actors, including those connected to Russian and Chinese companies, intersect in ways that challenge the current attribution practice and even the strategic communications doctrine at large.

The chapter below examines Latvia's strategic communications architecture, assesses its fitness for a multi-actor threat environment, and identifies adaptations still required.

The Threat Landscape: Two Actors, One Effect

Russia's information objectives vis-à-vis Latvia have remained unchanged over the past decades: amplifying Latvia's internal linguistic, geographical and societal fault lines to decrease support for a European and Transatlantic future. Russia's full-scale invasion of Ukraine in February 2022 intensified certain narratives, without altering this underlying strategic logic. Wider goals, to which Latvia is but a means to an end, include fracturing the Transatlantic community, decreasing support for Ukraine to ultimately discredit Ukrainian statehood, and gradually allowing Russia to gain more control regionally and a bigger standing internationally. Latvia has both symbolic and operational value for such goals. Symbolically, first, the nation followed a path of de-Sovietisation and succeeded in re-entering Western structures, second, it borders Russia and is thus a visible counterargument to pro-Russian geopolitical choices, and third, since Russian occupation of Crimea in 2014 it is increasingly hosting NATO and bilateral allied formations. Operationally, 34.6 percent of the population speak Russian at home,⁹ and research confirms that language spoken at home

remains the strongest predictor of narrative reception, outweighing locality, political spectrum positioning, and age.¹⁰ Hence Russia uses the linguistic and ethnic levers to reach its goals.

The 2022 ban on Russia-based media channels substantially altered the consumption landscape, but without eliminating their reach altogether – the content was still available via YouTube, mirror portals, Telegram and WhatsApp groups. Even when people did not deliberately seek out those channels, social media algorithms provided them anyway. Research by the Baltic Centre for Media Excellence shows that the news obtained via social media can be from traditional media, but “often without identifying the original source of the news.”¹¹ When such content is consumed at scale, the “firehose of falsehood” model (RAND), which operates not merely as external manipulation but as the ambient epistemological condition of Russia’s own information environment, has a negative effect on societal resilience. The long-term implication is, thus, that a person, without initially subscribing to it, falls victim to epistemic cynicism, meaning the conviction that truth is inaccessible by design: everybody lies, all media serve their owners, Big Brother is always in control.

China presents a structurally different challenge. PRC activity in the Latvian information space is self-referential: it does not engage with Latvian domestic politics except where Beijing’s “core interests” are directly implicated, and it spreads content through translations of CCTV and Xinhua output and official MFA channels rather than locally adapted production. The principal narrative clusters are: China as a reliable business partner that brings opportunity, as a global climate leader, and as the guardian of the UN-based international order. Conspicuously absent is any engagement with China’s most significant reputational liability in Latvia: its enabling role for Russia’s invasion of Ukraine. Beyond overt promotion, alarmingly, China practises information suppression, targeting academic and cultural institutions. Al-

though episodes are individually deniable, cumulatively, they strive for a narrowing of permissible public discourse and self-censorship.

The amplification dynamic between Russia and China does not require close coordination. The actors share narrative overlap on several key narratives (NATO as the root cause of the war in Europe, Western sanctions as self-defeating and against the spirit of free trade, Russia and China are the unrecognized forces beyond the defeat of global Fascism, etc.). Cross-platform reinforcement by state media outlets on both sides has been documented by the NATO StratCom COE.¹² The result is a compounding effect: Russian mass-manipulation and Chinese elite-targeting press on different parts of the Latvian information environment simultaneously, jointly reinforcing the conditions that make the other more effective.

The Hybrid Maritime-Information Nexus: Too Much to Handle?

Latvia has implemented visible development steps in the nation's institutional response to hybrid information threats. Notably, "The National Concept on Strategic Communication and Security of the Information Space (2023–2027),"¹³ marked a shift from earlier content-focused approaches toward a whole-of-society framework. It emphasised on early warning monitoring and rapid response crisis communication, grounded in the analytical logic of the EEAS framework rather than the adjudication of individual false claims, making it an efficient tool against perpetrator actors, be it Russia, China, or others. It also spotlights the ultimate goal – increasing societal resilience, formulated as "the ability of the state, institutions and citizens to detect, recognise and resist threats and crises of information space in a timely manner, including disinformation, as well as to quickly and effectively recover and become more skilled in order to avoid such situations in the future."¹⁴

Second, the 2024 amendment to the Criminal Law introduced liability for the malicious use of deepfake technology in electoral contexts,

imposing penalties of up to five years' imprisonment for fabricated defamatory content directed at candidates within a 120-day pre-election window. Latvia is among the first EU states to legislate specifically on deepfake-based electoral interference.¹⁵

On top of that, NATO StratCom Centre of Excellence in Riga operates as a multiplier for Latvia's own capabilities, publishing research on Russian and Chinese influence operations, among others, and thus providing think-tank analytical capacity that no single national government could sustain. Taken together, these instruments constitute a capable, legally grounded, and reasonably well-coordinated framework that covers detection, deterrence, punishment, and stratcom response.

However, some hybrid threats are more hybrid than others, meaning they contain several layers of pressures, and it is in these contexts where the gaps in the Latvian information response appear. A case in point is the emerging field of maritime grey zone threats close to the Latvian shores: the actual events are surrounded by and followed by an informational component, yet the very nature of the conflicting information surrounding the events in the public domain contributes to its hybridity. The events could be intentional or accidental; they could be attributed to a certain state, commercial actor, or none of the above; and they mostly continue without a clear resolution, meaning the investigations are communicated as "ongoing" over the years to come, or not communicated at all.

Since 2023, a series of Baltic undersea cable and pipeline incidents has introduced a new dimension to Latvia's hybrid threat environment. The Balticconnector rupture (October 2023), the Estlink-2 and Baltic cable severances (November 2024), the LVRTC Ventspils-Gotland cable damage (early 2025), and the Palanga-Liepāja optic cable incident (2026) share a common signature: civilian vessels, layered ownership structures pointing to commercial actors with links to Russia and, in some cases, China, and calibrated ambiguity. As the attributions regarding shadow fleet vessels in the Baltic attest, Russia has a strate-

gic interest in Baltic infrastructure disruption.¹⁶ China's interest is not clearly attributed but is consequential: commercial vessels with links to Russian commercial networks and Northern Sea Route logistics have featured in the incident pattern. Beijing has limited direct interest in the Baltic theatre, but the region offers something valuable: a low-cost laboratory for testing the international community's attribution threshold and response coherence. After all, China's unveiling of a first-of-its-kind deep-sea cable cutter signals its intent to adopt underwater sabotage as a core military tactic. Able to sever fortified communication and power lines at unprecedented depths of 4,000 meters, this new asset is designed for integration with China's advanced submersibles, giving Beijing a direct tool to paralyse global critical infrastructure and reshape maritime power dynamics.¹⁷

Chinese maritime actors state-linked shipping companies, vessels with opaque ownership structures – can gain operational experience in conducting or facilitating grey-zone maritime actions against critical infrastructure, generating learning that can transfer to theatres where China has direct strategic interests: the South China Sea, the Taiwan Strait, and undersea cable routes connecting East Asia to global communications networks.

In a situation where clarity is scarce, Latvia opts for drawing attention to the incidents instead of silence, perhaps recognising that passive communication creates information vacuums that adversaries will fill.

When in early 2025 a submarine optical fibre cable belonging to SJSC Latvia State Radio and Television Center was damaged in the Baltic Sea causing disruptions in data transmission services on the Ventspils-Gotland (Fårösund) segment, the Latvian Cabinet of Ministers stated the launch of “criminal procedural actions.”¹⁸

One year later, in 2026, when the optic cable Palanga (Sventāja)-Liepāja, the Latvian approach was again to communicate the event as possibly hybrid, as the State Police statement read: a criminal investigation has been launched and the vessel in question has been identified.¹⁹

The police boarded the vessel associated with the incident and communicated about it, the report making its rounds in the international media as well.²⁰ The then Latvian Prime Minister Evika Silina expressed suspicion of malign intent, and informed about NATO level coordination following Latvia's request. "We have determined that there is most likely external damage and that it is significant,"²¹ CNN quoted the Latvian PM. The country is also actively deepening cooperation on protecting undersea cables within the NATO and Nordic-Baltic 8 formats,²² and communicating about it, too. No cases with a Chinese component have been flagged in Latvia's waters to date, yet the role and presence of vessels with a Chinese connection in other incidents in the Baltic Sea could form a part of a wider strategy. In that case such an occurrence is only a matter of time, and for this, Latvia should have a clear stratcom plan.

The lesson is general: kinetic hybrid events have an immediate information phase, and losing that phase compounds the physical damage. Hybrid operations succeed not only through their material effects but through the cognitive and political uncertainty they generate. A state that responds to cable damage with process language rather than strategic communication cedes the information space at the moment of maximum public attention.

Conclusions

The accumulated institutional experience and the field-tested capabilities of Latvia are a transferable strategic asset to partners facing the same adversaries. However, the threat is an ever-developing one. There is the kinetic-to-information domain challenge. In the new domain of murky kinetic hybrid events with an information afterglow, Latvia's strategic communicators are still exploring how much attribution is helpful, and where caution and restraint should prevail, especially as the nation is in its parliamentary election year. However, waiting for the situation to solve itself by ignoring the event is also not prudent – after

all, strategic communication is precisely about acting fast and earning the contested information space from the adversary.

On top of that, there is the Russia-China challenge. The two actors do not need to coordinate to produce compounding effects: convergent interests, shared narrative infrastructure, and parallel pressure are sufficient. Latvia's existing architecture addresses this threat only partially.

Under a growing number of hybrid incidents, the question of what is the right approach remains as pertinent as ever. That work is best done collectively, within the Nordic-Baltic 8 and in close alignment with EU and NATO frameworks.

References

- 1 The author thanks Ms Karlina Jansone for research support.
- 2 Elina Vroblevska and Beniamino Irdi, "What's the Best Way to Deal with Russian Information Manipulation? Latvia Has Answers," Atlantic Council, May 14, 2025, <https://www.atlanticcouncil.org/blogs/new-atlanticist/whats-the-best-way-to-deal-with-russian-information-manipulation-latvia-has-answers/>.
- 3 Ministry of Foreign Affairs of the Republic of Latvia, "Latvia – an Initiator of a Resolution Just Adopted by the United Nations for Fighting the Spread of Disinformation and Misinformation," March 25, 2021, <https://www.mfa.gov.lv/en/article/latvia-initiator-resolution-just-adopted-united-nations-fighting-spread-disinformation-and-misinformation>.
- 4 European Commission, "Latvia's Decision to Suspend Broadcast of the Russian Language Channel 'Rossiya RTR' Complies with EU Law," May 6, 2019, <https://digital-strategy.ec.europa.eu/sl/node/1843>.
- 5 The following assessment addressing the playbooks of the actors in Latvia is based on: Una Aleksandra Bērziņa-Čerenkova, "Malign Information Influence in Latvia 2020–2025: Unchanged Goals yet Evolving Playbooks," in *Countering Foreign Information Manipulation in the Baltic Sea Region: Patterns, Responses and Gaps* (GSSC, 2026), 16–22.
- 6 J. Jurāns and Una Aleksandra Bērziņa-Čerenkova, "Small States, Big Stage: Latvia's Non-Establishment Actors and China's Evolving Strategy," *The Pacific Review* (2026): 1–18, <https://doi.org/10.1080/09512748.2026.2656402>.
- 7 OCCRP, "Latvia Says Belarus Helped Drive Migrants Into E.U. Using Military Vehicles," January 15, 2026, <https://www.occrp.org/en/news/latvia-says-belarus-helped-drive-migrants-into-eu-using-military-vehicles>.
- 8 LSM.lv, "Latvian Government Seriously Shaken by Drone Incidents," May 14, 2026, <https://eng.lsm.lv/article/politics/politics/14.05.2026-latvian-government-seriously-shaken-by-drone-incidents.a647051/>.
- 9 National Statistical System of Latvia, "PIA77: Mother Tongue and Language Used at Home by Region in 2022 (Percent of the Population in the Relevant Group)," https://data.stat.gov.lv/pxweb/en/OSP_OD/OSP_OD__apsekojumi__pieaug_izgl/PIA77.px/.

