FRIVÄRLD

KONRAD ADENAUER STIFTUNG

BOUND TOGETHER: SHARED CHALLENGES IN THE BALTIC SEA REGION

KATARINA TRACZ (ED.)

BOUND TOGETHER:
SHARED CHALLENGES IN THE BALTIC SEA REGION

Bound Together:
Shared Challenges in the Baltic Sea Region

KATARINA TRACZ (ED.)

This work has been funded and implemented by Konrad-Adenauer-Stiftung Nordic Countries Project and the Stockholm Free World Forum

Published by Stockholm Free World Forum and Konrad-Adenauer-Stiftung
Cover: Mikael Eisen
Layout: Tina Selander
Print: F4 Print
Stockholm 2021
ISBN: 978-91-7703-277-9

Contents

Foreword

When thinking about the history and development of the Baltic Sea region, I recall my stay as representative of the Konrad Adenauer Stiftung (KAS) in St. Petersburg, Russia until 2005. Economic and environmental issues in the Baltic Sea countries as well as political interconnections could still be discussed in those days at international conferences in Russia. At that time, the importance of cooperation in the Baltic Sea region was from a Russian viewpoint considered of importance even for other regions, such as the Black Sea.

Russian politics have since changed tremendously. For instance, the faculty of International Relations at the St. Petersburg State University is not allowed to conduct any conferences with international guests or partners. As a result of these unfortunate restrictions on Russian international academic cooperation, this anthology cannot present an independent Russian view. We acknowledge, however, that we should continue trying to connect with Russian civil society under the auspices of future projects in the region.

For centuries, the Baltic Sea region has harboured economic opportunities and cultural exchanges, as the period of the Hanseatic League demonstrates. On the other hand, continued environmental and security challenges in the region must be faced and resolved through joint efforts.

Many far-reaching political and economic changes have taken place in the history of the Baltic Sea region. The end of the Cold War started a new era of unparalleled regional development.

Today, the Baltic Sea region is arguably the most integrated and prosperous region in the world, and the extent of regional cooperation is unprecedented. The political development started with the 1992 establishment of the Council of the Baltic Sea States (CBSS), a joint German-Danish initiative. The purpose of CBSS was to support political cooperation in the region in order to ease the transition to new post-Cold War dynamics in the region. The work of the CBSS is guided by three long-term priorities: creating a regional identity, sustainability and prosperity, and security. Since then, the Baltic Sea Region has gone through a political re-definition: the EU enlargement of 2004 and the 2009 launch of the EU Strategy for the Baltic Sea Region (EUSBSR) defined and established a European macro-region. The EUSBSR once more underlines the significance and importance of the Baltic Sea Region for European development and integration. Focusing on environmental protection, economic and political cooperation – as well as security and regional connectivity – the Baltic Sea Region has become a model for regional cooperation and development.

Nevertheless, the region also faces challenges in environmental protection and energy policy, with the Nord Stream projects for instance creating much dissent among neighbouring countries. In addition, the ongoing strained relations between the EU and Russia and diverging security concerns must be addressed through a common understanding of threats. The effects of climate change and the re-shaping of global politics make regional cooperation more necessary than ever. The mutual opportunities and challenges facing the Baltic Sea region clearly bind our countries together. Therefore, the title of this anthology is all the more appropriate, and these chapters aim to keep the discussion about regional cooperation alive.

Gabriele Baumann
Head of the Konrad-Adenauer-Stiftung
Nordic Countries Project

Foreword

As the title of this anthology suggests, the Baltic Sea region is indeed bound together – not just physically and geographically, but also by a shared history, present realities and common challenges that will shape our future.

In fact, this interconnectedness has only increased over the years. Since the Soviet Union's collapse 30 years ago, the region has become ever more integrated economically, culturally and politically. In the spring of 1989, I visited Estonia while it was still under Soviet occupation and left an Ericsson Hotline cellphone that – under the right weather conditions – could be used to reach the outside world through Finnish telecom networks. Today, Estonia – just like its Baltic neighbours Latvia and Lithuania – is one of the most digitally advanced societies in the world. This contributes to the fact that the economies surrounding the Baltic Sea are not only deeply integrated parts of the European Union, but make up one of the most competitive clusters of the global economy through trade, entrepreneurship, innovations, investments, data flows, financial transactions, and power grids.

The ties that bind us together ensure that a safe, stable, and prosperous Baltic Sea region is a common interest. At the same time, they create shared vulnerabilities. Although the Soviet Union is long gone, the Baltic Sea region remains a flashpoint for tensions between Russia and the West. Such tensions don't just manifest in the physical domain, but in the digital world as well. Consequently, the Baltic Sea nations face similar challenges when it comes to ensuring cyber security and countering information

threats. Moreover, the Baltic Sea region faces risks related to climate change that may cause severe damage to our environment, infrastructure, and standard of living. All of these risks are dealt with in this book.

However, we are united not only as a function of the threats we face, but even more so because of our shared values and opportunities. An even more integrated Baltic Sea region is, in today's world, fundamentally a source of strength for all of us. Taken together, the Nordic countries, the Baltic countries, and Germany constitute one of the strongest economic regions in the world, second to none regarding innovations and advanced technologies. The Baltic Sea region is an economic and industrial powerhouse that could also be an internationally leading force for the democratic values that are so deeply ingrained in our part of the world.

Thus, more cooperation between the Baltic Sea nations has tremendous potential that goes beyond regional interests. By extension, the countries that surround the Baltic Sea – successful, stable democracies – can set a course for the future of the free world. Therefore, our bonds don't just need to be nurtured, but form a joint platform for prosperity and peace in our part of the world.

Gunnar Hökmark
Chairman of Stockholm Free World Forum

Security in Northern Europe in an age of "ufred"

Dr Karsten Friis

In his book *The Virtual Weapon*, cyber security expert Lucas Kello describes our world as one in 'unpeace' – a 'mid-spectrum rivalry lying below the physically destructive threshold of interstate violence, but whose harmful effects far surpass the tolerable level of peacetime competition.'[1] In Scandinavian languages, there is a similar word: 'ufred' ('ofred' in Swedish). It depicts an unpleasant war-like situation, typically associated with mediaeval times. It has not been applied to the current security environment, but perhaps it should. Today we are neither at war, in the traditional violent sense, nor at a state of deep peace. The adversaries of the Western democracies, being authoritarian states or radical extremists, are engaging and challenging us at a regular pace. Sometimes, or at least in some sectors, we may be in a regular competitive situation; in other situations, 'crisis' may be a more correct term. The threat is on and off, non-linear and unconventional, but nonetheless represents a persistent challenge to the very basic foundations that our

1 Kello 2017, *The Virtual Weapon*, p. 78.

societies rest on: democracy, freedom of speech, transparency, free press, independent institutions.

The idea of 'ufred' is how both Russia and China think of war. They do not operate with the same sharp distinction between peace and war as Western societies traditionally have. War, in their playbook, is not limited to kinetic violence but includes political warfare, active measures, bullish diplomacy, influence campaigns and other features we hear about or experience on a regular basis. The broad toolbox has been labelled, among others, as hybrid warfare, but the point is the same: a variety of measures are applied in a concerted way at various times and at various intensities for the adversary to achieve their political objectives.

Northern Europe is exposed to this, even if strong democratic institutions and consolidated political environments have proven rather resilient when facing these threats – compared to, for instance, some countries in South-East Europe. At the same time, the proximity of Russia, the presence of significant military assets in the region, and the renewed interest from other great powers to the Arctic and Baltic Sea makes 'ufred' a fitting description here.

All Baltic and Nordic states have experienced aggressive digital campaigns targeted against parliaments, governments or critical infrastructure. For example, attempts at political influence have targeted Swedish and Finnish NATO debates, and ethnic minority questions in the Baltic states. Other examples include the infamous Russian-owned island villas in the Finnish archipelago, and Russian and Chinese attempts at buying land and industry in strategic locations. Even if not all economic activity by these countries in the Nordic-Baltic region should be regarded as a part of a cunning strategic plan, critical assessment and healthy suspicion is well advised.

What does this mean for our Nordic-Baltic security and defence?

First, it is a challenge that our public sectors remain very compartmentalized. This way of organization implies separation of power, clear constitutional responsibilities and judicial demarcations, and is advantageous for day-to-day management of the public sector. However, as we have experienced over the last six to seven years, it is less efficient when dealing with hybrid threats that earmark the 'ufred'.

It is, for instance, complicated to make a clear distinction between the role of the police and the armed forces in situations below the threshold of armed conflict. This threshold is traditionally related to violations of Article 2 in the UN charter ('use of force against the territorial integrity'), but the armed forces cannot just sit idle and wait for a war to break out.[2] The military has a role to play in deterring adversaries, influencing their behaviour, signal capacities and willingness, training and exercising with friends and allies, and supporting civil society wherever possible.

Second, in 'ufred', our armed forces must operate in peacetime more or less as in war, because the situation may change quickly. Armies cannot, as before, rely primarily on massive mobilization but must be prepared to 'fight tonight'. This is because modern technology, such as precision guided cruise missiles, gives little if any warning. At the same time, to avoid unintended escalations, it is crucial that armed forces are able to defuse a crisis rather than calling for strong reinforcements right away. These are considerations that must be carefully balanced to maintain stability.

Third, our civilian security agencies – intelligence, police, customs, coast guard, etc. – must be given relevant tools to be able to fulfil their mandates in new dimensions, such as with digital technology. They must be provided the legislative, technical and organizational capacities to be able to uncover and respond to

2 United Nations Charter, Article 2.4

advanced security risks stemming from state actors. Recent rulings by the European Court of Human Rights may guide lawmakers in providing intelligence services with what they need to conduct mass collection of digital data, while simultaneously protecting personal integrity and individual freedoms.[3]

These security agencies may also need to be reformed and reorganized, or possibly split or merged, to be better able to respond to the broad risk picture. Many of these were designed for another time, when you could draw clear distinctions between the domestic and the international spheres, and between war and peace. Hybrid threats may require hybrid responses.

Fourth, public and private sectors in general must become 'security streamlined'. This means that agencies and ministries that have not traditionally thought about security must get it into their DNA. They must begin thinking security, not only safety, and plan for the possibility of being targeted by a malign state-controlled actor. This includes almost any sector or agency in society, such as fishery management, trade agencies, property registrations, real-estate agencies, media-platforms, health services, telecom, energy companies, water supply and more. Many of these, such as telecom, have already been addressing this for several years. Others, such as water supply, may have been defined as critical national infrastructure, therefore implementing precautionary measures already. However, sectors as a whole need to adapt and prepare for the likes of digital attacks, including ransomware, such as the recent Colonial Pipeline attack in the United States.

In short, without getting paranoid, all societal sectors need to become more aware of the risks and how to discover them, respond and restore normal functionality as soon as possible. Resilience

3 See e.g. *Centrum för rättvisa v. Sweden*, May 2021, 35252/08, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13279%22]}

– today's buzzword – is a cornerstone in these efforts. The term resilience has many applications and meanings, but includes the 'bouncebackability': to be able to restore normality swiftly after an attack. Both the EU Strategic Compass process and the NATO 2030 document are engaging with this strategy. Good resilience has, in itself, a deterring effect. It is deterrence by denial: there is no point in attacking if the effect can be expected to be minimal.

Now, even if hybrid and unconventional threats have become more common, it is still the use of massive force, or organized violence, by states that represents the most dangerous scenario. This has not changed in 'ufred'. The Nordic-Baltic region is neighbour to significant Russian forces, not only in Russia but also in the Kola peninsula, Kaliningrad and Belarus. Russia's active use of force in its foreign policy in Georgia, Ukraine and the Middle East has made many nervous in the West. Since 2014, collective defence has been reinvented by NATO, which is developing more detailed defence plans for Europe. NATO membership has proven to be the best strategical choice the Baltic states achieved after the Cold War (together with EU membership). It was a window of opportunity that they utilised wisely. Even if, theoretically, the Baltic countries can still be overrun by Russian tanks, NATO's Enhanced Forward Presence (EFP) ensures that this will not happen; not because of the size of the military forces at the front, but because an attack would trigger all of NATO's total military, political and economic might.

NATO has proven to be able to reform and adopt to a changed security landscape, and, as long as the US remains committed to it, it will be the strongest alliance in the world. In addition, the US has engaged with a series of bilateral defence engagements with many Nordic-Baltic countries. Such cooperation has strengthened US commitment to the region, and it has brought Sweden and Finland even more firmly into the Euro-Atlantic security fold. There

is, today, absolutely no doubt where Sweden and Finland would stand in case of conflict with Russia. The non-aligned status is politically comfortable in peacetime, but neither Russia nor others should be fooled by it. Furthermore, it may be wise for the countries to keep the status quo. There is no need to feed the Russian 'we are encroached by NATO' paranoia. As long as Swedish and Finnish armed forces are interoperable and in tune with NATO, military planners can live with the absence of Swedish and Finnish forces in the NATO defence plans. But it is of course also the full sovereign right of Sweden and Finland to apply for NATO membership should they so desire.

Since 2014, the Nordic Defence Cooperation (NORDEFCO) has been reenergized and is now much more focused on regional security cooperation. The latest ambition is to cooperate on military planning, with alternate landing bases, military mobility, exchange of radar pictures and increased joint exercising already taking place. The cooperation between the air forces has particularly proven fruitful, with weekly joint training and the biannual Arctic Challenge Exercise. The latter comprises around 100 planes from all over NATO, plus the Swedish and Finnish ones. From a military point of view, the combined Nordic air force is formidable and is very difficult to neutralize in case of conflict. If this cooperation can be deepened and broadened to also include, for instance, air defence systems, such cooperation would be even stronger. In short, the cooperation and integration of the Nordic air forces are arguably more important for Nordic-Baltic security than NATO membership is for Sweden and Finland.

On the maritime side, the annual maritime-focused exercise in the Baltic Sea, BALTOPS, is a cornerstone of cooperation. 2021 was the 50th anniversary of its execution. Over the years, BALTOPS has grown in size and significance, and this year 16 NATO allies, plus Sweden and Finland, participated with around 4,000

personnel. Interoperability, strike operations, missile defence and defensive cyber warfare were exercised. BALTOPS contributes to keeping allied focus in the region, including the US 6th fleet which is indispensable (together with the recently re-established 2nd fleet) for the defence of Europe.