- 10 This conclusion has also been proven true in reactions to PRC strategic narratives in Latvia. See, e.g., Simona Merkinaitė et al., “Classic Cleavages in a New Light: Chinese Informational Influence in the Baltics” (Eastern Europe Studies Centre, Latvian Institute of International Affairs, and International Centre for Defence and Security, 2024), 40, https://www.liia.lv/en/publications/classic-cleavages-in-a-new-light-chinese-informational-influence-in-the-baltics-1206?get_file=1.
- 11 Anda Rožukalne, “Changes in Media Consumption: Russian-Speaking Audiences in Estonia and Latvia,” focus group survey, Baltic Centre for Media Excellence, <https://bcme.eu/en/research/changes-in-media-consumption-russian-speaking-audiences-in-estonia-and-latvia/>.
- 12 The Diplomat, “How Does China Engage With Russia’s Media Market?,” May 2, 2023, <https://thediplomat.com/2023/05/how-does-china-engage-with-russias-media-market/>.
- 13 Cabinet of Ministers of the Republic of Latvia, “The National Concept on Strategic Communication and Security of the Information Space 2023–2027” (Riga, 2023), <https://www.mk.gov.lv/en/media/15446/download?attachment>.
- 14 Cabinet of Ministers of the Republic of Latvia, “The National Concept on Strategic Communication and Security of the Information Space 2023–2027” (Riga, 2023), <https://www.mk.gov.lv/en/media/15446/download?attachment>.
- 15 LV portāls, “Ieviesta kriminālatbildība par vēlēšanu procesa ietekmēšanu, izmantojot dziļviltojuma tehnoloģiju” [Criminal liability introduced for influencing the electoral process using deepfake technology], 2024, <https://lvportals.lv/skaidrojumi/363728-ievies-kriminalatbildibu-par-velesanu-procesa-ietekmesanu-izmantojot-dzilviltojuma-tehnologiju-2024>.
- 16 Yle, “Charges filed over New Year’s cable damage in Gulf of Finland”, June 15, 2025, <https://yle.fi/a/74-20231651>.
- 17 South China Morning Post, “China Unveils a Powerful Deep-Sea Cable Cutter That Could Reset the World Order,” March 22, 2025, <https://www.scmp.com/news/china/science/article/3303246/china-unveils-powerful-deep-sea-cable-cutter-could-reset-world-order>.
- 18 Cabinet of Ministers of the Republic of Latvia, “LVRTC: Submarine Optical Fiber Cable Damaged (Updated),” January 26, 2025, <https://www.mk.gov.lv/en/article/lvrtc-submarine-optical-fiber-cable-damaged-updated>.
- 19 Sargs.lv, “Par kabeļa bojājumu jūrā pie Liepājas sāks kriminālprocess un identificēts kuģis” [Criminal proceedings opened over cable damage at sea off Liepāja, vessel identified], January 4, 2026, [https://www.sargs.lv/lv/latvija/2026-01-04/par-kabela-bojajumu-jura-pie-liepajas-saks-kriminalprocess-un-identificets](https://www.sargs.lv/lv/latvija/2026-01-04/par-kabela-bojajumu-jura-pie-liepajas-saks-kriminalprocess-un-identificets-kuģis).
- 20 Reuters, “Latvia police board vessel after Baltic Sea telecom cable breach,” January 4, 2026, <https://www.reuters.com/business/media-telecom/latvia-pm-says-baltic-sea-optical-cable-has-been-damaged-2026-01-04/>.
- 21 CNN, “Baltic Undersea Cable Likely Damaged by External Force, Latvia Says,” January 26, 2025, <https://edition.cnn.com/2025/01/26/europe/latvia-baltic-undersea-cable-intl-latam>.
- 22 Ministry of Foreign Affairs of the Republic of Latvia, “The Nordic-Baltic Countries and the United States Affirm the Need to Deepen Practical Cooperation Through NATO on Protecting Undersea Cables,” January 16, 2025, <https://www.mfa.gov.lv/en/article/nordic-baltic-countries-and-united-states-affirm-need-deepen-practical-cooperation-through-na-to-protecting-undersea-cables>.



Access as Influence: China's Strategic Embeddedness in Germany

Ferdinand Gebringer

I. The Geometry of Access

More than 80 percent of the solar inverters installed in Germany come from Chinese manufacturers. A Chinese state-owned corporation holds a stake in Germany's largest seaport. Agents of a Chinese intelligence service have systematically cultivated professors at no fewer than eight German universities. CISPA, the Helmholtz Center for Information Security in Saarbrücken, has been under suspicion since June 2026 of passing sensitive research findings to China. And yet the public debate on hybrid threats revolves almost exclusively around Russia.

This asymmetry is of course no accident. Moscow acts loudly, aggressively and disruptively. Beijing's influence in Germany is quiet, long-term, systemic. It seeks not rupture but position and has built that position, in infrastructure, institutions, networks and norms – over decades and largely undisturbed. The central argument of this chapter is that China's influence in Germany operates primarily through the accumulation of access. By geometry of access I mean the constellation of economic, technological, academic and political entry points that, while individually benign, collectively create durable positions within Germany's economic, technological, political and societal systems. These positions facilitate information acquisition, dependency formation and the accumulation of strategic leverage. This chapter does not suggest

that every Chinese investment or partnership is malignant. Instead, it posits that cumulative effects of otherwise legitimate engagement gradually alter the strategic calculus until accommodation appears less costly than resistance.

The sections that follow map six vectors that are especially dangerous from a German perspective, because they exploit the very openness that defines a liberal democracy: economic leverage (IV), infrastructure penetration and sabotage (V), cyber operations (VI), academic espionage (VII), elite networks (VIII), and information operations and diaspora control (IX). Running alongside these is a further, more diffuse dimension, China's reach into international standard-setting bodies. This is not Germany-specific, but shapes the technological terrain on which all the vectors operate (see Section II). One organisational backbone is the Chinese Communist Party's United Front Work Department (UFWD), a party organ responsible for coordinating influence networks across society.¹

II. The Strategic Logic of Entanglement

China's influence-seeking in Germany follows a coherent strategic logic organised around four objectives. First, technological supremacy and resistance to decoupling. Through Made in China 2025 and Dual Circulation, Beijing pursues independence from foreign technology while keeping the world economy dependent on China.² Germany, as a technology exporter, is doubly affected. Its knowledge is siphoned off, its export markets shrink once China has built the capacities itself, and the 14th Five-Year Plan explicitly aims at "self-circulation in case of a combat situation."³

Second, neutralising resistance in a crisis: dependencies act as leverage in an escalation, say over Taiwan. This way economic entanglement doubles as insurance against European pushback. Third, reshaping the international order: Beijing seeks to shape international rules and technical standards in ways that are compatible with authoritarian

governance and that create durable positions of technological influence. Its growing presence in bodies such as the International Telecommunication Union, International Organization for Standardization, or 3rd Generation Partnership Project and support for proposals such as Huawei's "New IP" illustrate this approach.⁴ Because standards become embedded in infrastructure and are difficult to replace, standard-setting constitutes another form of strategic access. Germany's strong role in industrial standardisation and advanced manufacturing therefore makes it particularly exposed to long-term technological dependencies.

Fourth, securing the legitimacy of the party-state: at home and abroad. Beijings influence serves to mute criticism of China's human-rights, Taiwan or Xinjiang policies, control the diaspora, and establish the "China model" as an alternative to liberal democracy. These four objectives are the common thread running through every vector below.

III. The Alignment Apparatus

The decisive difference between Western and Chinese conceptions of intelligence services is that the People's Republic is an "intelligence state." The boundary between intelligence and economic, academic and diplomatic activity is deliberately kept permeable. Influence is not the task of individual agencies but a "whole-of-state" approach. The party, the state, the military and private actors all interlock.⁵

Three pillars anchor it. The UFWD, an organ of the CCP Central Committee elevated by Xi since 2012 into one of the party's "three magic weapons," builds networks of alignment among diaspora, elites, business and academia. Its budget reportedly exceeds US\$2.6 billion, more than China's foreign ministry.⁶ The Ministry of State Security (MSS) operates through decentralised bureaus and has exploited United Front-linked structures for intelligence purposes, including by posing as UFWD officials.⁷ The military component, chiefly the Strategic Support Force (2015), fuses cyber, space, electronic and psychological

warfare. The distinctive feature is involvement of private contractors. For instance the 2024 i-Soon leaks (see Vector VI) show private IT-security firms executing operations for the MSS – with the UFWD supplying “the networks, cover and institutions that intelligence services use.”⁸

For Germany this means the apparatus spans economic, academic, political and media domains at once. This way it eludes typical departmental logic and exploits democratic openness as entry points. The aim is self-alignment, creating conditions under which German actors serve Beijing’s interest from their own calculation without any direct instruction.⁹ This is Christopher Walker’s *Sharp Power*: the asymmetric use of democratic openness against democracy itself.¹⁰

IV. Dependency as Leverage: The Lithuania Test

Beijing treats dependency as a strategic instrument, ready to wield it when red lines are crossed. Bilateral trade grew more than 900 percent between 2001 and 2024, reaching €273 billion.¹¹ Two cases illustrate the pattern. First the 2016 acquisition of Germany’s robotics champion KUKA by the Chinese Midea Group exposed concerns over technology transfer and revealed the limited ability of German authorities to intervene in foreign takeovers of strategically relevant companies. Second, in 2022 six federal ministries, the Federal Intelligence Service (BND) and the domestic-intelligence agency (BfV) opposed a COSCO stake in the Tollerort container terminal. Despite this, former Chancellor Olaf Scholz pushed through a 24.99 percent stake against the entire security cabinet.¹²

Beijing’s active use of economic dependency is illustrated by Lithuania. After Vilnius allowed a Taiwanese office under the name “Taiwan” in late 2021, China imposed informal sanctions and pressured international firms — including Germany’s Continental — to remove Lithuanian inputs from supply chains.¹³ The episode demonstrated China’s ability to weaponise economic interdependence, while Lithuania’s lat-

er normalisation with Beijing showed the limits of sustained coercion once political costs increase.¹⁴

V. Switches in the Infrastructure: Whoever Controls the Hardware Controls the Grid

The degree of Chinese technological infiltration of Germany's energy and digital infrastructure raises concerns that certain components could potentially be exploited for remote access or disruption in a crisis. The vector runs in three stages: critical components, the sabotage capability that could grow from them, and the same pattern extended to spying activities. There are three distinct stages: access as a durable foothold in a system, the capability such access creates, and finally the activation of that capability.

More than 80 percent of the solar inverters installed in Germany come from Chinese makers such as Huawei, Sungrow and Deye, and are permanently connected to manufacturer clouds.¹⁵ The Federal Office for Information Security (BSI) rates this a “considerable security risk.”¹⁶ In 2025 US researchers found undocumented communication modules – potential backdoors for remote access – in several devices.¹⁷ One expert likens the resulting dependency to the one Germany once had on Russian gas.¹⁸ Since 46 percent of German electricity already came from wind and solar in 2025, that exposure grows with every step of the energy transition.¹⁹

The same pattern recurs across other hardware. The Waterkant wind farm off Borkum was to be fitted with turbines from China's Ming Yang. The operator switched to Siemens Gamesa after a defence-ministry assessment warned that the installations could surveil sea lanes and be shut down remotely.²⁰ Roughly 80 percent of the ship-to-shore cranes in Western ports come from the Chinese state group ZPMC – networked and remotely serviceable, and classified as a security risk under a 2024 US executive order. Yet Germany still has no comparable vetting requirement. And through HMN Technologies (formerly

Huawei Marine Networks), Beijing invests heavily in undersea cables that carry more than 95 percent of international data traffic.²¹

That China can also act on this embedded position was shown in November 2024, when two Baltic Sea cables — including the Finland-Germany C-Lion1 link — were cut by the Chinese freighter *Yi Peng 3* sailing with its AIS transponder switched off. Defence Minister Pistorius called the incident sabotage and intelligence circles suspected the captain had acted on Russian orders.²² Deniability is yet another component of the design.

Chinese embedding in critical components also extends to mobile sensors enabling data collection for spying purposes. Modern connected cars are rolling sensor platforms, with cameras, microphones, radar and a permanent cloud link to manufacturer servers. In early 2026 the BfV expressly warned of security risks posed by connected Chinese electric vehicles, whose internet interfaces could enable unauthorised access.²³ In February the interior ministry confirmed an “espionage potential” in fully networked Chinese cars,²⁴ and the defence ministry has already restricted certain vehicle types at sensitive sites.²⁵

The concern reaches beyond Germany too. Poland is weighing similar restrictions, Israel has barred Chinese vehicles from sensitive locations,²⁶ and Australia’s domestic-intelligence service advises against holding confidential conversations in connected cars at all. The BfV and the security authority ZITiS have reportedly spent over a year examining what data several Chinese manufacturers collect and whether it is transmitted abroad.²⁷

The pattern is no different than the inverters and cranes. Whoever controls the sensors and the cloud link gains insight into movement and environmental data, sharper still when the vehicles operate near barracks, ministries or critical infrastructure. In the worst case, such access could also be used to restrict, disable or manipulate system functions.

VI. Cyber Operations: Espionage, Sabotage, System Penetration

Chinese cyber operations against Germany are state-attributed, increasingly professional, and pursue two interconnected goals: strategic intelligence gathering and economic espionage. Persistent access to critical networks could also enable future disruptive or sabotage operations.

First, strategic intelligence gathering. On 31 July 2024 the German government publicly attributed a serious attack on the Federal Agency for Cartography and Geodesy (BKG) to state-directed Chinese actors, an unusually blunt step.²⁸ The agency supplies geodata for military logistics and disaster planning, and the agency had already been targeted in late 2021 by APT15, a China-linked advanced persistent threat (APT) actor. The BfV also identifies APT31, another China-linked cyber espionage group, which increasingly targets Western ministries, authorities, parties and foundations. They use compromised private end-devices as an obfuscation network.²⁹

Second, economic espionage in the shadows. The BfV estimates annual damages in the billions, with Chinese state-linked actors as the principal source; preferred targets are mid-sized firms in precision engineering, optics, biotechnology and chemicals.³⁰ The scale these operations have reached is laid bare by the i-Soon leaks of February 2024. Datasets of the Chinese IT-security company i-Soon, published on GitHub, documenting an industrialisation of cyber espionage — private firms attacking on a division-of-labour basis for the MSS and the Ministry of Public Security. The BfV analysed the leaks in a four-part report, finding APT units of more than 70 specialists and targets in governments, telecommunications and educational institutions in at least 17 countries, including NATO members.³¹

Third, sabotage preparation through pre-positioning. In 2024 it emerged that the group Volt Typhoon had lurked undetected for months in US energy, water and communications infrastructure, steal-

ing no data, purely positioning itself for the event of conflict.³² The switch is already installed and Beijing need only flip it. How far such access can reach was shown by Salt Typhoon, which in autumn 2024 held months-long access to the mobile networks of the US carriers AT&T, Verizon and Lumen, compromising the very interfaces that US authorities use for court-authorised surveillance.³³ German mobile operators are legally required to keep the same access provisions available. Whether they are adequately secured against state-sponsored actors is an open question. Cyber is thus a systemic enabler: what the infrastructure vector (V) embeds, the cyber vector can activate.

VII. Universities as a Gateway

The infiltration of Germany's research landscape is among the most consequential vectors, hard to see and shielded by institutional openness. In May 2026 the Federal Prosecutor General had two people arrested on suspicion of scouting scientists for a Chinese intelligence service at eight German universities across six states. They posed as interpreters to lure professors to China. A high-performance drone-technology chair at RWTH Aachen was searched,³⁴ after Correctiv had already linked 19 RWTH professors to Chinese military institutions. More troubling still is the June 2026 CISA case. Saarbrücken's leading cybersecurity institute stands suspected of channeling know-how to China via Chinese scientists and funding. In one research group, 18 of 19 members were reportedly of Chinese origin, prompting a special investigator and a freeze of all China projects.³⁵

Beyond espionage, Confucius Institutes function as a structural medium of influence. Unlike the British Council or the Goethe-Institut, they are often located directly at host universities, in Germany usually as registered associations jointly sponsored by a partner university and a Chinese one. This proximity breeds self-censorship. Researchers dependent on Chinese funding, partnerships or invitations avoid Tibet,

Taiwan or Xinjiang. Again, they are not expressly instructed to do so, they are instead incentivised to self-align.

The CCP's Thousand Talents Programme (2008) completes the picture, luring leading scientists worldwide with above-market pay into cooperation with Chinese institutions, the implicit exchange being technology transfer through legitimate channels, and has been classified by the FBI and the US Department of Justice as a knowledge-theft vehicle.

VIII. Networks of Alignment: Influence Without Instructions

Influence that commits no crime and leaves no evidence is the most effective and the kind for which Germany is worst prepared. Beijing's UFWD-linked organisations cultivate parliamentary friendship groups, business-association networks and city partnerships as institutionalised access points. This way Beijing can influence matters so that whoever has economic ties to China, depends on cooperation or receives invitations, begins to avoid China-critical statements on their own accord.³⁶ Especially effective is the revolving door, former officials and members of the Bundestag moving into China-linked advisory structures and handing Beijing insight into German positions, entirely legally.

Kiel illustrates the municipal level. Schleswig-Holstein's capital, a hub for German submarine construction with a naval base and defence firms, was negotiating a partnership with Qingdao – a major Chinese naval hub with key submarine facilities. The local center-right Christian Democratic Union (CDU) council group suspended the initiative in 2023, citing concerns that China's "elementary interest" in defence know-how made such an institutional partnership inappropriate.³⁷ The case highlights how municipal partnerships can inadvertently create channels for influence-building and potential intelligence-gathering, while local decision-makers are often insufficiently prepared for such risks.

IX. Narratives and Networks: Two Levels, One System

Information operations serve Beijing's domestic and external goals simultaneously. Externally, Chinese state media (CGTN, Global Times, Xinhua) aim at elite seeding. Journalists, think-tank staff and advisers adopt framings without identifying the source. For Germany, the relevance lies less in direct public persuasion than in shaping the policy environment in which decisions on China, technology dependencies, and security risks are made. Particularly relevant is the documented amplification of Russian narratives. In early 2022 Chinese officials were retweeted by Russian diplomats more than 140 times (nearly tenfold the prior rate) and Chinese embassies, including Paris, amplified Russian denials of war crimes in Bucha.³⁸ There is also documented synergy on COVID-19 origins, Taiwan, and Ukraine arms deliveries.³⁹

Internally, Beijing runs extraterritorial control over the diaspora. The unofficial "overseas police stations" documented by Safeguard Defenders in five German cities are parallel structures outside any German legal framework. They serve to intimidate active diaspora members, pressure returns and to mobilise the community around desired narratives.⁴⁰ The Federal Foreign Office demanded their closure in November 2022; yet an RTL/ntv investigation in December 2024 found the numbers and contacts of the officially closed stations still reachable.⁴¹ As the China expert Mareike Ohlberg (German Marshall Fund) puts it, the sign can be unscrewed but the networks behind it persist.⁴² WeChat adds a digital surveillance layer that drives self-censorship among Chinese users.

X. The Power of Combination

The six vectors are analytically separable but operationally intertwined and their effect is multiplicative. Each lowering the cost or raising the yield of the others.

The underlying logic is simple. Access creates options, and options can become leverage. Access and knowledge reinforce one another: economic entanglement (IV) opens access to companies and research;

academic infiltration (VII) supplies the knowledge that makes Chinese manufacturers competitive, creating the market position from which infrastructure dependency (V) grows.

The cyber vector (VI) potentiates all the rest. It supplies the reconnaissance that makes economic pressure precise, extracts what academic espionage cannot obtain legally, and in a crisis activates what infrastructure has prepared. Pre-positioning is the technical bracket between V and VI. And the “soft” vectors safeguard the “hard” elite networks (VIII) and information operations (IX) cause no direct harm, but dampen the political response to everything else. Meanwhile China’s reach into international standard-setting (Section II) means tomorrow’s rule-writer need not fear today’s defences.

From this follows the central analytical point: Chinese influence cannot be countered vector by vector. A measure addressing only the infrastructure vector (an inverter ban, say) leaves untouched the economic, academic and discursive base from which the next dependency grows. This is where the structural advantage of the UFWD approach (Section III) lies: it is organised on a whole-of-state basis, whereas Germany’s risk mitigation remains fragmented amongst departments.

XI. The Openness Paradox: Why Germany Is Vulnerable

Germany is not Beijing’s preferred European target by chance, four structural features make it especially vulnerable. Precisely because they are also its strengths as a liberal democracy. Federalism creates information silos where responsibilities are distributed, intelligence is not always systematically shared, and a common situational picture is often lacking. Critical infrastructure protection is further divided among actors such as various ministries, the Federal Office for Information Security (BSI), the Federal Office of Civil Protection and Disaster Assistance (BBK) and the providers. Intelligence services and law enforcement operate separately under the principle of separation. An actor operating across multiple states and jurisdictions therefore does

not face a single counterpart with a comprehensive picture, but rather a fragmented system in which relevant information exists but is not always effectively aggregated and shared.

Further, Germany's openness is an attack surface. Academic freedom, investment openness, press freedom and civic connectivity are core values that create precisely the access points a patient, systemic actor exploits. The paradox of liberal democracies is that their greatest strengths are at once their greatest attack vectors. Germany's vulnerability stems less from insufficient capabilities than from the interaction between openness, fragmentation and deep economic interdependence.

Germany's consensus-oriented decision-making complicates matters further. Once significant economic interests are at stake, political compromise can dilute security-driven positions. The COSCO case illustrated this dynamic: despite objections from the relevant security ministries, the cabinet approved a compromise allowing the investment to proceed. Historically Germany has exercised goodwill without reciprocity, from *Ostpolitik* to "change through trade." This extended China the benefit of the doubt for decades; the 2023 China Strategy corrects this, naming China for the first time a "systemic rival,"⁴³ though consequences follow only hesitantly.

XII. From Recognition to Resilience

The six vectors, together with China's reach into international standard-setting, are components of a mutually reinforcing system and Germany is responding. The 2023 China Strategy, the BKG attribution, tighter investment screening. But these are reactive and fragmented measures, while the Merz government's revised China Strategy is still awaited. What is missing is a response that coordinates across departmental and federal boundaries, recognises patterns across the vectors, and musters the will to bear short-term costs for long-term resilience. Five recommendations follow.

1. Establish a cross-departmental China coordination unit, modelled on the British “China Taskforce,” to bring regular joint situational assessments and defence strategies together within the National Security Council. Without institutional linkage, information keeps vanishing into silos.
2. Decouple critical infrastructure from Chinese hardware. The dependency on Chinese inverters, port cranes and wind turbines is a security-policy time bomb. As Waterkant shows, absent systematic vetting security is left to chance. The government must introduce binding certification and vendor-independence rules for all critical-infrastructure-relevant devices and a timetable for phased replacement in sensitive network segments.
3. Anchor a research-security framework in law, since CISPA and RWTH show voluntary commitments fail. Institutions should be obliged to vet high-risk cooperation, report risk-relevant projects to the BfV, and designate institutional responsibility, without treating academic freedom and security as opposites.
4. Apply investment screening consistently, including at municipal level. The Foreign Trade and Payments Act protects critical infrastructure when applied. COSCO shows political will is the bottleneck, and the Kiel–Qingdao case shows how naive local politics opens entry points later secured only at federal cost.
5. Sharpen public threat awareness. Germany’s greatest weakness is cognitive. China is still seen primarily as an economic partner and not a systemic rival – a reflex reinforced by the turn away from Washington. The government should publish regular public reports on Chinese influence, analogous to the annual domestic-intelligence report but China-specific and policy-oriented. An unnamed threat cannot be countered.