Another new feature that enhances Nordic-Baltic security is the British Joint Expeditionary Force (JEF). Originally planned as a global force, JEF currently focuses on northern Europe. The Nordic-Baltic countries have all joined JEF, providing yet another arena for enhanced defence cooperation. It also gives the region yet another layer of external security in addition to the bilateral US agreements and NATO. Brexit and the new Integrated Review and other strategic documents provides an opportunity now for the Nordic-Baltic countries to engage the UK with concrete and practical initiatives to cooperate more in the framework of JEF. The British perception of Russia is very much in line with the Nordic-Baltic countries, having experienced the Skripal attack and other incidents. The Integrated Review may indicate a rather 'global' Britain right now (with only scant mention of the EU); but, when the dust from Brexit settles, Europe will continue to be key for British security strategy.

The combined force of the Nordic-Baltic militaries is relatively small: the states are net receivers of allied assistance in case of crisis, they do not have much excess force to support each other, except with their airforces. The region therefore relies on external assistance in case of crisis. Nonetheless, the level of regular training and exercising, bilateral agreements with the US, and the NATO EFP, all function as rather good compensations. No rational military actor would mess with the region unless a serious crisis had already emerged.

Nonetheless, even if deterrence is likely to work for the Nordic-Baltic region, there is still a risk that political conflicts between

Russia and the West could escalate into a violent conflict. This could happen if the Kremlin were to pursue a more adventurous and bullish foreign policy than today – a policy which would force the West to draw a line. This is the most dangerous scenario because it implies a political leadership in Russia that is actively seeking a confrontation with the West. However, despite the increasingly paranoid and authoritarian features of today's Kremlin, trigger-happy hawks have yet to take control of the military-political echelons. Kremlin's *silovikis* do not want war; they want to stay filthy rich and in power.

Another scenario for armed conflict is an undesired escalation following an accident or misunderstanding. Given the density of Russian and Western military vessels and planes in the Nordic-Baltic region, an accidental collision cannot be ruled out; and given the very different world views of the two sides, such incidents may be interpreted differently. In such situations, with a high degree of uncertainty, stress and limited time for decision-making, tactical security dilemmas easily emerge; precautionary actions of one side are regarded as aggressive acts by the other side.

There are, however, well-established techniques to reduce the chances of such scenarios. One is the so-called 'Incident at sea', or Incsea, agreement. Several countries have such bilateral agreements with Russia, including the US. They regulate behaviour (for example, no simulated attacks), communication procedures and warning-times both at sea and in the air. Today, Norway is the only Nordic-Baltic country with such an agreement; other countries in northern Europe with a navy or airforce should establish similar systems.

NATO's 2D-approach to Russia – deterrence and dialogue – is, unfortunately, rather hollow. There is little dialogue, primarily because Russia refuses to meet in the NATO-Russia Council. NATO has cancelled all military-to-military engagement with

Russia, so, except for occasional meetings between SECEUR and the Russian Chief of Staff in Baku, Azerbaijan, the primary contact between NATO-countries and Russia is bilateral. Some countries have regular contact; other have close to none. Unfortunately, Russia tends to pursue a 'divide and rule' tactic at many occasions, seeking to drive a wedge between allies rather than genuinely search for solutions to improve relations. Nonetheless, channels of communication, informal contacts and dialogue may still be important in strained times.

Concluding remarks

The Nordic-Baltic states can live with 'ufred'. It is unpleasant at times, but not life-threatening. However, if it continues unchecked, it could erode European and transatlantic solidarity overtime leaving the countries vulnerable to violent attacks. The fact that the Biden-administration emphasises democratic values in its foreign policy should therefore be welcomed and supported by the Nordic-Baltic states. Strong democratic values are something we share, and our proximity to Belarus and Russia reminds us that none of this can be taken for granted. These values are, however, simultaneously the core ideological difference between authoritarian Russia and China, and us. Our promotion of democratic values is, from their perspective, an indirect or hybrid attack on their regimes; it makes them nervous. Still, these are our red lines. As it is stated in the Washington Treaty, the allies are determined to 'safeguard the freedom, common heritage and civilisation of their peoples, founded on the principles of democracy, individual liberty and the rule of law'.[4] Fighting to defend this is paramount – but the challenge is to do so without creating unnecessary tension

4 The North Atlantic Treaty, 1949.

or violent response. Striking this balance is at the heart of Nordic-Baltic security policies in 'ufred'.

Baltic Sea Cyber Security

Merle Maigre

The internet and the digital technologies that create cyberspace are transforming society, business and politics. People and enterprises respond to new opportunities online, react to cyber threats and change their behaviour accordingly. States compete and are increasingly weaponising information to gain advantage, breaking into other countries' networks to steal data, seed misinformation or disrupt critical infrastructure.

A variety of actors have a stake in cyber security. This is exemplified by criminal groups using ransomware for economic gain, adversaries linking espionage with data breaches and nation states using political interference. While some elements of the cyber threat have become more serious, in this chapter we first reflect on the rapidly changing cyber security landscape and discuss some key cyber threats, and secondly, describe responses that build resilience in the Baltic Sea region. We examine the present state and future potential of cyber security cooperation among the Nordic-Baltic countries and recommend a course of action.

Evolving Cyber Threat Picture

Increased Risk Due to Remote Working

The last three years have brought significant changes in the cyber threat landscape. Above all, this has been due to the unique set of factors generated by the COVID-19 pandemic. In March 2020, the pandemic led to social distancing measures and travel restrictions. The global effort to slow down infection rates caused a rapid shift to remote working.

In a short amount of time, IT security professionals had to respond to the challenges introduced by working-from-home arrangements, such as enterprise data movements whenever employees use their home internet to access cloud-based apps, corporate software, videoconferencing and file sharing.[5] Even though the hardware and software solutions may have been in place to secure an organisation's data, there were often no established policies to help employees through the jungle of threats and vulnerabilities they were to face when moving their workplace out of the traditional office environment.[6]

With a lack of appropriate guidelines, training and cybersecurity awareness, adapting to the new normal was difficult, and remote workers may inadvertently have acted in ways that exposed the business to cyber threats. Frequently reported examples of these kinds of mistakes were connecting work devices to public Wi-Fi networks, sharing corporate devices with family members without authorisation, connecting work devices to personal equipment without permission and using personal devices to access work applications and downloading unauthorised applications

5 ENISA, "Threat Landscape: The Year in Review. From January 2019 to April 2020," ETL, 2020.

6 NATO CCDCOE, "Recent Cyber Events: Considerations for Military and National Security Decision Makers," May 2021, https://ccdcoe.org/uploads/2021/05/Recent-Cyber-Events-10_May-2021.pdf.

contrary to organisational policy. All of these habits increased the risk of data exposure.

Most Vulnerable Sector: Health

According to the European Union Cybersecurity Agency (ENISA) study on main incidents in 2019–2020,[7] the most targeted sectors during this period were digital services, technology and financial industries, government administration and health. Attacks on digital service providers – such as e-mail, social and collaborative platforms and cloud providers – often served as proxies to reach other, more attractive targets. In contrast, attacks on the technology industry allowed malicious actors to compromise the supply chain or look for vulnerabilities to exploit. In the financial industry, the number of cyber incidents in financial organisations and banks increased substantially. Financial returns from ransom paid made the public sector an attractive target for ransomware attacks.

Above all, the pandemic has shown the vulnerability of the healthcare sector and of those who depend on it. Modern healthcare is deeply intertwined with technology. From the sophisticated machines used for diagnosing disease to the enterprise systems that store patient records, it is difficult to run any healthcare organisation today without heavily relying on information technology. Cyber attacks against hospitals, medical research units, medical data centres and even patients have been unprecedented. In July 2020 the British, American and Canadian intelligence services announced that a Russian state-backed hacker group known as APT 29 (also known as 'Cozy Bear' or 'the Dukes') was operating as part of the Russian intelligence services targeting British,

7 ENISA, "Threat Landscape: Main Incidents in the EU and Worldwide. From January 2019 to April 2020," https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents.

American and Canadian vaccine research and development organisations.[8] In May 2021, the Swedish Public Health Agency (*Folkhälsomyndigheten*) was investigating several attempts to hack into SmiNet, a database that stores reports of infectious diseases, including COVID-19 cases.[9]

In October 2020, a cyber attack occurred against the Psychotherapy Center Vastaamo in Finland, where sensitive information related to tens of thousands of patients was compromised. In the words of Mikko Hypponen, a researcher at the Finnish cyber security company F-Secure,

"The Vastaamo case is an example of an attacker who is motivated by money and attempting to monetise personal data by blackmailing not only healthcare institutions, but by directly contacting patients themselves."[10]

F-Secure expected this to become a trend in the near future, and the most recent ransomware cases in 2021 have demonstrated that their prediction has been correct.[11] Unlike corporate data, which is usually stored for a relatively short period, health data needs to remain always accessible, secure and private. With limited budgets and legacy systems, this is a massive challenge for the health sector. It will require both a deeper understanding of this emerging and growing threat, and a willingness to address it on all possible levels.

8 Ross Kelly, "Russian Hackers Exposed Trying to Steal Covid-19 Vaccine Research," *Digit*, 16 July 2020, https://digit.fyi/apt29-russian-hacker-group-exposed-trying-to-steal-coronavirus-vaccine-research/.

9 Ionut Arghire, "Swedish Public Health Agency Says Disease Database Targeted in Cyberattacks," *Security Week*, 1 June 2021, https://www.itsecuritynews.info/swedish-public-health-agency-says-disease-database-targeted-in-cyberattacks/.

10 F-Secure, "Attack Landscape Update," 2020, https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf.

11 Ibid.

Ransomware

The threat ecosystem keeps evolving, with attackers developing different techniques to achieve their goals. The ENISA Threat Landscape study covering the period 2019–2020 outlines that the number of incidents resulting in the theft of information, data and user credentials is the highest ever observed.[12] All across Europe, more than 620 million account details were stolen from sixteen hacked websites and offered for sale on the popular dark-web marketplace, Dream Market.[13]

Similarly, ransomware has hit the Baltic Sea states. In March 2019, the Norwegian aluminium company, Norsk Hydro, became a victim of a ransomware attack disrupting parts of production.[14] In February 2021, a major Finnish IT provider was hit with a ransomware attack that forced the company to turn off some services and infrastructure in a disruption to customers.[15] In July 2021, one of the major supermarket chains in Sweden, Coop was forced close 800 of its stores due to malfunctioning cash registers as a result of a global Kaseya ransomware attack.[16] In most cases, the intention is to steal data and information, and sell it on the dark web.

Currently, the most significant threat comes in the form of highly organised, technically proficient criminal syndicates. These pose a threat not only to countries in the Baltic Sea region but also

12 ENISA Threat Landscape, "Main Incidents in the EU and Worldwide. From January 2019 to April 2020."

13 Ibid.

14 Allan Liska, "LockerGoga Ransomware Disrupts Operations at Norwegian Aluminum Company," *Record Future*, 20 March 2019, https://www.recordedfuture.com/lockergoga-ransomware-insight/.

15 Elizabeth Montalbano, "Finnish IT Giant Hit with Ransomware Cyberattack," *ThreatPost*, 23 February 2021, https://threatpost.com/finnish-it-giant-ransomware-cyberattack/164193/.

16 Supantha Mukherjee and Colm Fulton, "Coop, other ransomware-hit firms, could take weeks to recover, say experts", 5 July 2021, https://www.reuters.com/technology/coop-other-ransomware-hit-firms-could-take-weeks-recover-say-experts-2021-07-05/

to businesses of all sizes, and even to individual citizens. These groups are trying to steal data or extort money through ransomware, which is one of the most potent threats that we face at the moment.

Ransomware attacks are becoming sophisticated not just in technical terms, but the criminals themselves appear to be studying victims. This intelligence gathering involves actively researching an organisation's turnover and profitability to estimate how much they can afford to pay. Ransomware criminals go around in circles trying doors and if the owner has been careless, the damage is quickly done. In some cases, ransomware criminals boldly advertise insiders the incentive of 40% of profit if they helped to install ransomware in their company Windows server.[17]

The Estonian Information System Authority 2021 annual review explains the logic of ransomware as follows,

"Classical ransomware attacks occur in three stages. First, an attacker installs ransomware on a victim's computer or server. Remote desktop protocol is increasingly used for this; however, a lot of malware is still sent via files and links added to e-mails. Second, the ransomware encrypts some of the files on the computer or server, or the entire hard drive. After that, the victim can no longer open their files. Third, the attacker demands a ransom for file recovery, i.e. for a decryption key, usually in some cryptocurrency, such as Bitcoin."[18]

Understanding the evolving tactics being employed by ransomware attackers is critical to mitigating this problem. One of the most significant developments in ransomware in 2020 was

17 Ravie Lakshmanan, Cybercrime Group Asking Insiders for Help in Planting Ransomware, *The Hacker News*, 20 August, 2021 https://thehackernews.com/2021/08/cybercrime-group-asking-insiders-for.html?m=1

18 Republic of Estonia Information System Authority, "Cyber Security in Estonia 2021," https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf.

the threat against target organisations to leak their stolen data and publish the exfiltrated data on a public internet site when the victim refuses to pay. This additional fear factor could be quite effective if the data is sensitive, such as a valuable trade secret or simply personal data, which would bring fines to the data holder if it became public. This is the evolution into 'ransomware 2.0'.[19]

Ransomware has become a popular weapon in the hands of malicious actors. Often an interplay occurs between financially motivated cybercriminals and nation-state hackers. Cybercriminal gangs are learning from the better-resourced nation-state groups. Likewise, the nation-state groups are borrowing from the criminal gangs – masquerading their disruptive attacks under the guise of ransomware with no indication as to whether victims will in fact get their files back in exchange for a ransom.

Espionage

But cyber security is not just about money. Another set of threats comes in the form of belligerent nation-states that seek to steal data for espionage purposes. The Baltic Sea states have recently become a high target of cyber spying.

In 2017, a report by Denmark's Centre for Cyber Security (CFCS) revealed that the emails of several Danish government agencies had been hacked by a foreign adversary and that Claus Hjort Frederiksen, who served as the Danish Minister of Defence from 2016 to 2019, accused the Russian authorities for this.[20] According to a study on cyber espionage by the Finnish Institute of International Affairs, the main factors behind the cyber espionage in the Baltic Sea region are "*First and foremost, trade espionage*

19 F-Secure, "Attack Landscape Update," 2020.

20 Eeva Haaramo, "Danish defence minister accuses Russia of cyber espionage," *Computer Weekly*, 26 April 2017, https://www.computerweekly.com/news/450417515/Danish-defence-minister-accuses-Russia-of-cyber-espionage.

against the region's advanced innovation economies and large portfolios of intellectual property; and second, information-gathering through the links that the region's states have with wider institutions and security organizations. /…/ In particular, the intellectual property of the region's communications technology, energy, shipping, bio-technology, and defence sectors provides the motivation for cyber-enabled theft."[21]

Similarly, in 2021, a Norwegian intelligence report warned that in the cyber domain, espionage is the main threat to Norway. The report maintains that "*Norwegian policy formulations – particularly relating to defence, foreign affairs and security – is of continued interest. There is similar interest in the High North and the healthcare and energy sectors. Information on contact networks and internal disagreements in Norwegian politics and Norwegian companies also has intelligence value, as this can be exploited in future operations.*"[22]

Political Interference

There are also politically-motivated cyber attacks that interfere in democratic processes and political discourse. Democratic institutions are vulnerable targets of intelligence operations. For instance, in September 2020, the email system of Norway's parliament was hacked.[23] Ine Eriksen Soreide , the Minister of Foreign Affairs of Norway, underlined the significance of the attack by calling it an important cyber incident that has an effect on the "most important

21 Mika Aaltola, "Cyber Attacks Go Beyond Espionage," FIIA Briefing Paper 200, August 2016, https://www.fiia.fi/wp-content/uploads/2017/01/bp200.pdf.

22 Norwegian Intelligence Service, "Focus 2021," https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Focus2021-english.pdf/_/attachment/inline/450b1ed0-1983-4e6b-bc65-4aa7631aa36f:21c5241a06c489fa1608472c3c8ab855c0ac3511/Focus2021-english.pdf.

23 Catalin Cimpanu, "Finland says hackers accessed MPs' emails accounts," *ZDNet*, 28 December 2020, https://www.zdnet.com/article/finland-says-hackers-accessed-mps-emails-accounts/.

democratic institution" of the country.[24] After this incident, the Norwegian authorities identified Russia as the actor responsible for the attack. This was the first time the Norwegian authorities made a political attribution to such an attack.

Around the same time that Russian hackers breached the Norwegian parliament's email system, the Finnish parliament was also the target of a cyber attack. In this instance, hackers gained entry to the internal IT system and accessed email accounts for some members of parliament. The Speaker of the Parliament described the breach as "a serious attack on our democracy and Finnish society".[25]

The 2021 annual review of the Estonian Information System Authority warned that "*Cyber attacks are often aimed at candidates or parties, not necessarily the organisers of elections. Websites of candidates and parties, their social media pages, or e-mail servers could be attacked by a foreign adversary, a domestic attacker or trolls.*"[26]

To counter this, the Cyber Security Branch of the Estonian Information System Authority provides free cyber hygiene trainings to politicians along with recommendations for improving their personal cybersecurity routines. The Information System Authority also offers a prop bono review of the security protocols of the web and email servers to any Estonian political party that cares for their cybersecurity.

24 "Norway blames Russia for cyber-attack on parliament," *BBC*, 13 October 2020, https://www.bbc.com/news/world-europe-54518106.

25 "Cyber attack in Finland hits email accounts of MPs and parliament," *Euronews*, 28 December 2020, https://www.euronews.com/2020/12/28/cyber-attack-in-finland-hits-email-accounts-of-mps-and-parliament.

26 Informatin System Authority of Estonia, *Cyber Security in Estonia 2021*, https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2021_eng_final.pdf

Supply Chain Attacks

According to the US National Institute of Standards and Technology (NIST) glossary, a supply chain attacks are "*Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, information technology products or services at any point during the life cycle.*"[27]

A report of the Atlantic Council further explains that *"A software supply chain attack occurs when an attacker accesses and modifies software in the complex software development supply chain to compromise a target farther down on the chain by inserting their own malicious code."*[28]

Such supply chain attacks often target the process by which a trusted organisation updates software for their clients. The effect of an attack on a single organisation can, thereby, be multiplied by the number of clients the organisation serves. Understanding how the supply chain may be compromised is important for organisations procuring or maintaining software so that they can assess the security measures taken across the supply chain. It is also of interest to anyone developing or customising software in-house. Any intermediary handling the software package, such as a reseller or systems integrator or even one's own IT department, may be targeted and checks need to be performed to ensure the integrity of the software through the entire chain.

Finally, there is also the question of end users. If end users are not prevented from installing software by technical security measures, they may be tricked into installing software if the attacker

27 https://csrc.nist.gov/glossary/term/supply_chain_attack

28 Trey Herr, William Loomis, Stewart Scott and June Lee, "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain," *Atlantic Council*, 26 July 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/

can make them believe that it is a legitimate software update. One example is a recently reported attempt to trick Android phone users to install malware masquerading as a system update.[29]

The use of third-party software components may bring particular vulnerabilities with it, meaning that a great degree of trust is placed in the hands of the software author possibly without transparency. However, outsourcing software production, or parts of it, and relying on code libraries, or using pre-built code, is not new and is practised by all kinds of organisations of all sizes.[30]

As an example, in December 2020, about a dozen of Swedish businesses IT systems and the Swedish Space Company became targets of a sophisticated cyber-attack. Investigators believe that the attacks started in March 2020, when a malign code was inserted in software updates and caused a malware to spread into various IT systems.[31]

Attacks Against Critical Infrastructure

Most worrying attacks occur when states or state-backed actors plan sophisticated malware as 'time bombs' in target countries' critical cyber networks, such as the energy sector, telecoms and transportation. For example, on at least two occasions – in December 2015 and 2016 – hackers have attacked Ukraine's electricity distribution system, putting thousands of citizens in the dark for extended periods of time. In a similar manner, in 2016, the Mimikatz malware that could later be linked to a Russian military intelligence service was spotted in the SCADA system of an Estonian

29 Aazim Yaswant, "New Advanced Android Malware Posing as 'System Update,'" *Zimperium*, 26 March 2021, https://blog.zimperium.com/new-advanced-android-malware-posing-as-system-update/.

30 NATO CCDCOE, "Recent Cyber Events: Considerations for Military and National Security Decision Makers," May 2021.

31 Oisin Sweeney, "Sweden Hit by Massive Cyber-Attack," *Euro Weekly News*, 22 December 2020, https://www.euroweeklynews.com/2020/12/22/sweden-hit-by-massive-cyber-attack/.

holding group of oil shale industry, power generation and public utility companies.[32]

Response Measures

The landmark 2009 Stoltenberg report on eight Nordic-Baltic countries (NB8) – a group that includes the five Nordic countries (Finland, Sweden, Norway, Denmark and Iceland) and the three Baltic states (Estonia, Latvia and Lithuania) – that was presented to the extraordinary meeting of Nordic Foreign Ministers suggested that Nordic countries could benefit greatly from cyber security cooperation. Since then, mature cyber security cooperation has emerged among the NB8 countries.[33]

The NB8 states also cooperate frequently at the working level in both formalised and ad-hoc ways through their participation in numerous international organisations, such as NATO, OSCE, the European Union, and the United Nations. Examples include Sweden and Finland participating in the work of the Tallinn-based NATO CCDCOE, and Lithuania's presentation of best practices in regional cooperation on behalf of all three Baltic States at an annual OSCE conference on confidence-building measures in cyberspace.

32 Republic of Estonia Information System Authority, "Annual Cyber Security Assessment 2017," https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf.

33 Read the Stoltenberg report here:
https://www.regjeringen.no/globalassets/upload/ud/vedlegg/nordiskrapport.pdf
Regarding broader security and defence cooperation in the region, the greater involvement of the US and UK has been a major objective of most NB8 countries. Both the US and UK have become involved within the regional security and defence initiatives, including in the area of cyber security. In 2010, Liam Fox, then-Secretary for Defence of the UK, launched the Northern Group of defence ministers with the purpose of fostering further defence cooperation with the NB8.

Nordic CERT Cooperation brings together Computer Emergency Response Teams (CERTs) from Finland, Sweden, Norway, Denmark and Iceland to carry out joint training in a variety of different aspects of cyber security. Since 2012, the NB8 countries have all participated in the Locked Shields exercise hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Estonia. Locked Shields is the largest technical live-fire cyber defence exercise of its kind in the world.

Looking at how decision-makers can become better prepared to anticipate and understand the effects of cyber-attacks, holding exercises to respond to cyber-attacks is one of the best ways to raise awareness at the political level.

In September 2017, Estonia organised the first-ever cyber exercise for all EU defence ministers, with the NATO Secretary-General also attending. Then-German Defence Minister, Ursula von der Leyen, called it an "extremely exciting" war game that showed the need for EU governments to be more aware of the impact of cyber-attacks on critical infrastructure in the EU.

In July 2018, European Union ministers of Internal Affairs gathered for a meeting in Helsinki and participated in a scenario-based discussion exercise that Finland had prepared as a host of the meeting. The exercise for ministers simulated a hybrid crisis that, *inter* alia, included cyber-attacks, disinformation campaigns. As the Finnish Minister of Internal Affairs, Maria Ohisalo, said, the aim was to "find a way to build resilience and raise awareness in the EU".[34]

34 Eszter Zalan, "Finnish presidency to war-game hybrid threat response," *Eurobserver*, 27 June 2019, https://euobserver.com/political/145283.

During the Nordic-Baltic foreign ministers meeting in Tallinn in September 2020, a 90-minute tabletop exercise was organised.[35] It tested the foreign ministers' ability to respond to an escalating cyber-attack. They answered multiple-choice questions about the transparency of the process and about possible diplomatic countermeasures to attacks. Ministers learned through first-hand experience that a timely exchange of technical information can be key to responding to any cyber-attack. "The shared view of the Nordic countries and Baltic states – especially when it comes to complicated issues – is crucial," said Urmas Reinsalu, then-Foreign Minister of Estonia.[36]

As the NATO CCDCOE, which annually organises the Locked Shields exercise that involves a strategic decision-making element, inserted about cyber exercises for the strategic level,

"It is important to exercise the strategic level of cybersecurity for decision-makers. Decision-making at the strategic level forms an integral part of cyber resilience and must therefore be part of exercises. National security is dependent on our ability to defend networks that support our critical functions. This is not purely a technical issue. How our national cybersecurity strategies are translated into policies and procedures needs to be understood by all stakeholders." [37]

35 Välisministeerium, "Joint Statement from Nordic-Baltic (NB8) Foreign Ministers' annual meeting," 9 September 2020, https://vm.ee/et/uudised/joint-statement-nordic-baltic-nb8-foreign-ministers-annual-meeting.

36 Press statement of the Ministry of Foreign Affairs of Estonia "Nordic and Baltic foreign ministers discuss regional and global politics in Tallinn" 9 September 2020, https://vm.ee/en/news/nordic-and-baltic-foreign-ministers-discuss-regional-and-global-politics-tallinn

37 NATO CCDCOE, "Recent Cyber Events: Considerations for Military and National Security Decision Makers," May 2021.

Conclusion

The COVID-19 crisis has increased our dependence on digital solutions. This means that a greater contribution toward the digital state and its security is needed. A number of high-profile cyber incidents in the Baltic Sea countries have raised awareness of the seriousness of the threat. But the information security managers of the public sector, the providers of public services and the wider cyber security community all need to be even more aware of the types of information that the attackers are after, the manners of using the data and the segments that need better monitoring. Although complete security against cyber-attacks cannot be achieved, investment in cyber security must be consistent and systematic and a workable crisis management plan must be in place to respond to a critical incident.

Cyber security in today's digital age is expensive and largely invisible. It can be often regarded as a nuisance to companies and authorities. Nevertheless, it is becoming indispensable, as it is cheaper for both companies and public authorities to prevent problems than it is to deal with the damage afterwards. The Nordic-Baltic countries, being some of the most digitised in the world, have all the more reason to take a more proactive approach to cyber security.

Information Threats and Security in the Baltic Sea Region

Janis Sarts

Throughout history, conflicts and wars were also played out in the information environment. Centuries ago, it was one of the least important elements of the conflict, but as technologies advanced (newspapers, radio, TV) and skills of different actors to use this space for their advantage in the conflict grew, so did the importance of the information space in the time of war and crises. Since the 2014 annexation of Crimea, which was essentially accomplished by an information-centric operation by Russian forces, this area has only grown in prominence and importance as a sphere of key strategic importance. In this short article, I will look into the key elements that will have an impact upon the information space security of the Baltic Sea Region. I will also look at the future trends and provide some thoughts on addressing these challenges in the regional context.

Information Landscape

Although much of the public discussion on information environment-related threats is focused on a few threat actors, one cannot fully understand the nature of the problem without looking at the underlying fundamentals of the changing information environment. The obvious key trend in the evolution of the information environment is the digitization of information. The scope of the change caused by this factor has been enormous as it has changed the ways information is created, distributed and consumed, and has increased the speed of information distribution to instantaneous.

One of the key factors of the new digital information environment is the **globality of information**. The digitization of information has removed many language-based barriers that have kept national information spaces insulated from one another over the centuries. Today, news and information easily transcend language barriers and it is increasingly difficult to discern the boundaries of national information spaces.

The second factor is that **social media** sites have de facto become the new public interaction space for societies; the new Agora. People increasingly execute their social interactions online – chatting, sharing news, expressing opinions. These trends have been strengthened by the Covid-19 pandemic-related lockdowns that have essentially moved everybody online. As our interactions have moved to different social media platforms, they have become subject to the business models of these companies. As a result of algorithms, which are tailored to the business models that these platforms are based on, we are increasingly seeing 'engaging' content, viral (emotional) posts and information that the algorithm has concluded we will like based on our previous viewing history on the given platform. This, in its turn, creates a phenomenon that

has been described as 'echo chambers' or 'information bubbles'.[38] Based on human biases and algorithm choices, people are starting to see very one-sided information and therefore interact with others who share similar world views, which ultimately encapsulates them in specific views with a decreased ability to listen, understand and relate to other views. A good, recent case-study that illustrates this phenomenon is the coronavirus vaccination efforts and the digital anti-vax community that is creating alternative realities and narratives.[39]

The third key factor is the **weakening of the traditional media model**. As the global digital giants become more influential, the local media markets struggle to adjust to the increased advertisement revenue redistribution towards global digital companies, such as Google and Facebook. According to Latvia's state revenue service, the combined revenue (mostly from advertisement services) of Facebook and Google in 2020 from Latvia was €220 million. At the same time, the total local advertisement market of Latvia in 2019 was just €81 million.[40] Considering that this is one of the key income generators for traditional media, it is clear that the dominance of global social media companies starves local media companies of revenues. This, in turn, forces many media houses to cut down on quality journalism and focus more on clickbait articles, ultimately becoming more dependent on external financial support. Although this trend is more visible in smaller

38 B.E. Auxier and J. Vitak, "Factors Motivating Customization and Echo Chamber Creation Within Digital News Environments," *Social Media + Society* 5/2 (2019), pp.1–13; N.J. Stroud, "Polarization and Partisan Selective Exposure," *Journal of Communication*, 60/3 (2010), pp. 556–76.