Each individual case appears manageable in isolation, but together they alter the strategic calculus by making accommodation seem easier than resistance. Germany’s challenge is therefore not only to defend against

visible attacks, but to recognise how incremental access can translate into strategic vulnerability. We must preserve the openness of our liberal democracy without allowing accumulated access to become strategic leverage.

References

- 1 M. Zenglein and M. Huotari, “Caught in Transition: Germany’s Dilemma over Strategic Recalibration with China” (Berlin: Mercator Institute for China Studies and Hinrich Foundation, May 2025), <https://merics.org/sites/default/files/2025-05/Germany%E2%80%99s%20dilemma%20over%20strategic%20recalibration%20with%20China%20-%20MERICS%20-%20Hinrich%20Foundation%20-%20May%202025.pdf>.
- 2 Alicia García-Herrero, “What Is Behind China’s Dual Circulation Strategy?,” working paper (Natisis; SSRN No. 3927117), September 1, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927117.
- 3 Switzerland Global Enterprise, “‘Made in China 2025’ and China’s Evolving Industrial Policy,” November 4, 2025, <https://www.s-ge.com/en/article/expertise/2022-e-china-c5-industrial-policy>.
- 4 A. Gross and M. Muriga, “Inside China’s Controversial Mission to Reinvent the Internet,” *Financial Times*, March 27, 2020, <https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f>.
- 5 Charles Parton, “What Is the United Front Work Department?,” *Observing China / Council on Geostrategy*, December 16, 2024, <https://www.observingchina.org.uk/p/the-investigator-03-2024>.
- 6 Alex Joske, “The Party Speaks for You: Foreign Interference and the CCP’s United Front System,” Policy Brief Report No. 32/2020 (Canberra: Australian Strategic Policy Institute, June 9, 2020), <https://www.aspi.org.au/report/party-speaks-you/>; Alexander Bowe, “China’s Overseas United Front Work: Background and Implications for the United States” (Washington, D.C.: U.S.-China Economic and Security Review Commission, August 24, 2018), <https://www.uscc.gov/research/chinas-overseas-united-front-work-background-and-implications-united-states>.
- 7 Alex Joske, “Testimony before the U.S.-China Economic and Security Review Commission: China’s Global Influence and Interference Activities,” March 23, 2023, https://www.uscc.gov/sites/default/files/2023-03/Alex_Joske_Testimony.pdf.
- 8 Joske, “The Party Speaks for You.”
- 9 Christopher Walker and Jessica Ludwig, “Sharp Power: Rising Authoritarian Influence” (Washington, D.C.: National Endowment for Democracy, 2017), p. 13 ff., <https://www.ned.org/wp-content/uploads/2017/12/Introduction-Sharp-Power-Rising-Authoritarian-Influence.pdf>.
- 10 Christopher Walker, “What Is Sharp Power?,” *Journal of Democracy* 29, no. 3 (2018): 9–23, <https://doi.org/10.1353/jod.2018.0041>.

- 11 Atlantic Council, "Germany's Policy on China: From Win-Win to Strategic Competition" (Washington, D.C.: Atlantic Council, November 10, 2025), <https://www.atlanticcouncil.org/in-depth-research-reports/report/germanys-policy-on-china-from-win-win-to-strategic-competition/>.
- 12 Deutscher Bundestag, "Antwort der Bundesregierung: COSCO-Beteiligung am Hamburger Containerterminal" [Federal Government reply: COSCO stake in the Hamburg container terminal], Drucksache 20/7022 (May 25, 2023), <https://dserver.bundestag.de/btd/20/070/2007022.pdf>.
- 13 J. Matthes and M. Fritsch, "Auswirkungen der Sanktionen Chinas gegen Litauen auf die EU" [The effects of China's sanctions against Lithuania on the EU], IW-Kurzbericht No. 4 (Cologne: Institut der deutschen Wirtschaft, January 28, 2022), <https://www.iwkoeln.de/studien/manuel-fritsch-juergen-matthes-auswirkungen-der-sanktionen-chinas-gegen-litauen-auf-die-eu.html>; J. Ammann, "Chinesischer Druck macht litauischen Unternehmen zu schaffen" [Chinese pressure weighs on Lithuanian companies], *Euractiv*, January 19, 2022, <https://euractiv.com/de/news/chinesischer-druck-macht-litauischen-unternehmen-zu-schaffen/>.
- 14 Milda Seputyte and O. Crook, "Lithuania Expects Improvement in China Ties Within Six Months," *Bloomberg*, June 18, 2026, <https://www.bloomberg.com/news/articles/2026-06-18/lithuania-agrees-to-chinese-diplomatic-office-after-taiwan-row>.
- 15 M. Kessler, "Sabotagegefahr: Könnte China deutsche PV-Anlagen abschalten?" [Sabotage risk: could China switch off German PV installations?], *ZDF*, February 8, 2025, <https://www.zdf.de/nachrichten/wirtschaft/photovoltaik-windkraft-china-internet-zugriff-blackout-100.html>.
- 16 Kessler, "Sabotagegefahr."
- 17 *t-online*, "Behörde warnt vor Hacker-Angriffen auf Solaranlagen" [Agency warns of hacker attacks on solar installations], August 25, 2025, https://www.t-online.de/heim-garten/aktuelles/id_100884582/blackout-gefahr-in-deutschland-bsi-warnt-vor-ungesicherten-solaranlagen.html.
- 18 Kessler, "Sabotagegefahr."
- 19 Statistisches Bundesamt, "Stromerzeugung aus Photovoltaik und Erdgas erreicht im Jahr 2025 neue Höchstwerte" [Electricity generation from photovoltaics and natural gas reaches new highs in 2025], press release no. 073, March 6, 2026, https://www.destatis.de/DE/Presse/Pressemitteilungen/2026/03/PD26_073_43312.html.
- 20 Business Insider Deutschland, "China könnte Windturbinen als politisches Druckmittel gegen Deutschland einsetzen, warnen Experten" [China could use wind turbines as political leverage against Germany, experts warn], March 4, 2025, <https://www.businessinsider.de/wirtschaft/wie-sich-deutschland-mit-windturbinen-aus-china-erpressbar-macht/>; D. Wetzel, "Jetzt erreicht die Angst vor Chinas Einfluss die Windparks in der deutschen Nordsee" [Now the fear of China's influence reaches the wind farms in the German North Sea], *Welt*, August 29, 2025, <https://www.welt.de/wirtschaft/weltplus/plus68ac64328c33b226bcae76be/Offshore-Windkraft-Jetzt-erreicht-die-Angst-vor-Chinas-Einfluss-die-deutsche-Nordsee.html>.

- 21 M. Kunzmann, "Unterseekabel: Strategisches Tauziehen zwischen den USA und China" [Undersea cables: a strategic tug-of-war between the US and China], *Telepolis*, November 10, 2024, <https://www.telepolis.de/article/Unterseekabel-Strategisches-Tauziehen-zwischen-den-USA-und-China-10003950.html>; H. Alamarzooqi, "Wired for Dominance: China's Undersea Cable Strategy," *TRENDS Research & Advisory*, August 8, 2025, <https://trendsresearch.org/insight/wired-for-dominance-chinas-undersea-cable-strategy/>.
- 22 A. Sawall, "Geheimdienstkreise: Zerstörung der Ostsee-Seekabel im Auftrag Russlands" [Intelligence circles: destruction of the Baltic Sea cables on Russian orders], *Golem.de*, December 13, 2024, <https://www.golem.de/news/geheimdienstkreise-zerstoerung-der-ostsee-seekabel-im-auftrag-russlands-2412-191695.html>.
- 23 T. Kuhn, "Sicherheitsbehörden warnen: Vernetzte Autos aus China können Spionagewerkzeug werden" [Security authorities warn: connected cars from China can become spying tools], *WirtschaftsWoche*, February 4, 2026, <https://www.wiwo.de/technologie/mobilitaet/sicherheitsbehoerden-warnen-vernetzte-autos-aus-china-koennen-spionagewerkzeug-werden/100197169.html>.
- 24 C. Maintz, "Spionage-Potenzial: Innenministerium hat China-Stromer genau im Blick" [Espionage potential: interior ministry keeps a close eye on Chinese EVs], *Auto Motor und Sport*, February 12, 2026, <https://www.auto-motor-und-sport.de/verkehr/spionage-potenzial-innenministerium-hat-china-stromer-genau-im-blick/>.
- 25 Ecomento.de, "Angst vor Chinas Autos: Jetzt trifft Peking der eigene Bann" [Fear of China's cars: now Beijing is hit by its own ban], *t-online*, February 12, 2026, https://www.t-online.de/mobilitaet/aktuelles/id_101144108/e-autos-aus-china-und-spionage-bundeswehr-und-bnd-erlassen-parkverbot.html.
- 26 A. Egozi, "Spionageverdacht: IDF verbannt chinesische Autos" [Espionage suspicion: IDF bans Chinese cars], *Defence-Network*, November 2025, <https://defence-network.com/spionageverdacht-idf-verbannt-china-autos/>.
- 27 *t-online*, "Daten in Gefahr? Geheimdienst warnt: Keine vertraulichen Gespräche im Auto," [Data at risk? Intelligence agency warns: No confidential conversations in the car], June 9, 2026, https://www.t-online.de/mobilitaet/aktuelles/id_101281576/spionage-durch-vernetzte-autos-geheimdienst-warnt-vor-geheimen-gespraechen.html.
- 28 Bundesministerium des Innern, "Schwerer Cyberangriff auf das Bundesamt für Kartographie und Geodäsie ist staatlichen chinesischen Angreifern zuzuordnen" [Serious cyberattack on the Federal Agency for Cartography and Geodesy attributable to state-controlled Chinese attackers], press release, July 31, 2024, <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/07/cyberangriff-bkg.html>; M. Holland, "Cyberspionage: Chinesische Gruppe hat deutsche Kartographiebehörde gehackt" [Cyber espionage: Chinese group hacked German cartography agency], *Heise Online*, August 31, 2023, <https://www.heise.de/news/Cyberspionage-Chinesische-Gruppe-hat-deutsche-Kartographiebehoerde-gehackt-9291268.html>.
- 29 Bundesamt für Verfassungsschutz, "BfV Cyber-Brief Nr. 01/2021 – Hinweis auf aktuelle Angriffskampagne," January 18, 2021, https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2021-01-bfv-cyber-brief.pdf?__blob=publicationFile&cv=10.