39 X. Yuan, R.J. Schuchard and A.T. Crooks, "Examining Emergent Communities and Social Bots Within the Polarized Online Vaccination Debate in Twitter," *Social Media + Society* 5/3 (2019), pp. 1–12.

40 Dace Skreija, "'Google' or 'Facebook' – which earns more in Latvia," *DelfiPlus*, 11 March 2021, https://www.delfi.lv/delfi-plus/bizness/google-vai-facebook-kas-latvija-pelna-vairak.d?id=53005903.

markets, it is increasingly affecting most of the Baltic Sea Region countries.

We are facing a technology-driven, information-consumption revolution that is creating a global information space, where national boundaries matter less and less. Social media business practices lead to stronger online echo chambers or information bubbles, which increases the fragmentation of society. The traditional media business model is struggling for resources and producing less high-quality, cost-intensive journalism in favour of clickbait article production. This information revolution has created new vulnerabilities and has deepened existing ones, creating opportunities for information space threat actors to exploit.

Threat Actors and Their Tools in the Baltic Sea Region

Due to the factors described above, the current information environment is a dream landscape for conducting hostile disinformation campaigns. Multiple threat actors are continuously exploiting vulnerabilities in our information space to advance their interests. These actors, with different motivations and pursuing differing interests, can broadly be classified into three groups.

The first group is motivated by **financial gain**. Actors in this group would be ready to relay on disinformation as a means of income. (Disinformation being conscious, consistent, coordinated use of false, misleading or interpreted information across various information channels to achieve the desired effect on a specific audience.) Strategies and tactics within this group vary widely. Some use fake stories and false news for traffic generation to their websites, which can be transformed into advertisement revenue streams. More elaborate actors run conspiracy theory networks that consistently relay one or a few conspiracy theories to lead

their followers into specific behaviours. Social media manipulation services are another layer of these 'for profit' actors. They sell mostly through social media robotic account networks (services to manipulate social media algorithms), fake traffic or engagement, or attack specific accounts with comments.[41] Ultimately, some information space manipulation is what one might call a full-service provider. They are ready to sell full-scale disinformation campaigns that include cross spectrum manipulation tools for influence.[42] In the Baltic Sea Region, we encounter a significant number of players that generate income from false news or conspiracy theories. As for the more advanced actors, they are also active here, but this industry is more concentrated in Russia and tends to focus on larger information spaces for profitability. However, from time to time, they do operate in smaller markets.

The second group of actors seek to achieve **political advantage**; to succeed, they are ready to step into the grey zone of disinformation to advance their ideas, attack political opponents or to advocate for a specific case. In the Baltic Sea Region, those mostly reverting to this tactic are fringe groups. However, there are countries where more mainstream political groups would be ready to employ some of these methods. The toolkit of these actors differs little from the one belonging to the first group of more elaborate players.

The third and the most dangerous group involves **states** reverting to disinformation as a tool for gaining influence in other countries, in conflict situations and as a way of weakening those they consider their adversaries.

41 Singularex, 2019. The Black Market for Social Media Manipulation. Riga: NATO Strategic Communications Centre of Excellence.

42 J. Corpus Ong and JVA Cabañes (2019), "Politics and Profit in the Fake News Industry: Four Work Models of Political Trolling in the Philippines", NATO Strategic Communications Centre of Excellence.

In the Baltic Sea Region, the primary state disinformation actor is Russia. It is arguably a global leader in employing information space attacks on other countries, as well as a leader in the amount of tools at its disposal for information space impact. To better understand the Kremlin's disinformation operations, I would like to take a closer look at three parameters: the approach, the infrastructure and the methods.

The Kremlin sees the information space as one of the central areas of conflict, and it believes that the West is waging information attacks on Russia.[43] It misreads journalistic practices and standards (such as independence, a critical approach to government policies and pluralism) employed by quality media in the West as a Western government-orchestrated attack on the Kremlin. It sees or portrays its actions as a response to such alleged attacks.

The Kremlin's operations are based on exploiting vulnerabilities in the societies they are targeting; these can be ethnic, religious, social, economic or political divisions. In general, Russia does not appear to mind being pointed at publicly for their disinformation operations, but more recently there has been increased efforts to hide their tracks and origins of some disinformation stories after attempts to interfere in the 2016 US elections.[44] In my assessment, this move is to counter an increased public resilience – especially in most Baltic Sea Region countries – to Russian disinformation practices.

Wide and diverse infrastructure for disinformation operations controlled by the Kremlin is one of the key success factors in its operations. Russia has invested significantly in this infrastruc-

43 V. Gerasimov, "The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations," trans. R. Coalson *Military Review* 96/1 (2016), pp. 23–9.

44 M. Bastos and J. Farkas, "'Donald Trump Is My President!': The Internet Research Agency Propaganda Machine," *Social Media + Society* 5/3 (2019), pp. 1–13.

ture. There are sizable populations in the Baltics that are fluent in the Russian language, and here state-controlled TV channels have been heavily used for propaganda dissemination. For others, the RT channel, Sputnik and their large online and social media presence have been used to the same effect. To counter increasing societal resilience to the Kremlin's disinformation, they have increasingly relied on so-called information laundering techniques (processing disinformation stories through various seemingly neutral sites unrelated to Russia to hide the original source). To accomplish this, the Kremlin is investing in creating proxy news outlets, blogs and online personalities to be used for these purposes.[45]

As described previously, the Kremlin also tends to rely on social media robotic networks in its online disinformation campaigns (as well as paid trolls) for increased virility of posts, attacks on specific accounts, rumour creation, infiltration of information bubbles, etc.[46] In my assessment, some of these networks are directly controlled by the Kremlin, while others are most likely paid for.

Ultimately, given the weak state of traditional media in the Baltic Sea Region, the Kremlin is one of the possible suitors for buying up traditional media with large audiences cheaply, thus increasing its foothold in that particular information space.

Most of the Kremlin's disinformation infrastructure in the everyday mode is used to produce variations on a number of narratives aligned with the established vulnerabilities, at times fine-tuning it for the policy objective of the day. We can say that, most of the time, this machinery is establishing preconditions that can be

45 Cepurītis, M., Juurvee, I., Keišs, A., Marnot, D., Ruston, S., & Carrasco Rodríguez, B. (2021). Russia's Footprint in the Nordic-Baltic Information Environment 2019/2020. NATO Strategic Communications Centre of Excellence.

46 Willemo J., (2019). Trends and Developments in the Malicious Use of Social Media. Riga: NATO Strategic Communications Centre of Excellence.

exploited at an opportune moment. Those moments are selected based on tactical opportunities (for example, elections), or during crises that are seen as essential for the Kremlin.

Another state threat actor emerging in the Baltic Sea Region is China. China's approach and methodology differs from that of Russia. It has a significantly lower risk appetite and is not running constant low-level disinformation campaigns in the region; however, when it sees that its interests are at stake, it does not shy away from using disinformation practices. The most recent example is China's attempts in the spring of 2020 to sow doubt on the origins of the coronavirus and counter criticism of the Chinese government's early response to the outbreak of this virus in Wuhan through disinformation practices.[47]

It is clear that China is much more efficient in using economic and market leverage to exert influence than it is in the information space. China's infrastructure, tools and understanding of European audiences are not mature enough to be effective in these activities. But China's technological capabilities – especially in the areas of emerging technologies – should be considered, as they might be detrimental to future information operations.

Future Trends

Many people who are dealing with responses to hostile information operations and disinformation in governments and in non-governmental structures might feel overwhelmed by the size and scope of the threats they have to counter. However, the pace of change in our information environment is increasing and, along with it, the potential vulnerabilities. It is therefore important to

47 R. Verma, "China's diplomacy and changing the COVID-19 narrative", *International Journal* 75/2 (2020), pp. 248–58.

foresee how emerging technologies will affect the information space and the types of risks involved.

Two current, interdependent and fast-developing technologies that will affect the information environment and its threats are big data and artificial intelligence (AI). Until recently, we have treated disinformation as a tool addressing significant segments of society at the same time, based on comparatively broad socioeconomic, linguistic and behavioural parameters. Now, the increase in data that we emit while living our digital lives is creating an ever more vibrant data market, and is increasingly making this data more accessible, richer and more structured.

The amount of data on an individual already available is huge. First and foremost, this means that privacy as a fundamental element is disappearing. This, in its turn, means that whoever is ready to pay can have a good insight into the personality, habits, beliefs and motivations of an individual through collected and structured data.

At the same time, advances in AI technologies make it increasingly plausible to exploit this knowledge to create individualized disinformation attacks. A similar mix of technologies – namely big data micro targeting – is increasingly used in political campaigns in the US. With increased efficiency of AI, this can be a very dangerous tool in the hands of hostile players. In 2018, we tested this hypothesis at the NATO Strategic Communications Centre of Excellence and ran an experiment during a military exercise in Latvia. As the exercise's 'red' team, our researchers were able to identify participating soldiers from an online environment, consequently scraping for open source data about them. These data sets were used to test whether they provided clues for how to alter the behaviour of these soldiers through disinformation. During this experiment, researchers were able to incite soldiers to disobey orders as well as revert to behaviours that where harmful to the

exercise's 'blue' team.[48] Although this experiment was small and limited, it demonstrated the potentially explosive risks that come from combining disinformation with big data and AI technologies.

The next technological advancement with significant impact on the future of the information space will be the emergence of the Internet of Things (IoT) combined with a wider adaptation of Augmented Reality. The combination of these two technologies will increasingly merge the physical reality with the digital reality. As in the early days of social media, we can tell that it will have an impact on how humans process reality. But the full scope of this impact – as well as the risks and vulnerabilities it will create – is hard to predict. Still, it is clear that it will revolutionize the information space as well as the human response to it once again.

The last big trend in the development of threats in the information space is the multiplication of threat actors. Already today, an increased number of countries invest in their offensive capability development for information operations. Unless we find a sufficient deterrent, this number will keep growing.

Solutions

To address the challenges to information space security in the Baltic Sea Region, we must take a comprehensive and long-term approach. The risks described above are too complex, too varied and too dynamic to be solved by simple fixes.

First, we need to correct the structural problems of the information space described at the beginning of this chapter. To return to healthier democratic interactions within societies, we need to

48 Bay S., Biteniece N., Fredheim R., Christie H.E., Dek A., Gallacher J.D., Kononova K., Marchenko T., (2019). The Current Digital Arena and its Risks to Serving Military Personnel. Riga: NATO Strategic Communications Centre of Excellence.

address the effects of social media business models on the public debate. Three principles to insert into the social media ecosystem are transparency, oversight and accountability. Today, when attempting to regulate the social media landscape, governments tend to focus on symptoms, such as removal of hate speech, incitement of violence, etc. In my perspective, we need to focus on the structural issues in order to improve the social media-created information space towards democratic standards. First, we need a standard of good social media practice that facilitates democratic interactions in society. Second, we need independent institutions that can oversee business choices, data practices, algorithm biases and efforts to root out hidden inauthentic account (robotic) networks on social media. Third, we need a set of agreed rules on the consequences to social media companies in case they are breaking these standards. Also, it is very important that regulations do not undermine individual speech online, as it would create a dangerous precedence from a democratic process perspective.

Societal resilience is another large area to focus on. Media literacy, high-quality journalism, non-governmental institutions capable of independently verifying processes and actors in the information space – all are important elements to increase resilience from information threats. Most Baltic Sea Region countries are at the forefront of building such resilience, but more can and should be done. Baltic and Nordic countries can also do more to promote these measures in other EU countries.

Governments must increase their focus on investments in capabilities to deal with information threats. Establishing cross-government level, strategic communications capabilities and practices increases resilience and serves as a limited deterrent to hostile actions. Since many of the information space threats have a technological dimension, governments need increased capabilities and

expertise in emerging technologies, such as artificial intelligence, big data, block chain, etc., to address these kinds of risks.

Most Baltic Sea Region countries have a strong and vibrant technology start-up scene. Many of the problems and threats in the information environment are linked to new technologies. We should be putting more emphasis on employing technological solutions to counter these risks. To achieve this, governments need to create instruments that incentivize technological innovation to address information threats.

Information threats are global in nature, while the response to these – due to the different values propagated by different states and different interests – cannot be global. But countries sharing similar values and interests should cooperate in answering to these threats. Most Baltic Sea Region countries are among the most advanced in their ability to address information threats and share similar values, which creates strong potential for regional cooperation.

The information space is the critical infrastructure for healthy democracies. Good, inclusive, fact-based societal debates lead to better choices and stronger democracies, while a fractured, aggressive and a facts-disregarding space weakens them. Therefore, it is of utmost importance to invest in a healthy information environment and to create societal resilience from hostile information attacks. Most Baltic Sea Region countries have recognized the risks and have started to invest in their mitigation. But without regional, European and transatlantic cooperation between democracies, it is impossible to successfully address those risks. The Baltic Sea Region countries and their cooperation on information space risks can set a global standard and lead the way for other democracies on these issues.

The Baltic Sea Region's role in the European security landscape

Barbara Kunz

With Russia's annexation of Crimea in 2014, the risk for territorial conflict in Europe has again become a reality. Territorial defence and deterrence have consequently made a return on the European security agenda. In geographical terms, and besides Ukraine itself, contact zones between NATO and Russia have been policy-makers' and analysts' focus alike. These contact zones include the Black Sea Region and the North Atlantic, but the most prominent example in the European security debate arguably is the Baltic Sea Region. Not only is it an area characterized by problematic security relations with Russia, which thus serves as a focal point for related concerns, but the positions on European security held by the region's countries also contribute to shaping the overall security and defence debate on the continent. Two ways in which the Baltic Sea region matters in the wider European security landscape may thus be distinguished: first, there is the question of how to best manage (in)security in the region itself, including with the help of outside partners. Second, in a wider European context, the so-called Eastern flank countries – which for the most part are to be found around the Baltic Sea – constitute one vociferous camp in the more general debate on the continent's security. Based on

their regional, Baltic Sea outlook, these same countries hold strong opinions on the issue at the heart of securing future Euro-Atlantic peace: the West's future relationship with Russia.