- 30 Bundesamt für Verfassungsschutz, “Verfassungsschutzbericht 2025” [Annual report on the protection of the constitution 2025], 2026, <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/verfassungsschutzberichte/2026-06-30-verfassungsschutzbericht-2025.html>.
- 31 Bundesamt für Verfassungsschutz, “BfV Cyber Insight: Die i-Soon-Leaks – Industrialisierung von Cyberspionage” [The i-Soon leaks – industrialisation of cyber espionage], Parts 1–4, August 2024, <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-08-01-bfv-cyber-insight-teil-1.html>.
- 32 Cybersecurity and Infrastructure Security Agency, National Security Agency, and Federal Bureau of Investigation, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,” Joint Cybersecurity Advisory AA24-038A, February 7, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.
- 33 *The New York Times*, “Unrestrained’ Chinese Cyberattackers May Have Stolen Data From Almost Every American,” September 4, 2025, <https://www.nytimes.com/2025/09/04/world/asia/china-hack-salt-typhoon.html>.
- 34 T. Eckert, M. Bernhard, and M. Murphy, “Von München bis Aachen: Im Netz der China-Agenten” [From Munich to Aachen: in the web of China’s agents], *Correctiv*, May 21, 2026, <https://correctiv.org/hybride-kriegsfuehrung/2026/05/21/von-muenchen-bis-aachen-im-netz-der-china-agenten/>; n-tv, “Wissenschaftsspionage für China? Zwei Verdächtige gefasst” [Academic espionage for China? Two suspects arrested], May 20, 2026, <https://www.n-tv.de/wirtschaft/Wissenschaftsspionage-fuer-China-Zwei-Verdaechtige-gefasst-id30840539.html>.
- 35 MSN, “Insider: China-Kontakte des Cisca-Instituts werden untersucht” [Insider: CIPSA institute’s China contacts under investigation], after Reuters, June 22, 2026, <https://www.msn.com/de-de/nachrichten/politik/insider-china-kontakte-von-cisca-institut-werden-untersucht-sonderpr%C3%BCfer-eingesetzt/ar-AA26gxM5>. [MSN link dead, see backup: <https://de.marketscreener.com/boerse-nachrichten/insider-china-kontakte-des-cisca-instituts-werden-untersucht-ce7f5cd3de8ff027>.]; M. Benninghoff, “Warum Chinas Forschungsmodell Risiken für Deutschland birgt” [Why China’s research model poses risks for Germany], *Handelsblatt*, June 25, 2026, <https://www.handelsblatt.com/politik/international/sicherheit-warum-chinas-forschungsmodell-risiken-fuer-deutschland-birgt-01/100235083.html>.
- 36 Bowe, “China’s Overseas United Front Work.”
- 37 CDU-Ratsfraktion Kiel, “Vorbereitungen einer Städtepartnerschaft mit Qingdao stoppen” [Halt the preparations for a city partnership with Qingdao], April 26, 2023, <https://www.cdu-ratsfraktion-kiel.de/artikel/vorbereitungen-einer-staedtepartnerschaft-mit-qingdao-stoppen>; K. Büchenbacher and R. Hoffer, “Deutschlands Chinapolitik: Kiel beerdigt Partnerschaft mit Qingdao” [Germany’s China policy: Kiel buries partnership with Qingdao], *Neue Zürcher Zeitung*, July 22, 2023, <https://www.nzz.ch/international/deutschlands-chinapolitik-kiel-beerdigt-partnerschaft-mit-qingdao-ld.1746598>.
- 38 U.S. Department of State, “How the People’s Republic of China Amplifies Russian Disinformation,” Foreign Press Center briefing, April 27, 2022, <https://2021-2025.state.gov/briefings-foreign-press-centers/how-the-prc-amplifies-russian-disinformation/>.

- 39 European External Action Service, “1st EEAS Report on Foreign Information Manipulation and Interference Threats” (Brussels: EEAS, July 2, 2023), <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>.
- 40 Safeguard Defenders, “110 Overseas: China’s Transnational Policing Gone Wild” (Madrid: Safeguard Defenders, September 2022), p. 4 ff., <https://safeguarddefenders.com/sites/default/files/pdf/110%20Overseas%20%28v5%29.pdf>.
- 41 M. Frenzel, “China betreibt weiter geheime Polizeistationen in Deutschland” [China continues to operate secret police stations in Germany], *n-tv*, November 27, 2024, <https://www.n-tv.de/politik/China-betreibt-weiter-geheime-Polizeistationen-in-Deutschland-article25392467.html>.
- 42 Radio Free Asia, “China yet to close two overseas police stations in Germany after official request,” March 16, 2023, <https://www.rfa.org/english/news/china/germany-police-stations-03162023154300.html>.
- 43 Bundesregierung, “Strategie der Bundesregierung zu China” [The Federal Government’s strategy on China] (Berlin, 2023), <https://www.auswaertiges-amt.de/resource/blob/2608578/810fdade376b1467f20bdb697b2acd58/china-strategie-data.pdf>.



Beyond the Mirage: A Decade of UK-China Relations and the Price of Asymmetry

Luke de Pulford

Ten years ago, British foreign policy toward the People's Republic of China (PRC) was anchored in a brand of economic romanticism that, in retrospect, verged on the negligent. 2015 marked the high-water mark of the so-called 'Golden Era' of UK China relations. This was the heady period where successive British administrations operated under the assumption that commercial integration would naturally bind Beijing to the rules-based international order. We were told that by opening our critical national infrastructure, welcoming capital into our premier universities, and rolling out the red carpet for Chairman Xi, the United Kingdom would secure a prosperous, post-imperial future as China's 'best partner in the West'.¹

A decade later, that illusion has collapsed. Marketed as a symbiotic partnership, the UK/China bilateral has revealed itself to be a structural asymmetry, deliberately exploited by the Chinese Communist Party (CCP) to engineer dependence and erode institutional resilience. The British experience is not unique, but it is uniquely instructive for a European audience. As the continent grapples with its own economic dependencies, the UK's trajectory from enthusiastic cheerleader to exposed, reactive outlier offers a stark lesson: in the geopolitical calculus of modern Beijing, commercial engagement is never merely economic; it is the frontline of a sophisticated strategy of political subversion, narrative control, and institutional capture.

The structural vulnerability of the United Kingdom was not an accident of geography or market forces; it was permitted by a naive China strategy that systematically ignored the clearly and repeatedly stated direction of travel in Beijing. While Whitehall focused on short-term capital inflows, the CCP was executing a long-range blueprint for global industrial hegemony.

This was explicitly articulated by Xi Jinping in 2020 during a speech to the Central Financial and Economic Affairs Commission. Xi was clear that China must ‘pull tight the reins of global supply chains’ and develop ‘killer technologies’ to ‘foster industrial dominance and dependency among foreign nations’.² This was not the language of a ‘win-win’ stakeholder; it was an explicit declaration of asymmetric economic warfare.

UK assumption	CCP reality
Market integration: Open market access will foster liberalisation and turn Beijing into a responsible stakeholder.	Interdependence as a strategic tool: Turning supply chains into political leverage.
Academic partnerships: Joint endeavours and funding will benefit British research institutions.	Intellectual co-option: Broad-scale IP appropriation and enforcement of extra-territorial compliance.
Critical infrastructure partnerships: Welcoming investment will mitigate capital shortfalls.	Structural leverage: Securing long-term leverage over vital systems, including energy, transport, AI, water, communications.

The UK ignored these warnings, allowing deep dependencies to develop across critical sectors. Our higher education funding model became dangerously reliant on Chinese tuition fees, turning British universities into hotspots for intellectual property transfer and battlegrounds for free speech.³ In infrastructure, the state permitted Chinese state-owned enterprises to embed themselves into the civil nuclear power supply chain, most notably at Hinkley Point C and through initial stakes in Sizewell C.⁴ Eventually, the state woke up to the security implications, but, by this time, the cost of unwinding these relationships had bal-

looned, leaving the UK with diminished resilience and a civil service culturally conditioned to prioritise perceived commercial benefit over national security.

The most insidious element of Beijing's operations in the UK has been the systematic deployment of elite capture. This is not to be conflated with traditional notions of espionage; it is the sophisticated cultivation of influential figures across politics, business, and media to act as domestic amplifiers for Beijing's interests, or at least to be less inclined to resist the policy aims of the Party-State. The objective is what the CCP calls United Front work, an amorphous, state-directed effort to neutralize opposition and control the narrative within foreign democracies.⁵

The scale of this capture was brought into sharp focus by the MI5 Security Service Interference Alert regarding Christine Lee, a solicitor who had successfully penetrated the highest levels of the Westminster establishment, donating hundreds of thousands of pounds to Members of Parliament to facilitate access for state-linked actors.⁶ Yet, the political sphere is only one corridor of influence. The corporate and media sectors remain highly vulnerable to proxy acquisitions designed to secure narrative dominance. A prime example is the protracted turmoil surrounding the sale of the Daily Telegraph. The bid by private equity firm RedBird Capital Partners was thrown into chaos following revelations concerning its chairman, John Thornton, and his extensive, high-level engagements with senior CCP officials, including Cai Qi, a member of the Politburo Standing Committee.⁷ Lawmakers rightly warned that allowing an individual with such deep connections to the Chinese state apparatus to control a major national newspaper posed a severe threat to media independence and national security.⁸ Happily, the bid was eventually withdrawn.

This strategy relies on the revolving-door culture of British public life, where former politicians and senior civil servants routinely transition into lucrative advisory roles for firms heavily entangled with Chi-

nese state capital, effectively laundering Beijing's geopolitical objectives through respectable British voices. What emerges is an environment where explicit espionage is largely unnecessary; narrative control is maintained via economic incentives and pre-emptive structural compliance.

Beyond the boardrooms and corridors of power, the United Front strategy operates an extensive grassroots infrastructure within the UK, which, in addition to influence and interference activities, is designed to monitor, intimidate, and suppress dissident voices. Among other institutions, the United Front infrastructure operates through Chinese Students and Scholars Associations on campus and, most egregiously, illicit Overseas 'Police' stations operating under the guise of administrative service centres.⁹

These stations are among the physical infrastructure of Transnational Repression. They allow the Chinese security state to project its authoritarian reach directly into British towns and cities, monitoring critics, threatening their families back home, and enforcing a chilling effect on democratic participation.¹⁰ For years, the UK was structurally and legally ill-prepared to confront this hybrid threat. Recent legal and legislative developments indicate an overdue shift in posture. The National Security Act 2023 significantly modernised the UK's counter-espionage framework, introducing new offenses for foreign interference and providing law enforcement with the tools necessary to prosecute state-backed actors.¹¹

This new framework seems to be working. The UK recently witnessed landmark prosecutions under the Act involving individuals connected to the Hong Kong Economic and Trade Office in London, proving that the state is finally willing to disrupt state-sponsored intelligence and surveillance operations on British soil.¹² Despite these successes, the threat remains highly adaptive, hidden within the banality of localised associations and commercial fronts that defy easy legal categorization.

Campaigners for Brexit foresaw an independent foreign policy capable of defending the rules-based international order. The reality, however, has been one of economic exposure and weakened state leverage. Stripped of the collective economic power of the European Single Market, the UK has found itself vulnerable to bilateral coercion by Beijing.

This structural weakness has generated a pervasive culture of pre-emptive self-censorship within Whitehall. The most damning indictments of this timidity is the government's continued failure to publish the comprehensive China Audit, a cross-departmental review intended to map the UK's systemic dependencies on the PRC, and permitting Beijing to build the largest embassy in Europe in the heart of London.¹³ The audit remains buried, precisely because its findings would expose the extent of British vulnerability and demand economic adjustments that a fragile state is reluctant to make. As Jonathan Holslag observed, the UK's independent China policy has frequently degenerated into a series of uncoordinated, defensive maneuvers, paralysed by the fear of economic retaliation.¹⁴

This paralysis is also evident in the implementation of the Foreign Influence Registration Scheme (FIRS), introduced by the National Security Act 2023. While FIRS was designed to mandate transparency for foreign state activity, the government has stubbornly hesitated to place China in the scheme's enhanced tier, a designation reserved for countries posing a direct risk to national safety, which currently applies only to jurisdictions like Iran and Russia.¹⁵ By failing to place the PRC in the enhanced tier, the UK has failed to name the elephant in the room, allowing Chinese state-controlled entities to continue operating across British industry without the strict disclosure requirements applied to other adversarial states. It is worth noting that, according to the architect of the legislation, Tom Tugendhat MP, the National Security Act was designed with China particularly in mind. Consequently, strategic blueprints like the 2023 Integrated Review Refresh, which labe-

led China an epoch-defining challenge, rather than a clear threat, have been exposed as rhetorical exercises unsupported by regulatory teeth.¹⁶

The British experience over the past decade demonstrates the perils of unilateral engagement with an authoritarian superpower. It proves that a middle power, acting alone, cannot successfully navigate economic integration with a state that weaponises commercial interdependence as a matter of national doctrine.

For a European audience, the lessons are clear. The vulnerabilities exposed in London are present in Paris, Berlin, and Brussels. The solution cannot be found in isolated national policies, which Beijing easily exploits through divide and rule diplomacy. Instead, European security demands absolute alignment around the de-risking framework championed by European Commission President Ursula von der Leyen.¹⁷ True collective resilience requires deep regulatory harmonisation across the Channel and the Continent. We must build unified, legally binding frameworks to address supply chain vulnerabilities, mandate rigorous corporate due diligence against state-backed forced labour, and implement strict security screenings for critical infrastructure investment.¹⁸ The UK's decade of drift should serve as a warning: without collective regulatory solidarity, democratic societies will continue to see their institutions captured, their security compromised, and their autonomy quietly leased away.