Several factors are of relevance in this context. First, countries in the region are among the most vociferous participants of the European security debate. This particularly refers to Poland, but also to Lithuania, Latvia, Estonia and Sweden. With very active think tanks, as well as various annual forums, these countries ensure Baltic Sea security issues – and thus a threat emanating from Russia – are kept on European and transatlantic agendas. Second, and in contrast to the other 'contact zones', these countries are also (relatively) unified in their positions regarding security matters. Factors such as military alignment status – on the Western side, the Baltic Sea region is composed of both NATO members and non-aligned Sweden and Finland –matter little in this respect. Such a situation stands in contrast with the Arctic, where, for example, NATO-members Denmark and Norway hold different views on the role to be played by the Alliance. It contrasts even more with the Black Sea Region, with Turkey increasingly playing the role of a 'problem ally' within NATO.

Managing (In)security in the Baltic Sea Region

Managing the security situation in the Baltic Sea Region has been high on both European and regional agendas. How to respond in case of Russian aggression is the key question, as well as how accidental escalation can be prevented. These are matters of concern for actors beyond the more narrowly defined region itself. The Baltic Sea Region is thus at the heart of a considerable portion of wider European and transatlantic security, and deteriorated regional security has consequently led to increased cooperation. Efforts have been multilateral (NATO, EU) as well as bilateral,

just as individual states play important security roles in the region, in particular the United States and the United Kingdom. At the multilateral level, the return of the Atlantic Alliance to its initial purpose enshrined in Article 5 of the Washington Treaty – after decades of focus on crisis management operations – is among the many consequences of the 2014 annexation of Crimea: providing security guarantees and reassurance for its members. The Baltic Sea Region is at the heart of this endeavour, given that it is the geographical area with the most extensive reassurance measures for Eastern Flank countries. While Baltic Air Policing was launched when the Baltic states joined NATO in 2004 and thus predates the 2014 events, the Alliance's Enhanced Forward Presence has been in place since 2017 as a direct reaction to what was viewed as a new security situation. Moreover, given that the Baltic Sea Region needs to be considered a unified strategic environment, NATO has developed new forms of cooperation with the non-aligned partner countries Finland and Sweden. As of today, both Finland and Sweden have very close ties with the Alliance that go beyond cooperation on crisis management operations (such as formerly in Afghanistan), although they are not encompassed in any security guarantees that come with membership. The EU, though not directly concerned with collective and territorial defence, has also taken measures intended to improve the Eastern Flank's military security. Most prominently, the PESCO project on Military Mobility aims to remove obstacles to swift movements of military personnel and assets, which is of particular importance in case of conflict in the region and should the need to deploy reinforcements arise. Norway, Canada and the US are partners in this EU endeavour, which is widely considered to be the flagship project of enhanced EU-NATO cooperation.

The security situation in the region has also led to increased cooperation among states, often building upon pre-existing and

sometimes long-standing partnerships. It has led to more bilateral and plurilateral cooperation among actors from both within the region and external partners. Perhaps the most prominent example of intra-regional cooperation is Finland and Sweden working together in unprecedented ways, including 'beyond peacetime'. External actors take the stage in various ways, particularly the US which is undoubtedly considered the most important partner throughout the region. American troops have been deployed based on bilateral agreements within the framework of the European Deterrence Initiative (formerly European Reassurance Initiative). US bilateral cooperation has also been deepened with both Finland and Sweden, as well as in trilateral formats among the three countries. The UK is also a key partner for many countries around the Baltic Sea, and the region is also a focal point for Germany's military engagement as the latter serves as a framework nation in Lithuania in the Alliance's Enhanced Forward Presence.

Keeping the region stable and countering any Russian aggression is certainly of key importance for the security of Europe. Likewise, reassurance of allies located in the region needs to remain high on NATO's agenda. The situation in the Baltic Sea Region, however, also has implications for the wider European security debate, beyond purely regional factors.

A symbol and one pole in the European defence debate

In a wider context, the security situation of the Baltic Sea Region has become a symbol or focal point when illustrating a potential Russian threat against European and Euro-Atlantic security. Russia's repeated incursions into other countries' airspace, for example, are often viewed as an illustration for more generally problematic Russian intentions, warranting the West to closely watch the situation and take appropriate measures for deterrence and defence.

While the narrative on the Arctic for a long time focused on cooperation[49], the Baltic Sea Region has, since 2014, often been framed as an area where World War III could potentially be started, notably because the Baltic states would be 'next' after Ukraine.[50] The Baltic Sea Region has thus often served as the key example of an area where European security is threatened by Russia – in a 'traditional' military way, but also in terms of hybrid warfare strategies or cyber-attacks. Conflict scenarios for the region have almost become a genre of its own; for example, being a popular location in wargames that involve Russian attacks on the Baltic States or Gotland.[51] Numerous reports on the security situation in the Baltic Sea Region have been published in recent years. The security situation in the region thus also serves as the prime illustration for the arguments put forward by one camp in the wider European defence debate: that is, (1) Russia poses a direct threat to European security; and (2) Europe is unable to defend itself without the help of the US.[52] These two points are the main arguments put forward by what may be labelled the 'Atlanticist' camp in the

49 Mikkel Runge Olesen, "The end of Arctic exceptionalism? A review of the academic debates and what the Arctic prospects mean for the Kingdom of Denmark," *Danish Foreign Policy Review (2020)*, *pp.* 103–27.

50 Paul D. Miller, "How World War III Could Begin in Latvia," *Foreign Policy*, 16 November 2016, https://foreignpolicy.com/2016/11/16/how-world-war-iii-could-begin-in-latvia/.

51 See, for example, David A. Shlapak and Michael Johnson, "Reinforcing Deterrence on NATO's Eastern Flank. Wargaming the Defense of the Baltics," Document RR-1253-A, *RAND Corporation*, 2016, https://www.rand.org/pubs/research_reports/RR1253.html. For another example of a relatively influential report on the security situation in the Baltic Sea region, see Edward Lucas, "The Coming Storm. Baltic Sea Security Report," *CEPA*, June 2015, https://cepa.org/the-coming-storm/.

52 In a wider context, the security of the Baltic states is also described as a litmus test for the US' willingness and ability to protect its allies. This view obviously has ramifications well beyond Europe as it, for instance, concerns Washington's Asian allies.

European security debate, and in particular the debate on European strategic autonomy.[53]

Currently, there are two main 'poles' in the European debate on security and defence. Threat perception is the principal factor in explaining which pole a country belongs to. One of these poles is the group of countries primarily concerned with the threat emanating from Russia. The other pole is essentially France, which is primarily concerned with jihadi terrorism in Africa and the Middle East. Even before 2014, Poland and the three Baltic states were warning against aggressive Russian foreign policy behaviour. However, in an era when European governments, and to a certain extent also US administrations, were mostly concerned with crisis management operations and the fight against terrorism, these warnings remained largely unheard. This has changed since the annexation of Crimea. While some of the alarmism in earlier Baltic wargaming and conflict scenarios may have worn off, the events of 2014 have led to the Russian threat being firmly set on European security agendas. As noted above, the largely shared outlook among the countries in the region, and Poland, Sweden and the Baltic states in particular, has contributed to allowing Baltic Sea states to play a major role in the wider European defence debate.

Besides keeping a potential Russian threat on the agenda, the same group of countries has also played an instrumental role in averting certain developments. Members of the first pole – those chiefly concerned with a Russian threat – tend to reject the idea of European strategic autonomy, framing it as 'decoupling' from the US and therefore endangering European security. Members of

53 For more details on this debate, see, for example, Barbara Kunz, "The Evolving Transatlantic Link: What European Response? *Disentangling* the European Security Debate," in *Alliances and Power Politics in the Trump Era. America in Retreat?*, edited by Maud Quessard, Frédéric Heurtebize and Frédérick Gagnon (London: Palgrave Macmillan, 2020), pp. 33–51.

the second pole, in turn, see the need for greater European ability to act independently from the US. By framing European strategic autonomy as an attempt to decouple European security from the US, governments such as in Poland contributed to making the debate – at least implicitly – a debate about the US.[54] That actual decoupling has clearly not been the proponents' intention has never mattered much in this context. Roughly five years after this debate started, there is still no European consensus on whether 'strategic autonomy' should be the EU's objective and, if so, how this is to be attained. As noted above, these differences are ultimately rooted in diverging threat perceptions throughout the EU. While they are hard to reconcile given that 'compromises' on threat perception are hard to imagine given the nature of the matter, Europeans today recognize that all threat perceptions need to be considered – even though different European capitals emphasize and prioritize different security risks.

The pole represented by Baltic Sea Region states thus has clearly managed to shape European debates and policies on security and defence, based on regional experiences and priorities. But it has also had an impact on the second pole in the debate, in particular French approaches to European security. Paris was initially not very interested in treating Russia as a – or even the main – threat to Europe's security. France's position has nevertheless evolved in recent years. Paris, of course, never supported Russia's foreign policies. Rather, it did not consider Russia the primary problem in ensuring the continent's security, and it focused (and still focuses) mostly on terrorism and instability in the 'South'. Yet, France is today more engaged in the Baltic Sea Region. For France, it is increasingly clear that threats from the East and the South

54 See Barbara Kunz, "Europe's defense debate is all about America," *War on the Rocks*, 4 March 2020, https://warontherocks.com/2020/03/europes-defense-debate-is-all-about-america/.

cannot be considered entirely separate. Russia's role in Syria and the Central African Republic, for example, has raised awareness, as well as issues including cyber-threats that transcend geography. Moreover, and considering the overstretching of French armed forces, France is increasingly interested in military support from other countries for its operations in Africa. When Emmanuel Macron came to power in 2017, the Eastern Flank was soon identified as an untapped reservoir of potential supporters for French endeavours, in both a military and a political sense. This relatively novel strategy of reaching out to countries in the Baltic Sea Region paid off: Estonia, for example, sends troops to France's Operation Barkhane in the Sahel region. Finland became one of the main supporters of President Macron's initiative to fill the solidarity clause of the Lisbon Treaty (Article 42.7) with more substance. Estonia, Finland, Sweden and Denmark (as well as Germany) are today part of the French-launched European Intervention Initiative.[55] Although threat perceptions continue to differ, there is more cooperation today than before 2014.

Concluding remarks

Even though some attention now seems to have moved to the Arctic, the Baltic Sea Region will continue to play an important role in the European security landscape, likely in both the ways outlined above: as a contact zone between the West and Russia, and as a group of countries from the same region that has a certain outlook on European security. Many other security threats and challenges notwithstanding, the West's relationship with Russia will remain the single most important variable for Euro-Atlantic

55 See French Ministry of the Armed Forces, "European Intervention Initiative," last updated 17 April 2020, https://www.defense.gouv.fr/english/dgris/international-action/l-iei/l-initiative-europeenne-d-intervention.

security in the foreseeable future. This, of course, extends beyond the Baltic Sea Region.

Entering an era characterized by great power competition, one key question for European security will be whether or not at least peaceful coexistence – as the minimum desirable outcome – with Russia is achievable. This, of course, also depends on Russia's foreign policy choices. On the Western side, one question to ask is: which narrative will win? Is Russia simply a revisionist state that must be countered by all means? Or, is the West ready to adopt a more nuanced perspective that allows for at least the possibility that Russia may have some valid security concerns? The latter question pertains to Russia's relations with the US, that – although purely bilateral in theory – have a direct impact upon European security. This is, of course, not to say that Russia's breaching of the rules enshrined in the Paris Charter and undermining the European security order should in any way be excused or tolerated. However, strategic stability in Europe is clearly in Europeans' interest. Whether this can be achieved solely through a strategy of 'the more deterrence, the better' is an open question. It should be asked in the process leading up to NATO's next Strategic Concept.

Gaps in addressing new and emerging climate risks

Evelin Piirsalu and Heidi Tuhkanen

National risk assessments only tend to cover known and historical risks, and very few consider the new and emerging threats that have yet to be experienced.[56] Of all EU Member States in 2013, only a few had included potential impacts on economy, employment and transboundary issues in their climate adaptation plans or strategies. Furthermore, only four EU member states had added transboundary risks to their adaptation strategies or plans in 2017.[57] This lack of engagement is due to multiple barriers that countries face locally and nationally in their adaptation work. At the same time, numerous weather events occur annually that bring consequences that societies have rarely experienced before and which can be related to climate change. Identifying and overcoming the barriers in adaptation work is crucial for our communities to cope with the consequences that climate change will inevitably bring.

56 European Commission (2017), "Overview of natural and man-made disaster risks the European Union may face", https://op.europa.eu:443/en/publication-detail/-/publication/285d038f-b543-11e7-837e-01aa75ed71a1.

57 R. Smithers, J. Tweed, R. Phillips-Itty, M. Nesbit, A. Illes, et al. (2018), "Study to Support the Evaluation of the EU Adaptation Strategy. Final Report".

The aim of this article is twofold: (1) to give an overview of new emerging risks that the local risk assessments and adaptation plans should include; and (2) to explain which barriers municipalities can potentially face with their adaptation work and howto overcome these obstacles. This article is based on two reports created during the CASCADE project funded by the European Union Civil Protection and Humanitarian Aid.[58]

New and emerging climate change-related hazards

Various climate drivers and hazards cause climate-related risks, but the level of risk for society is determined by the exposure of societal groups to these hazards and their vulnerability.[59] Climate drivers include temperature change, windstorms, sea-level rise, water temperature, and precipitation intensity and salinity. The leading causes of climate hazards are anthropogenic climate change and variability. In contrast, socioeconomic processes, including development pathways and measures taken for adaptation, mitigation and governance, influence exposure and vulnerability within society,.[60]

The climate drivers lead to various weather-related hazard events, which tend to become more extreme due to climate change.

58 H. Tuhkanen, L. Vilbiks and E. Piirsalu, "Overcoming barriers to climate adaptation" (2020), https://www.cascade-bsr.eu/sites/cascade-bsr/files/outputs/overcoming_barriers_to_climate_ adaptation_0.pdf;
H. Tuhkanen and E. Piirsalu, "Overview of climate risk drivers, hazards and consequences" (2020), http://www.cascade-bsr.eu/sites/cascade-bsr/files/publications/cascade_overview_of_climate_drivers_and_ hazards_final_version_0.pdf; CASCADE.

59 IPCC (2019), *IPCC Special Report on the Ocean and Cryosphere in a Changing Climate*. Cambridge: Cambridge University Press.