References

- 1 HM Government, *The UK-China Relations: A Strategic Partnership Agreement* (London: The Stationery Office, 2015), p. 12.
- 2 Xi Jinping, 'Certain Major Issues Regarding China's Current Long-Term Economic and Social Strategy', *Qiusbi*, November 16, 2020.
- 3 House of Commons Foreign Affairs Committee, 'Autocracies and UK Universities: Responding to Foreign Interference', HC 114 (London: Parliament, 2021), pp. 24–28.
- 4 Intelligence and Security Committee of Parliament, 'China', HC 1603 (London: The Stationery Office, 2023), p. 54.
- 5 Alexander Bowe, 'China's Overseas United Front Work: Background and Implications for the West' (Washington, D.C.: U.S.-China Economic and Security Review Commission, 2018), p. 5.

- 6 MI5 Security Service, 'Interference Alert: Christine Ching Kui Lee' (London: MI5, January 2022).
- 7 *The Guardian*, 'Telegraph Sale in Turmoil after Lead Bidder Linked to China's Politburo', October 29, 2025.
- 8 Domino Theory, 'Telegraph Takeover Called Into Question Over China Links', July 18, 2025.
- 9 Safeguard Defenders, '110 Overseas: Chinese Transnational Policing Gone Wild' (Madrid: Safeguard Defenders, 2022), pp. 14–17.
- 10 Freedom House, 'Defending Democracy in Exile: Understanding and Responding to Transnational Repression' (Washington, D.C.: Freedom House, 2022), p. 33.
- 11 National Security Act 2023, c. 32, Part 4, Foreign Influence Registration Scheme.
- 12 Crown Prosecution Service, *R v. Yuen et al.* (Central Criminal Court) (London: CPS Case Report, 2024).
- 13 Council on Geostrategy, 'Mapping Dependency: The Missing UK-China Audit' (London: CoG Publishing, 2024), p. 8.
- 14 Jonathan Holslag, *The Silk Road Trap: How China's Trade Strategy Is Reshaping the World* (Cambridge: Polity Press, 2021), p. 142.
- 15 Home Office, 'Foreign Influence Registration Scheme (FIRS): Guidance for Implementation' (London: Government Digital Service, May 2025).
- 16 HM Government, 'Integrated Review Refresh 2023: Responding to a More Volatile and Contested World', Cm 811 (London: The Stationery Office, 2023), p. 31.
- 17 Ursula von der Leyen, 'Speech on EU-China Relations to the Mercator Institute for China Studies' (Brussels: European Commission, March 30, 2023).
- 18 European Parliament, 'Directive on Corporate Sustainability Due Diligence and Its Geopolitical Implications' (Brussels: European Parliament Research Service, 2024), p. 19.



Chinese Influence and Espionage Activities in Denmark

Jeanette Serritzlev

“China and the Chinese Communist Party’s global ambitions and willingness to challenge the West are also reflected in the threat landscape in Denmark.”

The quote is from the Danish Security and Intelligence Service’s (DSIS) latest national assessment of the espionage threat.¹ There are frequent public discussions in Denmark regarding Chinese espionage and the risks of using Chinese equipment such as surveillance cameras.² As in many other European countries, the potential risks from TikTok have been a subject of political and public discussion.³ But what have we actually seen in Denmark? That is the purpose of this chapter to examine.

Denmark-China Relations

In the spring of 2023, the Danish Minister of Foreign Affairs Lars Løkke Rasmussen introduced an approach to foreign policy guided by “pragmatic idealism.”⁴ A few months later, before the minister went on an official trip to China, Rasmussen elaborated on the need for that approach in regards to China, summarized in this quote: “*We must be critical of a number of China’s global ambitions and their political system, while cooperating on trade and climate. This requires a committed, clear-sighted and realistic China policy.*”⁵ That frames the Chinese-Danish relationship in a nutshell.

On the one hand, China's cooperation with Russia and support in different means for Russia's war in Ukraine means a greater divide between China and the West. On the other hand, the more tense relationship between Trump's USA and the EU also means that the EU as a whole, as well as Denmark specifically, has chosen to adopt a more pragmatic position towards China. For both the EU and China, there is a mutual interest in cooperation on trade and on agendas such as climate. China is the EU's third largest trading partner for goods and services combined, while the EU is China's largest trading partner.⁶ China is also Denmark's third largest export market and second largest import market outside the EU, based on 2024 figures.⁷

In 2008, China and Denmark agreed on the establishment of a Comprehensive Strategic Partnership,⁸ and in 2023, a new Green Joint Work Programme was ratified, focusing on cooperation between the countries regarding sustainable green transition across sectors. This includes, among others, areas such as Climate and Energy, Environment and Water, and Food and Agriculture.⁹

Despite the mutual interests in cooperation, the Danish Defence Intelligence Service (DDIS) assesses in its yearly public threat assessment that China continues to conduct espionage in order to acquire technology from countries such as Denmark, making what DDIS calls "extensive knowledge-transfer," *"the greatest threat to Danish research, innovation and technology."*¹⁰

The Arctic Dimension: Greenland & the Faroe Islands

The Kingdom of Denmark consists of three parts: Denmark, Greenland, and the Faroe Islands. While foreign and security policy remains a matter for Copenhagen, large infrastructure and commercial decisions are devolved to Nuuk and Tórshavn – and it is precisely where some of the most well-documented examples of Chinese pressure within the Realm can be found. Where attributable Chinese influence activities are difficult to pinpoint in Denmark proper, the Arctic parts of the

Realm offer several concrete cases in which the Danish government has actively intervened.

Although there has been a lot of talk of Chinese companies showing interest in Greenland, it has not so far translated into concrete results, according to the DDIS, elaborating that China is expected to continue pursuing cooperation with Greenland within fields of research as well as commercially.¹¹ Some cases, however, are worth having a closer look at.

Greenland has attracted Chinese commercial and strategic interest for more than a decade. In 2016, the Danish government took the abandoned naval station Grønnedal in southern Greenland off the market after the mining company General Nice had expressed interest in buying it; the Ministry of Defence instead chose to reactivate the facility.¹²

The pattern repeated itself on a larger scale in 2018, when the Chinese state-owned China Communications Construction Company (CCCC) was shortlisted by the Greenlandic company Kalaallit Airports to bid on the construction of new airports in Nuuk, Ilulissat and Qaqortoq. The prospect of a Chinese state-owned enterprise building critical infrastructure close to the American Thule Air Base (today Pituffik Space Base) caused concern in both Copenhagen and Washington.¹³

The Danish government subsequently agreed in September 2018 to co-finance the airports through equity and loans. CCCC withdrew its bid in June 2019.¹⁴ None of these cases constitutes influence operations in a narrow sense. They do, however, demonstrate two things: that China pursues long-term strategic positioning through commercial means in the Arctic part of the Realm, and that the Danish state is willing to intervene, quietly and with considerable sums, when it considers such positioning a security concern.

The clearest documented example of coercive Chinese diplomacy within the Kingdom, however, comes from the Faroe Islands. In November 2019, the Chinese ambassador to Denmark, Feng Tie, held

meetings with leading Faroese politicians, including the prime minister (løgmaður) Bárður á Steig Nielsen. According to an audio recording obtained by the Faroese broadcaster Kringvarp Føroya – accidentally capturing the trade minister’s conversation with his permanent secretary – the ambassador had stated a clear message: If the Faroese telecommunications company Føroya Tele chose Huawei as supplier of the islands’ 5G network, a free trade agreement between the Faroe Islands and China, of great importance to Faroese salmon exports, would be within reach. If not, there would be no agreement.¹⁵ The Faroese government obtained a court injunction against the broadcaster minutes before the story was to air, and the case only became public when Berlingske and DR reported on it in December 2019. China has subsequently denied that any pressure had been exerted.¹⁶

China’s Carrot & Stick Approach

Traditionally, China has used both ‘carrot and stick’ in the country’s diplomatic approach, including in regard to Denmark. This mix of carrots (rewards) and sticks (punishments) has proven effective in shaping, or restraining, the opponent’s room for maneuver – taking Panda Diplomacy as one well-known example.

The well-known digital ‘Wolf Warriors’, often Chinese diplomats adopting a highly offensive online discourse, attacking every critique of the Chinese Communist Party’s policies, have not been a real issue in Denmark. However, Jakobsson and Okholm coin the intuitively decodable term ‘Shadow Wolf Warriors’ in a case-study to describe a strategy used beyond the public eye, in Erving Goffman’s terms ‘backstage’, and examine examples of this in a Danish context.¹⁷ The then chairman of the Foreign Policy Committee, MP Søren Espersen describes such a situation in an opinion piece in the Danish newspaper Jyllands-Posten: The Foreign Policy Committee was on a visit to Beijing, where it had come to the knowledge of the Chinese hosts that the exiled Prime Minister of Tibet would be visiting the Danish Parliament. Espersen

recalls: *“We received a verbal warning from a Chinese minister, and I was instructed by him – as chairman of the committee and party colleague of the Speaker of the Folketing – to tell her to say no to the visit.”*

After his return, Søren Espersen did in fact meet with the exiled Prime Minister of Tibet, resulting in a phone call from the Chinese embassy, angrily protesting that the meeting had taken place. *“It was just a phone call,”* Espersen writes. *“China never leaves a trace when they threaten and harass.”*¹⁸

Panda Diplomacy & the Battle of a Map

During a state visit to China in 2017, the then prime minister Lars Løkke Rasmussen met the two pandas that were going to be leased to Copenhagen Zoo. In a Facebook post, the then prime minister explicitly connects the “panda diplomacy” with a greater interstate relationship: The pandas are a *“cute symbol of Danish-Chinese friendship”* and mentions in the same post that Denmark is *“easing visa procedures and making it easier to attract Chinese tourists to Denmark.”* It is hardly a secret that the Panda Diplomacy is about more than pandas. The interesting part of this is, however, the explicit correlation between the “cute symbols” and “real diplomacy.”

The pandas arrived at Copenhagen Zoo in 2019. Shortly before the opening, a Chinese delegation had a tour of the panda facilities in the zoo, noticing that Taiwan was marked as an independent country on a map. Unsurprisingly, that caused a harsh reaction from the Chinese delegation. The Kingdom of Denmark supports a One China Policy, and the Copenhagen Zoo changed the sign. However, maybe as a small kind of protest, the Zoo not only changed the sign, but also the map it was showing: The Zoo zoomed in completely on the Chinese mainland, and thus Taiwan does not appear at all on the map. The Zoo’s scientific director Bengt Holst explained the decision as such: *“In this way, we avoid taking a position either one way or the other.”*¹⁹

New Year & Cultural Power

While Russian disinformation and propaganda can be observed in the Danish information environment, Chinese influence works by different means. Other soft power initiatives such as Chinese New Year celebrations and Confucius Institutes at educational institutions have also been used in Denmark. The New Year celebration was a huge event in Copenhagen for years, but also outside the capital region in cities such as Sønderborg in the southern part of Denmark. Confucius Institutes were opened at Copenhagen Business School (2007) and Aalborg University (2009), and “*Confucius classrooms*” were established at Danish upper secondary schools.²⁰ As of today, one Confucius Institute is still up and running in Denmark, at the International Business Academy in the city of Kolding. According to the academy itself, this “*collaboration, across all of the different activities we organize, enables participants to bring different cultures closer together, and to gain a better understanding of the Chinese culture and lifestyle.*”²¹ The upper secondary school EUC Nord has also resumed its Chinese cooperation in 2024,²² despite earlier political criticism.²³

The Chinese Diaspora

In the 2023 national assessment of the espionage threat, the Danish Security and Intelligence Service describes how the Chinese authorities attempt to exercise control over Chinese living in Denmark. According to the Danish Security and Intelligence Service, the objective is partly to strengthen the relationship between the Chinese Communist Party and Chinese living abroad, and partly to monitor and mitigate critique of the Communist Party.²⁴ This regime does not only focus on people living abroad on a permanent basis, but also on Chinese exchange students.²⁵ A central tool in this effort is the United Front, which is directly subordinate to the Communist Party’s Central Committee. According to the Danish Security and Intelligence Service, the United Front is also active in Denmark.²⁶ The United Front network works through dif-

ferent organisations, among other means. According to Jakobsson and Okholm, “*United Front activities in Denmark thus includes both (synthetic) civil society associations and official intergovernmental cooperation.*”²⁷

Espionage & Influence

Chinese intelligence services and organizations affiliated with the Communist Party are used to influence foreign policymakers, including in Europe and Denmark.²⁸ The threat from Chinese intelligence manifests from a wide range of actors and is aimed first and foremost against certain types of Danish technology and research and against Chinese residents in Denmark, especially Chinese dissidents.²⁹

Both DSIS and DDIS currently assess China as a real intelligence threat to Denmark. It is, however, important to distinguish between documented espionage, suspicions of industrial espionage and more general security concerns. One of the cases of concern covered in the media is from Aalborg University, where researchers, together with the company Hikvision, developed an algorithm that can be used for mass surveillance.³⁰ In 2021, the Danish newspaper Politiken reported how a Chinese talent program had been recruiting top researchers in Denmark’s wind turbine industry for several years. According to the FBI, the talent program has been used specifically for industrial espionage. At least some of the Danish researchers working within this program had done so without informing their employers.³¹ Probably the most prominent case of espionage allegations concerns the Chinese company Huawei, regarding the Danish telecommunications company TDC: In 2019, TDC became convinced that the Chinese company Huawei was monitoring TDC in an attempt to win a contract for a 5G network ahead of the Swedish company Ericsson. The monitoring allegedly included a mole inside TDC, covert listening devices – and a surveillance drone.³² TDC chose Ericsson in 2019, and Denmark subsequently tightened investment screening and supplier security requirements — showing that the cases had policy consequences.

Chinese transfer of knowledge and technology takes place especially in areas that China prioritizes strategically, which among other things include quantum research, artificial intelligence, robotics, bio- and medical technology, maritime technology, space technology and green technology. This exploitation can be conducted through research cooperation.³³ In 2024, DSIS warned of Chinese espionage.³⁴

The threat from cyber espionage from Russia and China is assessed as very high in the 2025 assessment, which states that Russia and China in particular are continuously targeting Danish organizations with cyberattacks in an attempt to gain information regarding foreign and security policy as well as Denmark's defense.³⁵

While China has been involved in election interference abroad, there is, according to the Swedish National China Centre, no evidence of sustained campaigns to influence elections in Europe.³⁶ This is in line with the public threat assessment prior to the 2026 Danish general election, which addresses the threat from actors from Russia, the USA, and China. While it is assessed as *“possible that Russia will carry out influence activities in an attempt to exploit the elections to advance Russian agendas,”* it is *“less likely that China will prioritize influencing Denmark specifically in connection with the general elections.”*³⁷

Conclusion

The threat from espionage is explicitly addressed in the public publications from respectively the Danish Defence Intelligence Service (DDIS) and the Danish Security and Intelligence Service (DSIS), and it is a regular part of the political and public discussions. When trying to pinpoint specific attributed grey or covert activities, it becomes, however more complex. This makes the Faroese case that more interesting. It shows the carrot and the stick fused into a single instrument: The trade agreement offered as reward and its withdrawal as punishment. It shows influence exercised precisely where Jakobsson and Okholm locate it – in the shadow, backstage, and leaving no trace except, in this

instance, a microphone that happened to be live. It also shows that parts of the Kingdom of Denmark, where economic dependencies are greater and the security policy apparatus is far away in Copenhagen, potentially constitutes an attack surface, pressure can be applied on.

In contrast to Russia, Denmark and China have a strategic partnership, including research activities and commercial interests. Denmark has a “pragmatic-idealistic approach” to its foreign policy, including towards China. While the espionage threat is obvious and real, the Chinese interest in influencing the public narrative or decision-makers in the Kingdom of Denmark is primarily pursued through means of soft power, using Shadow Wolf Warriors when needed, and exercising control over the diaspora, limiting criticism of the Chinese Communist Party.

References

- 1 Danish Security and Intelligence Service (DSIS), “Vurdering af spionagetruslen mod Danmark 2023” [Assessment of the espionage threat against Denmark 2023] (DSIS, 2023), p. 7, https://pet.dk/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vurdering-af-spionagetruslen-mod-danmark-2023_dk_web.pdf.
- 2 E. V. S. Jensen, “Alle kameraer fra Kina var væk, sagde Troels Lund – men det var forkert” [All cameras from China were gone, said Troels Lund – but that was wrong], *TV 2*, June 17, 2026, <https://nyheder.tv2.dk/politik/2026-06-17-alle-kameraer-fra-kina-var-vaek-sagde-troels-lund-men-det-var-forkert>.
- 3 K. S. Ørbæk, “Forskere advarer om, at Kina kan bruge TikTok som våben” [Researchers warn that China can use TikTok as a weapon], *TV 2*, March 25, 2023, <https://nyheder.tv2.dk/udland/2023-03-25-forskere-advarer-om-at-kina-kan-bruge-tiktok-som-vaaben>.
- 4 L. L. Rasmussen, “Vores politik skal være styret af ’pragmatisk idealisme’” [Our policy must be guided by ‘pragmatic idealism’], op-ed originally published in *Altinget*, May 17, 2023, republished by the Danish Ministry of Foreign Affairs, <https://um.dk/om-os/ministrene/udenrigsministeren/udenrigsminister-lars-loekke-rasmussen/vores-politik-skal-vaere-styret-af-pragmatisk-idealisme/>.
- 5 L. L. Rasmussen, “Vi vil føre en klarsynet og realistisk Kina-politik” [We will pursue a clear-sighted and realistic China policy], op-ed originally published in *Jyllands-Posten*, August 15, 2023, republished by the Danish Ministry of Foreign Affairs, <https://um.dk/om-os/ministrene/udenrigsministeren/udenrigsminister-lars-loekke-rasmussen/vi-vil-foere-en-klarsynet-og-realistisk-kina-politik/>.

- 6 European Council, "Handel mellem EU og Kina: Fakta og tal" [Trade between the EU and China: facts and figures], accessed August 26, 2026, <https://www.consilium.europa.eu/da/infographics/eu-china-trade/>.
- 7 Folketingets EU-Oplysning [Danish Parliament's EU Information Service], "International handel i tal" [International trade in figures], accessed August 26, 2026, <https://www.eu.dk/da/temaer/frihandel-og-vaekst/international-handel-i-tal>.
- 8 Danish Ministry of Foreign Affairs, "Joint Statement Between the Government of the People's Republic of China and the Government of the Kingdom of Denmark on the Establishment of a Comprehensive Strategic Partnership," 2008, <https://um.dk/media/awgjq02a/cn-dk-joint-statement-on-the-establishment-of-a-strategic-partnership.pdf>.
- 9 Danish Ministry of Foreign Affairs, "Green Joint Work Programme between the Government of the People's Republic of China and the Government of the Kingdom of Denmark 2023–2026," 2023, <https://um.dk/media/t2edqc54/green-joint-work-programme-23-26-eng.pdf>.
- 10 Danish Defence Intelligence Service (DDIS), "Intelligence Outlook 2025" (DDIS, 2025), p. 48.
- 11 DDIS, "Intelligence Outlook 2025," p. 37.
- 12 M. Breum, "Stoppede Løkke kinesisk opkøb i Grønland?" [Did Løkke stop a Chinese acquisition in Greenland?], martinbreum.dk, 2016, <https://www.martinbreum.dk/stoppede-loekke-kinesisk-opkoeb-i-groenland/>.
- 13 T. Jensen, "Greenland Shortlists Chinese Company for Airport Construction Despite Denmark's Concerns," *Reuters*, March 27, 2018, <https://www.reuters.com/article/world/greenland-shortlists-chinese-company-for-airport-construction-despite-denmarks-idUSK-BN1H32XG/>.
- 14 Reuters, "China Withdraws Bid for Greenland Airport Projects: Sermitsiaq Newspaper," June 4, 2019, <https://www.reuters.com/article/business/china-withdraws-bid-for-greenland-airport-projects-sermitsiaq-newspaper-idUSKCN1T5190/>.
- 15 T. Foght, "Hemmelig lydoptagelse: Kina pressede Færøerne til at vælge Huawei" [Secret audio recording: China pressured the Faroe Islands to choose Huawei], *DR*, December 10, 2019, <https://www.dr.dk/nyheder/indland/hemmelig-lydoptagelse-kina-pressede-faer-oerne-til-vaelge-huawei>.
- 16 L. Winther, S. Kruse, and M. Danielsen, "Kina afviser afpresning på Færøerne: »Det bunder i en skjult dagsorden«" [China denies coercion in the Faroe Islands: 'It stems from a hidden agenda'], *Berlingske*, December 11, 2019, <https://www.berlingske.dk/internationalt/kina-afviser-afpresning-paa-faeroerne-det-bunder-i-en-skjult-dagsorden>.
- 17 A. K. Jakobsson and C. S. Okholm, "Chinese Influence in the Kingdom of Denmark: Shadow Wolf Warrior—Directing the Backstage, Shunning the Frontstage," in *China's Influence in the Nordic–Baltic Information Environment: Denmark and Lithuania* (Riga: NATO Strategic Communications Centre of Excellence, 2026), p. 53.
- 18 S. Espersen, "Kina truer Danmark – igen og igen" [China threatens Denmark – again and again], *Jyllands-Posten*, December 25, 2018, <https://jyllands-posten.dk/debat/international/ECE11085570/kina-truer-danmark-igen-og-igen/>.

- 19 DR, "Kina fik Københavns Zoo til at bortredigere Taiwan fra verdenskort" [China got Copenhagen Zoo to edit Taiwan out of a world map], August 8, 2019, <https://www.dr.dk/nyheder/indland/kina-fik-koebenhavns-zoo-til-bortredigere-taiwan-fra-verdenskort>.
- 20 Sinolytica, "Fra ulvediplomati til Chinamaxxing: Er Kina ved at blive cool?" [From wolf diplomacy to Chinamaxxing: is China becoming cool?], March 18, 2026, <https://www.sinolytica.dk/fra-ulvediplomati-til-chinamaxxing-er-kina-ved-at-blive-cool/>.
- 21 IBA Erhvervsakademi Kolding, "IBA Confucius Institute – International Education," accessed August 24, 2026, <https://iba.dk/international/confucius/>.
- 22 EUC Nord, Facebook post, 2024, <https://www.facebook.com/eucnord.dk/photos/efter-en-lang-pause-p%C3%A5-fem-%C3%A5r-er-vi-glade-for-at-kunne-annoncere-genstarter-af-v/1087704876211099/>.
- 23 P. Witten, "EUC Nord beskyldes for at bruge kinesisk propaganda" [EUC Nord accused of using Chinese propaganda], *Nordjyske*, July 20, 2020, <https://nordjyske.dk/nyheder/nordjyl-land/euc-nord-beskyldes-for-at-bruge-kinesisk-propaganda/6553cf60-64a5-43d4-8c3a-81716e6cef1c>.
- 24 DSIS, "Vurdering af spionagetruslen mod Danmark 2023," p. 16.
- 25 Ibid.
- 26 Ibid.
- 27 Jakobsson and Okholm, "Chinese Influence in the Kingdom of Denmark," p. 55 ff.
- 28 DDIS, "Intelligence Outlook 2025," p. 51.
- 29 DSIS, "Vurdering af spionagetruslen mod Danmark 2023," p. 16.
- 30 S. S. Kjeldtoft, "Aalborg Universitet har hjulpet omstridt kinesisk firma, der bidrager til forfølgelse og overvågning af millioner" [Aalborg University has helped controversial Chinese company that contributes to the persecution and surveillance of millions], *Politiken*, June 23, 2020, https://politiken.dk/internationalt/int_kina/art7835507/Aalborg-Universitet-har-hjulpet-omstridt-kinesisk-firma-der-bidrager-til-forf%C3%B8lgelse-og-overv%C3%A5gning-af-millioer.
- 31 S. S. Kjeldtoft, "Flere danske forskere har arbejdet for Kina uden at sige det til deres arbejdsplads" [Several Danish researchers have worked for China without telling their employers], *Politiken*, May 2, 2021, <https://politiken.dk/danmark/art8186958/Flere-danske-forskere-har-arbejdet-for-Kina-uden-at-sige-det-til-deres-arbejdsplads>.
- 32 S. Neupert and Ritzau, "TDC genkender dele af historie om kinesisk spionage" [TDC recognises parts of story about Chinese espionage], *TV2*, June 16, 2023, <https://nyheder.tv2.dk/business/2023-06-16-tdc-genkender-dele-af-historie-om-kinesisk-spionage>.
- 33 DSIS, "Vurdering af spionagetruslen mod Danmark 2023," p. 17.
- 34 M. Juhl, "PET advarer om kinesisk spionage. Alligevel fortsætter danske universiteter med at sende studerende til Kina" [PET warns of Chinese espionage. Danish universities nevertheless continue to send students to China], *Uniavisen*, September 13, 2024, <https://uniavisen.dk/pet-advarer-om-kinesisk-spionage-alligevel-fortsætter-danske-universiteter-med-at-sende-studerende-til-kina/>.
- 35 Styrelsen for Samfundssikkerhed [Danish Agency for Societal Security], "Trusselsvurdering: Cybertruslen mod Danmark 2025" [Threat assessment: the cyber threat against Denmark 2025] (Styrelsen for Samfundssikkerhed, 2025), p. 6.