60 M. Oppenheimer, M. Campos, R. Warren, J. Birkmann, G. Luber, B. O'Neill and K. Takahashi (2014), "Emergent Risks and Key Vulnerabilities," in: *Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects*. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, pp. 1039–99.

These hazards cause secondary hazard events, such as flood events, drought, forest and wildfires, and changes in maritime ice sheets. Climate change-related threats have both direct and indirect consequences for society.[61] Since countries nowadays depend significantly on the global world economy, there are also several pathways for transboundary impacts. If multiple events that can be both climate and non-climate-related overlap, compound effects occur. This chapter gives an overview of climate-induced extreme weather events and secondary hazards as well as direct and indirect (cascading and transboundary) consequences and compound events (see Figure 1).

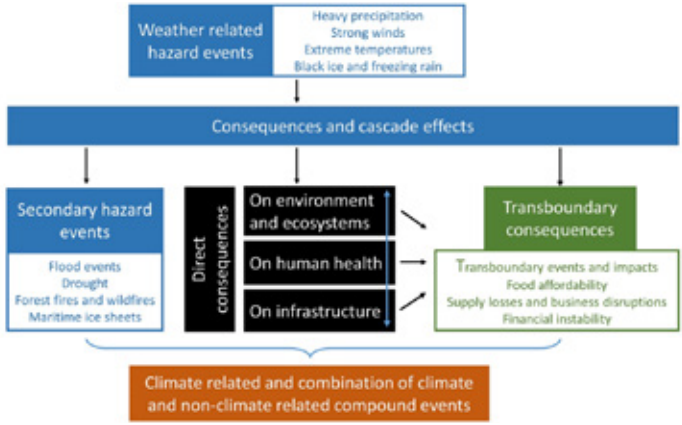

Figure 1. Overview of climate-induced extreme weather events and secondary hazards, direct and indirect (transboundary) consequences, and compound events.

61 UN (2016), "Report of the Open-Ended Intergovernmental Expert Working Group on Indicators and Terminology Relating to Disaster Risk Reduction", https://www.preventionweb.net/files/50683_oiewgreportenglish.pdf.

Weather-related hazards and secondary hazard events

The impacts of climate change differ across the Baltic Sea Region since it is biogeographically rather diverse. Furthermore, risks vary due to the differences in vulnerability and exposure. Therefore, extreme weather conditions, such as extreme heat and cold and heavy windstorms, play out differently and bring along different secondary hazard events across various parts in the Baltic Sea Region. All the region's countries had considered extreme weather events in their 2016–17 National Risk Assessments. These assessments included extreme temperatures, storms and frequent freezing, but only three of those eight countries also considered specific cascading effects.[62]

Weather-related hazards are heavy precipitation events (rain and snow), strong windstorms, extreme temperatures and black ice and freezing rain. In the future, severe precipitation events, such as heavy rain, will be more frequent in northern Europe and Scandinavia.[63] These events can result in secondary hazards, such as flooding, mud and landslides, which may cause damage to buildings and infrastructure but also have an impact upon the economy.[64] Furthermore, extreme precipitation can have widespread and costly consequences to infrastructure, health, property, etc., particularly in urban areas.

The other weather-related hazards are strong winds. The most relevant types of wind-related threats to the Baltic Sea Region are

62 European Commission (2021), "Overview of natural and man-made disaster risks the European Union may face".

63 European Environment Agency (2019), "Heavy precipitation in Europe," https://www.eea.europa.eu/data-and-maps/indicators/precipitation-extremes-in-europe-3/assessment-1.

64 A. Necci, S. Girgin and E. Krausmann (2018), "Understanding Natech Risk Due to Storms – Lessons learned and recommendations", https://publications.jrc.ec.europa.eu/repository/bitstream/JRC114176/storms_natech_analysis_final.pdf.

windstorms and convective wind gusts, and tornados. Storms usually take place in the autumn or winter. Only Denmark, Lithuania, Poland and Norway have included hurricanes and 'whirlwinds' in their risk assessments.

Extreme temperatures can include both cold and hot temperatures. However, one of the main weather climate risks for the BSR, especially in cities, is extreme temperatures and heatwaves. The definitions for heatwave vary in the Baltic Sea Region countries, but the World Health Organization defines them as situations in 'which the maximum and minimum apparent temperatures are over the ninetieth percentile of the monthly distribution for at least two days'.[65] Extreme temperatures and the heatwave intensity have been increasing in Europe for the past few centuries, resulting in long and intense heat periods. In addition, heat waves cause secondary hazard events, such as droughts and forest fires, that can have severe consequences for society and the economy.

Direct consequences and cascading effects

Weather-related hazards can cause direct consequences (cascading effects) on the environment (for example, coastal erosion and loss of biodiversity), human health (including diseases and loss of life), and infrastructure (such as infrastructure damage and loss of property). Abajo et al. define these cascading effects as 'a succession of events that each produces the circumstances necessary for the commencement of the next [event]'.[66] Thus, for example, the direct

65 World Health Organization (2020), "Heat threatens health: key figures for Europe", http://www.euro.who.int/en/health-topics/environment-and-health/Climate-change/activities/public-health-responses-to-weather-extremes2/heathealth-action-plans/heat-threatens-health-key-figures-for-europe.

66 B. Abajo, G. Garcia-Blanco, L. Gutierrez, J.A. Martinez, M. Mendizabal, H. Nassopoulus and M. Ehret (2015), "State of the Art Report (5) Adaptation Approaches", https://resin-cities.eu/fileadmin/user_upload/D1-1-SOTAAdaptation-Tecnalia-20151130-Annex.pdf.

effects of a storm can cause a cascading effect across society, such as the disruption of power affecting telecommunications networks, heating or rescue services, all of which are crucial for society.

Consequences on environment

The consequences for the environment include coastal erosion, animal and plant diseases and pests, and biodiversity loss. For example, strong winds and flooding can cause coastal erosion, which means that countries lose land from their coastline. Coastal erosion has further impacts on tourism and recreational possibilities in particular.[67] Furthermore, climate change brings milder winters and more extended vegetation periods, enabling new diseases and pests to spread, having an impact upon crop production and forest health.[68] Climate change also causes the spread of animal diseases, including classic swine fever, African swine fever, foot and mouth disease, and avian influenza, all of which currently pose the highest risk for the EU.[69] As these diseases are highly contagious, they often require removing a considerable share of life stock, if not all, which can seriously affect the agricultural and related sectors in particular.[70]

Consequences on human health

Climate change affects human health through various weather-related primary and secondary hazards and their cascading effects. In

67 T.A. Łabuz (2015), "Environmental Impacts—Coastal Erosion and Coastline Changes," in *Second Assessment of Climate Change for the Baltic Sea Basin*, edited by the BACC II Author Team, Cham, Springer International Publishing, pp. 381–96.

68 European Commission (2021), "Overview of natural and man-made disaster risks the European Union may face."

69 Ibid.

70 Tuhkanen and Piirsalu (2020), "Overview of climate risk drivers, hazards and consequences".

particular, the elderly, children, workers in exposed environments and migrants are groups at risk across Europe.[71] Some examples of consequences for society include health problems from heatwaves and health damages due to slippery roads. Forest fires, heavy rains and flooding incidents as a result of climate change can aggravate diseases related to air and water pollution.

Consequences on infrastructure

The more frequent extreme weather events and higher temperatures due to climate change can all have an impact upon transport, energy and IT systems critical for societal functioning, and can also cause numerous cascading impacts on society, the economy and even the environment. For example: windstorms causing damage to wind and hydropower generation plants resulting in power failures; flooding of steam wells and heating pipes disrupting heating or hot water; flooding-related water and moisture damage of IT equipment disrupting IT systems and mobile phone networks, and/or causing electrical fires; heavy rain or snowfall disrupting transportation, etc.

Another cascading effect related to critical infrastructure is the Natural Hazard Triggering Technological Disasters (Natech). Poljanšek et al. have defined Natech incidents as 'technological accidents triggered by a natural hazard or disaster which result in consequences involving hazardous substances (e.g. fire, explosion, toxic release)'.[72] All hazardous industrial sites are potentially at risk of having Natech accidents. For example, weather events including lightning, strong winds, flooding, low temperatures or rain can

71 World Health Organization (2020), "Heat threatens health: key figures for Europe."
72 K. Poljanšek, A. Casajus Valles, M. Marín Ferrer, A. De Jager, F. Dottori, et al. (2019), "Recommendations for National Risk Assessment for Disaster Risk Management in EU: Approaches for Identifying, Analysing and Evaluating Risks: Version 0", http://publications.europa.eu/publication/manifestation_identifier/PUB_KJNA29557ENN.

damage industrial facilities and thus activate a Natech incident.[73] As a result, significant consequences may follow, such as the flow of highly hazardous substances to the sea or other water bodies.

Transboundary consequences

Transboundary consequences occur due to the interconnectedness of our current world and the ingrained nature of various global networks in society. Thus, climate change can have an impact upon international trade systems, the stability and conflict in certain regions, and financial and business markets; it can create risks for those participating in these systems. The examples of transboundary cascading effects are: impacts on food in terms of decreased food security, food availability and food affordability; migration caused by the climate-related displacement of various vulnerable countries, especially in Africa and Asia; supply losses and business disruptions due to disturbances in global supply chains; and financial instability.

Compound effects

Compound events are events where multiple hazards coincide, contributing to societal or environmental risk. Thus, if numerous climate-related hazards occur and cause a set of cascading effects simultaneously, together they can have more severe consequences. For example, high temperature, low precipitation, relative humid-

73 European Union (2008), "COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF;
S. Girgin, A. Necci and E. Krausmann (2019), "Dealing with cascading multi-hazard risks in national risk assessment: The case of Natech accidents," *International Journal of Disaster Risk Reduction*, 35.

ity, wind and lightning occurring simultaneously can create a higher risk of forest fire.[74]

Compound events can also relate to a combination of climate-related and non-climate-related events (civil unrest, pandemic, financial shock, etc.), or two non-climate related hazards co-occur. A timely example of this is the climate hazard events that took place during the COVID-19 pandemic, as can be seen in the events which were projected to take place during the pandemic.

Barriers to climate change adaptation

In the Baltic Sea Region, climate change adaptation planning has occurred at varying paces in different countries, and many municipalities have been slower than expected. This is due to various barriers that local and regional governments face in their climate change adaptation work. These barriers can be divided into eight main categories based on an modified typology originally developed by Weyrich.[75] These categories apply to the different parts of the climate adaptation process – understanding, planning and managing phases.[76]

Conflicting timescales and conflicts of interest

Climate adaptation often requires long-term investments into infrastructures to resist the impacts of various extreme weather events and slow onset effects of climate change. However, such

74 J. Zscheischler, S. Westra, B.J.J.M. van den Hurk, S.I. Seneviratne, P.J. Ward, et al. (2018), "Future climate risk from compound events," *Nature Climate Change* 8/6, pp. 469–77.

75 The original categorization of barriers to adaptation by Weyrich (2016) uses nine categories. The authors have merged two categories (Politics and Conflicting Timescales and conflicts of interest) for use in the CASCADE project. Weyrich, P. (2016). *Barriers to Climate Change Adaptation in Urban Areas in Germany*. 26. Climate Service Center Germany.

76 J. Ekstrom and S. Moser (2014), "Identifying and overcoming barriers in urban climate adaptation".

long-term measures can conflict with short-termism dominant in business and political cycles where the pressure to show results short-term is evident.[77] Furthermore, as the benefits of successfully mitigated disasters are challenging to estimate and accounted for (avoided losses, etc.), decisionmakers may be less incentivised to champion controversial investments.[78] Also, successful adaptation requires cross-sectoral collaboration. However, the timings of various processes may need to be adjusted to ensure they support adaptation. For example, integrating green infrastructure into the urban environment requires early and close collaboration between transport, landscape and planning experts. Conflicts can also occur due to differences in priorities for development, for example between short and long-term needs. It may be difficult to prioritise certain long-term investments into adaptation, when specific and immediate needs in other sectors may also require investments. There can even be competition between investments for adaptation and mitigation. This links directly with Section 2.3. (Resources).

Leadership

Leadership is essential to understanding the need for climate change adaptation and to initiate the adaptation process phase.[79] It is also vital for continued recognition, mainstreaming, further

77 R. Biesbroek, J. Klostermann, C. Termeer, and P. Kabat (2011), "Barriers to climate change adaptation in the Netherlands," *Climate Law*, 2/2, pp. 181–99; Ekstrom and Moser, "Identifying and overcoming barriers in urban climate adaptation" (2014); Vorhies, F. (2012), "The Economics of Public Sector Investment in Disaster Risk Reduction. A Working Paper Based on a Review of Current Literature Prepared for the UNISDR", Education for Safety, Resilience and Social Cohesion: Paris, France.

78 Mullin, M.; Rubado, M.E. (2017), "Local Response to Water Crisis: Explaining Variation in Usage Restrictions During a Texas Drought", Urban Aff. Rev. 53, pp. 752–774.

79 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany", Climate Service Center Germany.

development and long-term funding of the adaptation at the local level.[80] The obstacles related to leadership can arise due to weak leadership, too many leaders or the lack of leaders.[81] Leadership on climate issues requires an understanding of the basic climate issues, skills to guide the process and ensure that adaptation is being mainstreamed at multiple levels, different sectors, and across both the public and private sectors. Leaders also need to be able to tackle all of the other relevant barriers mentioned in Section 2.

Resources

Weyrich clusters this barrier around the unavailability or inaccessibility of "human, financial and technical resources".[82] The resources needed for climate adaptation include staff capacities and expertise, time, and funding, which can be used to gain the missing and needed resources. Resources are essential in each planning, management and implementation phases of planning. [83] It is further needed for the more detailed designing and implementation of the actual adaptation measures.[84] Allocating resources – especially financial resources – indicates that these issues are a

80 A. Jensen, H.Ø. Nielsen and M.L. Nielsen (2016), "Climate adaptation in local governance: Institutional barriers in Danish municipalities", http://dce2.au.dk/pub/SR104.pdf.

81 Ekstrom and Moser (2014), "Identifying and overcoming barriers in urban climate adaptation"; K. Eisenack, S.C. Moser, E. Hoffmann, R.J.T. Klein, C. Oberlack, A. Pechan, M. Rotter and C.J.A.M. Termeer (2014), "Explaining and overcoming barriers to climate change adaptation," *Nature Climate Change* 4/10, pp. 867–72.

82 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany", Climate Service Center Germany.

83 S.C. Moser and J.A. Ekstrom (2010), "A framework to diagnose barriers to climate change Adaptation," *Proceedings of the National Academy of Sciences* 107/51, pp. 22026–31; Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany".