- 36 A. von Sydow, "China's Foreign Election Interference: An Overview of Its Global Impact," Swedish National China Centre, 2024, <https://kinacentrum.se/en/publications/chinas-for-eign-election-interference-an-overview-of-its-global-impact/>.
- 37 Danish Defence Intelligence Service and Danish Security and Intelligence Service, "Truslen fra påvirkningsaktiviteter mod folketingsvalget 2026" [The threat from influence activities against the 2026 general election], 2026, <https://www.fe-ddis.dk/globalassets/fe/dokumenter/2026/trusselsvurderinger/-truslen-fra-pavirkningsaktiviteter-.pdf>.

Conclusion & Recommendations

The hybrid and grey zone landscape – in our region to a large extent carved out by Russia – is in 2026 becoming more clearly defined and addressed. When assessing other actors, a rightly handling of the established foreknowledge and insights could indeed be a great advantage for us. However, the complexity of interrelations between these actors, the integration and overlapping activities between them, and to the individual differences in its craftings, makes the overall challenge also growingly demanding.

In order to successfully tackle the hybrid threats and attacks on our countries, societies at large, including populations, institutions, businesses, politics and so on, all desperately need to have a similar understanding of the threats and the actors posing them. A mature comprehension of the hostilities is the only reliable way to secure both the short and long term upholding of our democracies, as it is *democracy per se* (and not its “side-departments” or expressions) that undemocratic actors are targeting.

The way forward when it comes to dealing with China both as an enabler and actor in the hybrid theatre involves, among other things: revising current knowledge about hybrid events that do not make it to the centre of the debate, applying historical gained knowledge to new situations and contexts, identifying the long term influence aimed at brittling down our resistance, and fostering a culture of collective action, readiness and endurance (encompassing all of Europe, and all democratic societies).

Recommendations below should not be regarded as exhaustive. Some of which have been touched upon and explored in the anthology include:

Prepare for Russia-China Strategic Sync

- Plan for simultaneous crises in Europe and the Indo-Pacific. A major China contingency could constrain US submarines, air and missile defence, long-range strike, ISR, lift and munitions even if Washington remains committed to Europe.
- Build European capacity to manage a Russian contingency with less immediate US combat power through stronger logistics, ammunition stocks, air and missile defence, industrial output and resilient command structures.

Integrate China Expertise and Strategic Warning

- Break up governmental silos through cross-departmental China co-ordination and joint situational assessments. In different national contexts this can imply different actions. Build a fused Russia-China warning picture linking political and military contacts, exercises, defence-industrial flows, cyber activity, infrastructure incidents and Chinese pressure in the Indo-Pacific. Treat China as both an enabler for Russia and a hybrid actor in its own right.

Protect Infrastructure, Research and Societal Resilience

- Treat reinforcement infrastructure as part of the defence architecture. Ports, railways, energy systems, telecommunications, data centres and undersea cables require cyber defence, redundancy, counter-sabotage and rapid attribution.
- Anchor research security in law by requiring institutions to vet high-risk cooperation, report relevant risks and assign clear responsibility, without treating academic freedom and security as opposites.
- Deepen collective protection of undersea cables and other critical infrastructure through the Nordic-Baltic Eight, additional working formats with Poland, Germany, in the whole of EU, and NATO, as well as within coalitions and with other free countries at large.

Counter Interference and Win the Information Phase

- Give foreign-interference policy regulatory strength. Sharpen public threat awareness and crisis communication through regular China-specific reporting and pre-planned strategic communication for ambiguous hybrid incidents. Passive process language cedes the information space when public attention is at its highest.

De-Risk Economic and Technological Dependencies

- Align European de-risking efforts because isolated national policies invite divide-and-rule. Use common rules for supply-chain vulnerabilities, corporate due diligence and security screening of critical infrastructure investment.
- Apply investment screening consistently, including locally, and assess cumulative access rather than individual transactions in isolation. Commercial, research and municipal ties can together create strategic leverage.
- Reduce high-risk technology dependencies through binding certification and vendor-independence rules for sensitive infrastructure, with phased replacement where necessary.

Invest in Future Resilience and Strengthen our Strategic Outlook

- Strengthening democratic systems from within includes education and investment in a wider range of competencies, including languages, history, culture, cognitive sciences, and more, in addition to economics, technology, STEM etc. Cultivating a more sophisticated long-term strategic outlook on not just foreign policy but on international relations in a variety of contexts (research, business, global environments) more broadly speaking, is essential in order to be able to face adversaries on today's borderless global battlefields centered on information, where psychology, attention and identity are driving and motivating factors.

Afterword from Konrad-Adenauer-Stiftung

The contributions to this publication make clear that the central challenge in addressing hybrid threats is not simply to identify and counter individual activities. What matters is understanding the connections between economic dependencies and political influence, between research and security, between critical infrastructure and strategic vulnerabilities, and between physical incidents and the struggle to shape their interpretation.

Open societies are particularly vulnerable in this regard. Their strength lies in the free flow of information, academic freedom, international interconnectedness and pluralistic debate. Yet it is precisely this openness that can be deliberately exploited – through economic and technological dependencies, research cooperation, social networks, or the targeted engagement of political and societal actors.

Artificial intelligence further expands the possibilities for hybrid influence. Disinformation can be produced and disseminated faster, more cheaply and with greater precision. Deepfakes, automated campaigns and personalised content can amplify existing divisions within societies and undermine trust in the media, public institutions and democratic processes. The ability to assess information, identify manipulation at an early stage and communicate credibly in times of crisis is therefore becoming an essential element of societal resilience.

Russia and China pursue different strategies and should not be treated as identical actors. Their activities can, however, complement and

reinforce one another. Europe must therefore also be prepared for situations in which military, economic, technological and informational pressure occurs simultaneously.

The answer, however, cannot be isolation. Europe's open societies, academic freedom, economic interconnectedness and culture of democratic debate are not weaknesses to be abandoned. They are essential foundations of our political and economic strength. But openness requires an awareness of risks, clear rules and the ability to set boundaries. De-risking therefore does not mean ending relationships, but identifying and reducing dependencies where they threaten our political or security-related freedom of action.

No European democracy can meet this challenge alone. National measures remain necessary, but they are insufficient in the face of cross-border supply chains, research networks, digital infrastructure and information spaces. For the Nordic and Baltic countries, Germany and their European partners, closer cooperation is therefore particularly important – within the EU and NATO, in the Nordic-Baltic framework, and together with other democratic partners.

Ultimately, this is about more than countering individual hybrid activities. It is about the ability of democratic societies to remain capable of acting over the long term: to identify risks early, bring together knowledge and act collectively even under pressure.

Resilience is therefore not a capability that can be achieved once and for all, but a continuous task. It requires vigilance, institutional learning and strategic foresight – and, above all, a willingness to combine the openness of our democracies with the determination to protect them.

Christine Leuchtenmüller,
Konrad-Adenauer-Stiftung,
Resident Representative to the Nordic Countries.

Editor



Anna Rennéus Guthrie is Director of the think tank Stockholm Free World Forum (Frivärld). With a background as a journalist and opinion leader, she explores the connections between fields that are often considered separately. Her recent work has focused on Ukraine and the future of European and transatlantic security, the influence of authoritarian states, and the changing relationship between economic interdependence and security, including in relation to China. She examines how cultural and societal forces shape security and foreign policy, in addition to how information can be weaponized and used as a tool of influence. Her broader work is rooted in the defence of liberal values, including democracy, free speech, free media, market economics and the rule of law.

Authors



Dr Una Aleksandra Bērziņa-Čerenkova is a China scholar and a discourse analyst. She serves as Director of the Latvian Institute of International Affairs and Head of the Global Studies Centre at Riga Stradins University. She has held research fellowships at Fudan, Stanford, Oxford and Hokkaido Universities, and is affiliated with King's College London and MERICS. Dr. Bērziņa-Čerenkova publishes on PRC political discourse, contemporary Chinese ideology, EU-China relations, Russia-China, the Baltics and hybrid threats. She is the author of 'Perfect Imbalance: China and Russia' (World Scientific, 2022) and the editor of 'Discourse, Rhetoric and Shifting Political Behaviour in China' (Routledge, 2023).



Ferdinand A. Gehringer has been Director and Lead Defense & Security at FTI Consulting Germany since January 2026. In this role, he advises companies and international organizations on issues of economic and corporate security (including protection against sabotage and espionage, cybersecurity, and geopolitical dependencies), as well as on defense and security policy matters. He occasionally serves as an expert to the German Bundestag, most recently on the implementation of the NIS2 Cybersecurity Directive and on disinformation campaigns conducted by autocratic states. Ferdinand Gehringer is a co-author of the book 'Deutschland im Ernstfall' (Germany in a State of Emergency) and is a licensed attorney as well as a certified mediator. In addition, he is a Non-Resident Fellow at the Institute for Security Policy at Kiel University. Between March 2021 and December 2025, he worked at the Konrad Adenauer Foundation, initially as a Policy Advisor for International Law and Public International Law and as Coordinator of the Foundation's Rule of Law Programs.



Patrik Oksanen is a resident senior fellow at Stockholm Free World Forum (SFWF), with responsibility for CIDA (Center for Influence and Disinformation Analysis) at SFWF. Oksanen is a member of the Royal Swedish Academy of War Sciences and Royal Swedish Society of Naval Sciences and is also associated with the Centre of Societal Security at the Swedish Defense University. He appears regularly as a columnist and commentator for various Swedish media. Oksanen has a background as a TV journalist and political editor, and has written extensively on matters related to security, total defense and influence operations. The most recent books are 'Den sista lögnen – Estonia och den ryske spionens arv' (The Last Lie – Estonia and the Legacy of the Russian Spy) and 'Rysslands hemliga krig mot Sverige' (Russia's Secret War Against Sweden).



Luke de Pulford is the founder and Executive Director of the Inter-Parliamentary Alliance on China (IPAC), which comprises more than 300 lawmaker members from 45 legislatures – the largest and most active organisation of its type in the world, seeking to reform the approach of democracies towards China. He previously co-founded the anti-slavery charity Arise, which he ran from its inception until 2022. He is well known among global parliamentarians for his long-standing work in defence of human rights.



Jeanette Serritzlev is a military analyst at the Royal Danish Defence College, specialising in hybrid warfare and Information Warfare. Jeanette holds a Master's degree in Communication Studies, and another in Military Studies. She is also the author of a book about Information Warfare in Modern Warfare (2023) and the contributor to other books and reports.