84 K. Goldie-Ryder, H. Tuhkanen and E. Piirsalu (2021), "Integrating climate change adaptation and disaster risk reduction in the Baltic Sea Region. Policy recommendations", http://www.cascade-bsr.eu/sites/cascade-bsr/files/publications/policy_recommendations_report_final.pdf.

priority for the leadership. Lack of resources is perceived as a top local level barrier to adaptation,[85] but it can be especially problematic for both small municipalities[86] and small and medium sized companies. Furthermore, it should be recognised that in some cases, this barrier can link with the competition for resources and allocation between different priorities in Section 2.1.

Scientific data and knowledge

Science-related barriers are especially relevant in the planning phase of the adaptation process, particularly in gathering and using information.[87] The obstacles related to science include both a lack of data, information or the lack of access to information.[88] In addition, local municipalities in the Baltic Sea Region are often challenged to understand what these scientific data mean for their localities. This is also partly due to the lack of high resolution climate projections at the current time.[89]

Municipalities also have challenges dealing with uncertainties inherent in the scientific projections related to long-term climate change impacts. Uncertainties can be problematic to grasp for local authorities, especially in cases where climate change impacts have not yet been evident in a particular municipality and are therefore only theoretical and intangible.[90]. There are also uncertainties

85 Tuhkanen et al. (2020), "Overcoming barriers to climate adaptation".

86 Jensen, et al. (2016), "Climate adaptation in local governance: Institutional barriers in Danish municipalities."

87 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany".

88 Biesbroek, et al. (2011), "Barriers to climate change adaptation in the Netherlands."

89 Goldie-Ryder, et al. (2021), "Integrating climate change adaptation and disaster risk reduction in the Baltic Sea Region"; Ekstrom and Moser (2014), "Identifying and overcoming barriers in urban climate adaptation."

90 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany"; Goldie-Ryder, et al. (2021), "Integrating climate change adaptation and disaster risk reduction in the Baltic Sea Region".

related to the effectiveness of some adaptation measures, such as nature based solutions, for which the longterm impacts are still unknown.

While most municipalities are including the historical and known risks, such as flood risks, in their risk assessments, new and emerging risks are commonly missing.[91] This includes risks, such as heat, and drought, as well as the cascading effects and the interactions of risks between the ecosystem, our infrastructure systems, and human health.[92]

Governance and institutional constraints

This category of barriers involves legislation, coordination and cooperation, and covers the entire adaptation cycle from understanding the problem to implementing the measures. Specific regulatory requirements related to permiting or insurance, [93] or alternatively, the lack of legal mandates for working on adaptation can hinder progress.[94] The lack of well-established or informal processes of or networks for collaboration can slow the initiation of required cross-disciplinary, cross-sectoral and multi-level work.[95] Thus, there is a need for working across silos within an authority

91 Ibid.

92 H. Tuhkanen and E. Piirsalu (2020), "Overview of climate risk drivers, hazards and consequences".

93 C. McGuire (2018), "Examining legal and regulatory barriers to climate change adaptation in the coastal zone of the United States," *Cogent Environmental Science* 4/1, pp. 1491096.

94 S. Burch (2010), "Transforming barriers into enablers of action on climate change: Insights from three municipal case studies in British Columbia, Canada", *Global Environmental Change* 20/2, pp. 287–97;
T.G. Measham, B.L. Preston, T.F. Smith, C. Brooke, R. Gorddard, G. Withycombe and C. Morrison (2011), "Adapting to climate change through local municipal planning: barriers and challenges," *Mitigation and Adaptation Strategies for Global Change*, 16/8, pp. 889–909.

95 Eisenack, et al. (2014), "Explaining and overcoming barriers to climate change adaptation".

but also broadening the spectrum of stakeholders to include perspectives from the private sector, non-governmental sectors and the public.

Lack of awareness and communication

This category of barriers relates to communication that builds awareness about climate change and its implications for so many other issues[96]. We also need to broaden our understanding of how we, as a society, construct climate risk in both our everyday actions, as well as our long-term decisions. This includes understanding the role of actors, assets (for example, infrastructure) and activities in determining the consequences of climate change impacts on society; adaptation-related timescales, as well as the costs of inaction, and the costs and benefits of various solutions. The lack of awareness can stem from lack of communication, miscommunication, but also mistrust.[97] Through communication, it is possible to influence issues such as a stakeholder's understanding of climate change, perceptions of climate risks, as well as adaptation options. Communication with stakeholders, including the public, should be adapted to actors' particular needs to allow them to understand their own role in adaptation.

Attitudes, values and motivations

The barriers in this category are related to social and cultural aspects, such as culture, beliefs, motivations, social norms, trust

96 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany".

97 Ekstrom and Moser (2014), "Identifying and overcoming barriers in urban climate adaptation";
C. Huggel, D. Stone, M. Auffhammer and G. Hansen (2013), "Loss and damage attribution," *Nature Climate Change* 3/8, pp. 694–6.

in science and risk perception values.[98] These aspects are essential when working with decision-makers, influencers and people who are expected to change their behaviour as part of the solution. In addition, risk perception and subsequent decision-making are influenced by personal aspects, such as the role of traditional knowledge, political affiliation, education and trust in different sources of information.[99] This cluster of barriers plays a key role in the beginning of the adaptation process (i.e. while detecting the problem, gathering information and redefining the problem). However, if not dealt with at the beginning, they may reappear as a barrier during the implementation phase.[100]

Adaptation process

The final category of barriers to adaptation is connected to the adaptation process itself. This includes difficulties with starting the process, selecting the scope and criteria, identifying the most suitable and efficient options for adaptation,[101] or which risks to include in the risk assessment. As adaptation is location specific and less replicable than mitigation efforts, it is not as easy to learn from other regions. This is because local solutions should be based on risk assessments tailored to that area in terms of the specific geography and landscape, as well as the local stakeholders, regulations and financial resources available.

98 Ibid.

99 R.J.T. Klein, G.F. Midgley, B.L. Preston, M. Alam, F.G.H. Berkhout, K. Dow and M.R. Shaw (2014), "Adaptation opportunities, constraints, and limits" in *Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*, edited by C.B. Field, et al., Cambridge: Cambridge University Press, pp. 899–943.

100 P. Weyrich (2016), "Barriers to Climate Change Adaptation in Urban Areas in Germany".

101 Klein, et al., "Adaptation opportunities, constraints, and limits."

Overcoming the barriers in local authority

A short guide has been developed to overcome the barriers related to climate adaptation and to help municipalities move forward with the adaptation process. The guide includes two parts: a self-evaluation survey to identify the barriers in local authority; and a resource guide that provides advice on how to deal with obstacles. The self-evaluation survey in this guide can be used to identify current or expected barriers to successful climate risk assessment and adaptation option selection processes within a local authority.[102] The survey uses the same eight categories outlined above and 39 specific barriers described within those. Each of the barriers should be rated on a scale of 1–5 (1 representing no challenge; 5 representing significant challenge). If needed, it is possible to add other obstacles not listed in the survey. The survey should take around 20 minutes to complete. However, it is essential that the survey is not just answered by one person but is circulated to several people in different departments relevant to climate adaptation work to gather different perspectives. Therefore, the survey answers should be anonymous.

The resource guide gathers existing resources according to the eight categories outlined above.[103] These resources are provided as video clips, guides and critical questions relevant to each of the 39 barriers. Video clips and guides offer different perspectives and inspiration on how to deal with obstacles. In addition, critical questions linked with the videos and guides are meant to help start discussions with stakeholders around the key topics.

102 Tuhkanen, et al., *Overcoming barriers to climate adaptation*, chapter 3.
103 Ibid., chapter 4.

Conclusions

The impacts of climate change are more visible and tangible every year, posing potentially severe consequences on society, economy and environment. Adaptation plans should consider, besides current and historical risks, new and emerging risks, such as consequences of plant and animal diseases, biodiversity loss, and cascading effects on human health and infrastructure. Overcoming barriers, such as a lack of resources (human, finances, time and competence), understanding and interpreting scientific data, barriers to collaboration, climate scepticism and disbelief, etc., is crucial in the successful adaptation process.

In pursuit of a European entrepreneurial culture

Björn Weigel

Weak entrepreneurial culture apparently tempers the EU's ability to make money from science. This warrants a closer look at entrepreneurial areas of the Baltic Sea Region that bucks the downward trend.

Innovation, competitiveness and making money from science were, naturally, always important for the EU and, subsequently, a recurring theme in policies, speeches and papers. The Lisbon Strategy of March 2000 noted as much, stating that the EU was to be 'the most competitive and dynamic knowledge-based economy in the world'.[104] Seemingly to speed things up, five years later the European Council decided to 'invest … more in knowledge and innovation' and in 'unlocking business potential, especially for SMEs' (small and medium enterprises).[105] The European Council's

104 European Council (2000), "Presidency Conclusions: Lisbon European Council 23 and 24 March 2000"
105 European Council (2006), "Presidency Conclusions: Brussels European Council 22 and 23 March 2006"

strategic agenda for 2019–2024 returned to this theme once again with talks of 'developing a strong and vibrant economic base'.[106]

Such grand statements are not mere visions as substantial effort and money have been put to the task. The research and innovation programme, Horizon 2020, was granted nearly €80 billion between 2014 and 2020.[107] Horizon Europe, a programme run in the same vein, has been granted over €95 billion until 2027 as it 'facilitates collaboration and strengthens the impact of research and innovation'.[108] EU leaders are not shying away from challenging tasks; the European Innovation Council, for instance, is supposed to 'identify and support breakthrough technologies and game changing innovations to create new markets and scale up internationally'.[109] This is all in addition to the effort and money invested by EU member states independently.

Ample signs, however, reveal that the EU falls short of its aspirations. Only think of lagging productivity growth across the EU, years before the pandemic. Or of all the less innovative firms, typically referred to as 'zombie firms' and artificially kept alive by credit extension, standing in the way for more innovative firms. Brexit and the loss of the City of London has dampened hopes for an EU Silicon Valley, but it was an escaping proposition long before the UK referendum. The EU still highlights its position as one of the largest economies in the world, yet only a handful of EU companies make the greatest global companies list by market capitalisation.[110] Among global tech titans valued to at least $50 billion,

106 European Council (2019), "A New Strategic Agenda".
107 Horizon 2020 (2020), "What is Horizon 2020?", https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020.
108 European Commission (2021), "Horizon Europe".
109 European Innovation Council (2021), "About the European Innovation Council", https://eic.ec.europa.eu/about-european-innovation-council_en.
110 The Economist (2021), "Europe is now a corporate also-ran. Can it recover its footing?".

not a single one was of EU descent in mid-2020.[111] The EU has struggled to keep up with corporate global frontrunners in areas such as artificial intelligence, quantum computing, blockchain, genomics, robotics, cybersecurity, and others. It is naturally better than its rivals in some areas, but, all considered, the EU appears far from the dynamic innovative economy it aspired to be in the Lisbon Strategy over 20 years ago.

So, it came as no surprise when Ursula von der Leyen, the President of the European Commission, recently pondered that: 'We, Europeans, are excellent in making science with money. But we are not so good in making money out of science.'[112] She implied that the EU's problem is less about innovation and more about creating businesses from innovation. This put the spotlight on the commercialisation of innovation, ideas and opportunities, and the EU's weak entrepreneurial culture. Yet, there are exceptions – salient areas of entrepreneurial culture that have been more successful in making money out of science, such as in the Baltic Sea Region.

Entrepreneurial culture and the Baltic Sea Region

The deep winter sun barely makes it over the horizon, if at all in the farthest north. The sparsely populated Nordics, on the shores of the Baltic Sea, forces travellers to go on for hours to leave one city for the next. Climate is, at times, as unwelcoming as languages are exotic. On the surface, the Baltic Sea Region appears anything but the kind of habitat a commission president dedicated to making money from science should be particularly attentive to. Yet, in some respects, it is.

111 GP Bullhound (2020), "Titans of Tech 2020".
112 European Commission (2021), "Opening speech by President von der Leyen at the European Innovation Council Launch Ceremony".

According to investment experts, more than half of Europe's billion-dollar corporate exits between 2005 and 2014 came from four countries alone: Sweden, Finland, Norway and Denmark, with Sweden roughly as large as the others combined.[113] This period was neither a coincidence nor an outlier. Irrespective of mature firms that may well be defined by strong entrepreneurial culture too, there is no denying that the Baltic Sea Region – and particularly Sweden – keeps churning out new innovative companies at an impressive rate on the back of a strong entrepreneurial culture.

Only consider Skype (Sweden/Denmark), SuperCell, Rovio and Iceye (Finland), Klarna, iZettle, EA Digital Illusions, Mojang (Sweden), Bolt (Estonia), Kahoot! (Norway), Unity and Sitecore (Denmark). Northvolt (Sweden) have invested billions of euros to establish Europe's largest battery cell factory. Kry (Sweden) has challenged vested interests with digital healthcare. Wolt (Finland) has delivered food to doorsteps in over 20 countries. The open banking platform Tink (Sweden) was recently sold to VISA for €1.8 billion.[114] Truecaller (Sweden) boasts hundreds of millions of daily users, identifying unknown callers. Spotify (Sweden) has revolutionised the way people listen to music. There are other renowned firms from the region too, not to mention all the many smaller or less famous, yet fast-growing entrepreneurial companies promising to make it big, and emerging industries such as green energy, fintech and insuretech. The new Swedish computer gaming industry alone was equal in export volume to the old Swedish iron ore and pulp industries combined (excluding pro-

113 Creandum (2016), "The Nordics in context: The Creandum Exits Report".
114 Megaw (2021), "Visa buys Swedish fintech Tink in €1.8bn deal", *Financial Times*.

cessed goods) with close to SEK 25 billion (around €2.5 billion) and growing at nearly 30 percent in 2019.[115]

In fact, when experts rank global entrepreneurial hotspots, Baltic Sea countries commonly rank close to the top. Consider, for example, some recent innovation rankings: Sweden ranked first, followed by Finland and Denmark, in the EU Commission's Innovative Scoreboard 2020. Sweden, Denmark and Finland were all positioned among the top ten in Bloomberg's 2021 Innovation Index. The Global Innovation Index 2020 – a collaboration between INSEAD, Cornell University and the World Intellectual Property Organization (WIPO) – ranked Sweden second in the global high-income group and second in Europe (including the UK). The list goes on.

Baltic Sea countries, in general, are not much different from economies struggling with weak productivity growth, zombie companies and growing bureaucratisation. This is not a story of Nordic exceptionalism, but of entrepreneurial culture. And what is interesting and remarkable is that the Nordic countries have not been leaders in entrepreneurial culture for long, but the roots of such culture can be traced back almost 30 years.

Entrepreneurial culture springs to life

An important yet often-forgotten fact, according to author and innovation expert Matt Ridley, is that, throughout history, big innovations commonly come about as several people invent similar innovations virtually simultaneously and separately. Apparently, as many as 23 people can lay claim to having invented the light bulb, and 'more or less independently … produced, published or

115 Dataspelsbranschen (2020), "Spel ikapp malm och massa", https://dataspelsbranschen.se/nyheter/2020/10/20/spel-ikapp-malm-och-massa.

patented it'.[116] However, only Thomas Edison has earned fame for it. The point, with regards to entrepreneurial culture, is that, while a narrow quest for ever more light bulbs (or innovations as such) is the usual way that nations aspire to find success with innovations, it is not enough to make money out of science. For the latter to happen, innovations must become diffused and ultimately used by companies, institutions and people. And that is where entrepreneurial culture comes in.

Innovation success is a quest for breaking down barriers to innovation diffusion, including barriers such as infrastructure, legislation, vested interests, competing products, behaviours, customer preferences and bureaucracy. Breaking down barriers creates market space for new medical drugs, self-driving cars, green energy, interstellar travels, or whatever innovation we may think of. But innovation diffusion, as it were, does not normally come easily. It is rather cluttered with resistance and challenges, and requires change agents or entrepreneurs to succeed. The famous economist Joseph Schumpeter's acclaimed notion of 'creative destruction' (*schöpferische zerstörung*) of a continuously evolving economy at the heart of economic development is impossible without entrepreneurs.

A sudden presence of entrepreneurs some 30 years ago propelled the remarkable change in the Nordic countries to become leaders in entrepreneurial culture. At that time, talented people got together and pursued entrepreneurial opportunities on a much larger scale than before. Typically, they did not only chase after innovations as such, or 'new light bulbs', but rather sought to commercialize assets and ideas, and to build profitable companies from innovations. What set them apart from previous generations

116 Ridley (2018), "Hayek Lecture 2018: How Many Light Bulbs Does It Take To Change The World?", *Institute of Economics Affairs*.

was a benevolent approach to business uncertainties, and a diligent exploration of business opportunities. But why did it happen when it did, why not ten years earlier, or not at all?

Entrepreneurial culture burgeoned in the Baltic Sea Region for two reasons. First, when socialism crumbled after the fall of the Berlin Wall and the collapse of Soviet communism in 1989 and 1991, a path opened for entrepreneurial culture. It was a shock to the system and prompted changes in policies and perceptions in both the East and the West. Even countries on the western side of the iron curtain changed. It also had a profound impact on the Nordic countries, especially in terms of entrepreneurial behaviours. Resistance to entrepreneurial behaviours was numbed: bureaucratic control of economic growth and development was pushed back, and ideas of top-down planned and politically controlled systems for innovations fell out of fashion, at least for some time. In essence, society opened up to entrepreneurs.

Parts of society became perceptibly more aspiring. Threats of a catastrophic military conflict that had loomed for centuries were replaced by desires for a new future. As the appetite for chasing down business opportunities grew, entrepreneurial culture burgeoned. 'Economic change in all periods depends, more than most economists think, on what people believe', stated historian Joel Mokyr.[117] People aligned with the spirit of creative destruction and entrepreneurial behaviours, but, as Mokyr continued, 'intellectual innovation could only occur in the kind of tolerant societies in which sometimes outrageous ideas proposed by highly eccentric men would not entail a violent response against "heresy" and "apostasy"'.[118] Intolerance to intellectual innovations are common throughout history, but following the fall of the Berlin Wall, soci-

117 Mokyr (2009), "The Enlightened Economy: An Economic History of Britain, 1700-1850".
118 Ibid.

ety was rather tolerant, at least to the effect that it supported entrepreneurial culture, or to the very least not opposed it; and so the perception of entrepreneurs changed.

Swedish entrepreneur Jan Stenbeck illustrates the change. A decisive force behind successful companies like Tele2, Comviq, Metro, Radio Rix, TV3, TV-Shop, TV1000 and Viasat, and with a special instinct for uncertain business territory, Stenbeck fought (sometimes fiercely) against vested interests and government authorities to make room for new innovations. Already in the 1980s, before the end of the Cold War, he worked hard to break the Swedish telephone monopoly. Ahead of his time, Stenbeck was controversial in some quarters until his death in 2002. Yet, thanks to him and other influential entrepreneurs, society and the perception of entrepreneurs changed, and Nordic countries migrated towards 'a business respecting civilization', to borrow Deirdre McCloskey's words.[119] Stenbeck earned appreciation, and inspired generations to explore uncertainties and challenge vested interests. Meanwhile, entrepreneurial culture grew stronger. In only a few years, the region went from almost deprived to almost overwhelmed by entrepreneurial behaviours in some parts. As the 1990s came to an end, what is today known as the first dot-com boom was full in the making.

Spearheaded by a new generation of entrepreneurs targeting the old corporate aristocracy and archaic political beliefs, the dot-com boom unfolded as numerous companies were launched on the back of the emerging digital economy. Digitization was the second reason for why entrepreneurial culture came to life when it did. It changed the rules of the game in favour of young entrepreneurs. They could reap the benefits from having played computer games and disassembled Atari and Amiga computers in their youth. The

119 McCloskey (2016), "Bourgeois Equality", p. 641.

PC revolution provided a generation of young entrepreneurs with unique digital skills and acquainted them with the future digital economy. Furthermore, digital entrepreneurs harvested a rather hands-off regulatory approach and government investments in digital infrastructure. Broadband, widely available when digitization was still in its infancy, at least in Sweden, and the making of personal computers available to broad swaths of the population, paved the way for digital markets as well as consumers.

This new generation of entrepreneurs aspired to make it big; the dot-com boom was an explosion of the mind, a boomerang effect from cloistered times, a reaction that eventually went too far and became too excessive. Enforced by a growing can-do spirit, expanding internationally right from the start, turning weaknesses of small home markets into advantages, from the 'Interrail generation' explorers of Europe by train, fluent in English, German and French, with the rigid times before the 'fall of the wall' fresh in memory – it was only natural that they pushed forward. However, the dot-com boom was a hype that eventually became unsustainable.

Entrepreneurial culture

The dot-com boom had to come to an end at some point, and it did in a rather spectacular crash, as publicly traded tech-stocks dropped sharply in value and company growth capital was not available as before. Investors lost money and companies went bankrupt. Framfab, the internet consulting firm that had mesmerized spectators by skyrocketing equity values despite meagre revenues, and by its founder always dressing in a furry fibre sweater (*fiberpälströja*), never again came close to its past glory. Icon Medialab, another recognized consultancy firm partly founded by people who had worked with Jan Stenbeck, vanished. Boo.com travelled

from acclaimed start-up in March 1999 to bankrupt 15 months later, after having depleted nearly 1.4 billion SEK (€140 million) of growth capital to sell branded fashion apparel over the internet. Several others lost substantial shareholder value or disappeared. By late 2001 the boom was all but over. But it was not the end of entrepreneurial culture.

Entrepreneurial culture continued and evolved. Today, entrepreneurial culture flourishes in the Baltic Sea Region – not everywhere of course, and not without flaws. Yet, entrepreneurial culture in the region is recognized by three essential attributes: entrepreneurs breaking barriers, a rich habitat of entrepreneurial company investors and a multifaceted confluence or web of support that make up a resilient entrepreneurial foundation.

There are many entrepreneurs in the region arduously labouring to break down barriers and diffuse innovations: Fintech companies contesting the big banks for instance, or green energy entrepreneurs replacing fossil fuels; the foodtech entrepreneurs changing what people eat and how food is produced; and the insuretech entrepreneurs, robotics, transportation, health care – the list goes on. Think of all of them and how they epitomize the Schumpeterian vision of creative destruction, and how their behaviours, ambitions and demeanour is traceable back to the burgeoning entrepreneurial culture some 30 years ago. To them, success is measured in the change they bring about – not in the government support they may or may not receive, neither in policies nor research spending.

Another attribute of entrepreneurial culture is the entrepreneurial company investor – vital for obvious reasons. 'Capitalism is a system for the ownership of production, and it simply cannot work without its main character, the capitalist.'[120] But not just any

120 Erixon and Weigel (2016), "The Innovation Illusion".

investor capitalist. Entrepreneurial culture cannot strive without entrepreneurial investors. When much of Europe's corporate equity scene is comprised of grey capital owners, like some pension funds unfit to offer entrepreneurial support, the Nordic tech scene is somewhat different. It harbours grey capital too, but also entrepreneurial equity investors who support entrepreneurial efforts and are attuned with entrepreneurial culture. The investor community is advanced in terms of its ability to support entrepreneurial companies in different phases of development. This is true for many of the region's venture capitalists, corporate investors, family offices, successful entrepreneurs turned investors and others.

Finally, let us consider the third attribute: entrepreneurial underpinning. Consider how years of working with entrepreneurs have trained business consultants, law firms, headhunters and the like to support entrepreneurs, and the start-up networks that support early-stage companies, such as Stockholm Innovation & Growth (STING) and Sup46 (a community for members). Consequently, talent moves to the region as well. According to the Insead Business Schools Global Talent Competitiveness Index from 2018, Stockholm, Oslo, Copenhagen and Helsinki are all in the top five cities analyzed in attracting talent.[121] First and second-generation immigrants are increasingly becoming entrepreneurs that start and run companies too.

Planning machine vs entrepreneurial culture

The complexities of entrepreneurship script success and failure as close neighbours. Some failed entrepreneurs from the dotcom crash returned to launch new companies; others did not, and some of those who did come back failed again as to be expected – such is the living nature of entrepreneurial culture set in motion

121 Global Talent Competitiveness Index (2018).

some 30 years ago. This is only one example of what the EU must learn to accept and even inspire to, if it is sincere in its ambition to strengthen entrepreneurial culture and make money from science. But is that where the EU is heading? Is the EU becoming more or less entrepreneurial?

A recent paper by Karl Wennberg and Peter G. Klein questions the EU's increasingly mission-led policy interventions, stating that 'targeted policy interventions systematically fail to achieve their intended goals, while also bringing side effects that distort society's long-term ability to generate innovations.'[122] According to the study, the EU distorts competition, has negative crowding out effects and increases risks for corruption. Wennberg and Klein are not alone in questioning the EU's current path for mission-led innovations. Ross Brown takes stock with innovation policies that are mission-oriented in the context of the Scottish National Investment Bank, arguing that policy 'should be context-led rather than mission-led', and 'tailored and aligned to the demand conditions within their local innovation and entrepreneurial ecosystem.'[123] If such studies are correct, all interested in entrepreneurial culture in the EU has reason to be concerned. And there is more.

The Commission ponders on how to protect EU businesses from what it considers unfair competition, including shielding domestic companies from foreign companies (including Chinese firms if they enjoy subsidies, state-backed loans or other forms of government support). The Commission is right to guard against unfair competition and to appraise countries like China. However, unfair competition is a difficult concept and could well be used

122 Klein, Peter G. et al. (2021), "Policy for innovative entrepreneurship: Institutions, interventions, and societal challenges", *Strategic Entrepreneurship Journal*.
123 Ross Brown (2021), "Mission-oriented or mission adrift? A critical examination of mission-oriented innovation policies", European Planning Studies, Taylor & Francis Journals, vol. 29(4), pp. 739-761.

as an excuse for those who like to keep entrepreneurial culture on a tight leash. To decide what's fair and what's not is naturally difficult, and risks not only increasing the monitoring and control of markets, but also influences the EU even more towards a bureaucratic mission-led planning machine. Too much power in the hands of bureaucrats to overtake the role of free markets and to decide on corporate winners and losers is, unfortunately, not likely to help entrepreneurial culture.

It is in the nature of policymaking to sometimes mix or even reverse ends and means, and this is not an unfamiliar theme to the EU either, according to Chris Bickerton. Writing recently about Europe's allegedly failed vaccination efforts, Bickerton stated: 'Until European leaders stop treating policies as an opportunity for pursuing other – often unrelated – goals … we can expect Europe to fail, and fail again.'[124] Entrepreneurial culture is rather sensitive to such mix-ups, and could easily become the victim of unsuspecting political interference. After all, there is no shortage of policies venturing to become oppressive bootheels on entrepreneurial culture in the EU as it is. Entrepreneurial culture may be able to withstand economic downturns, like the dot-com crash, but is not equally resilient to the wrong type of political interference.

It all comes down to this: if the EU desire money from science, it should be watchful of any policy or action that weakens entrepreneurial culture. Secondly, the EU should encourage attributes that make up entrepreneurial culture, including entrepreneurs that break down barriers to new innovations, entrepreneurial company investors, and the constituents of entrepreneurial foundations.

124 Bickerton (2021), "Europe Failed Miserably With Vaccines. Of Course It Did.", *New York Times*.

The EU legislators and member states should consider regional entrepreneurial habitats as precious spaces for entrepreneurs to explore business opportunities and allow for aspirations and explorations of uncertainties – even to the extent that it allows for vested interests to be disrupted and stagnant companies to, ultimately, go bust.

Finally, if the EU wants to make more money from science, obstacles and barriers to innovations, including bureaucracy that delays disruptive innovations, must be replaced with more space for permission-less innovation, and mission-led policy interventions left to rest.

About the authors

Dr. Karsten Friis is a Senior Research Fellow and head of the Norwegian Institute of International Affairs' (NUPI) Research Group on Security and Defence.

Merle Maigre is the Senior Expert on Cyber Security at the non-profit think tank e-Governance Academy (eGA). Previously, she served as the Director of the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE).

Janis Sarts is the Director of the NATO Strategic Communications Centre of Excellence (NATO StratCom CoE) in Riga. He has worked in several positions in the Latvian government, including as a State Secretary at the Ministry of Defence.

Barbara Kunz is a Senior Researcher at the Institute for Peace Research and Security Policy (ISFH) in Hamburg, where she works on European, transatlantic and Nordic security affairs.

Evelin Piirsalu and **Heidi Tuhkanen** are both Senior Experts at the Stockholm Environment Institute's Environmental Management programme in Tallinn.

Björn Weigel is an entrepreneur and business strategist. He is the co-author of *The Innovation Illusion – How so Little is Created by so Many Working so Hard* (2016) with Fredrik Erixon.