Report

The Geopolitics of Power Grids

Political and Security Aspects of Baltic Electricity Synchronization

| Emmet Tuohy | Tomas Jermalavičius | Anna Bulakh |
| Nolan Theisen | Julia Vainio | Artūras Petkus | Hayretdin Bahşi | Yuri Tsarik |

March 2018

RKK ICDS
RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

elering

GLOBSEC
IDEAS SHAPING THE WORLD

Title: The Geopolitics of Power Grids – Political and Security Aspects of Baltic Electricity Synchronization
Authors: Bahşi, Hayretdin; Bulakh, Anna; Jermalavičius, Tomas; Petkus, Artūras; Theisen, Nolan; Tuohy, Emmet; Tsarik, Yuri; Vainio, Julia
Project director: Jermalavičius, Tomas
Publication date: March 2018
Category: Report

Cover page photo: Pylons of high-voltage electricity power lines are seen after sunset outside Goussainville, near Paris, France (REUTERS/Christian Hartmann).
Photo on page 96: Starlings gather on a high voltage electric wire prior to their seasonal migration in Strazeele, northern France (AFP/Philippe Huguen).

Keywords: synchronization, electricity, geopolitics, politics, security, resilience, risk, hybrid threats, Continental grid, Nordic grid, Estonia, Finland, Latvia, Lithuania, Poland, Russia, Sweden

ISSN 2228-0529
ISBN 978-9949-9972-8-2 (PDF)

63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

Table of Contents

Acknowledgments

We would like to thank Elering AS, Estonia's gas and electricity transmission system operator, for its wide-ranging support in producing this report. Throughout numerous in-person meetings and extensive correspondence, our partners at Elering displayed considerable patience in sharing knowledge and insights without which our research and informed judgement would have been impossible; accordingly, we are very grateful to all those members of its team who contributed to our efforts. We also would like to thank all those policymakers and experts in Tallinn, Vilnius, Helsinki, Stockholm, Oslo, Copenhagen, Berlin, Warsaw, Prague, Bratislava, and Budapest who took time from their busy schedules to be interviewed or respond to our requests for information. Because of their candid willingness to share their views and perspectives, we were able to tap into an impressive pool of expertise spanning energy and foreign policy; electricity markets; power generation, transmission and distribution; cyber security; critical energy infrastructure protection; border, maritime and internal security, and defense issues. Needless to say, all errors, omissions, or misjudgments that may appear in this report are solely our own.

Executive Summary

- Russia's grand strategy and its enthusiastic use of various measures short of war (what is known as hybrid war) suggests that the desynchronization of the Baltic states from the IPS/UPS system and synchronization with the Continental (or Nordic) synchronous area may plausibly be exploited by Moscow to further its geopolitical and strategic goals. The range of such goals may include: undermining, discrediting, and destabilizing the Baltic states; isolating them from their allies and partners in NATO and the EU while undermining cohesion and solidarity within both organizations; coercing strategic partners of the Baltic states into accepting or tolerating Russian influence while creating opportunities for various forms of intervention in the three countries.

- Energy has long been Russia's favorite tool of coercion, though to date the focus of attention has been on sectors such as gas and oil. However, electricity generation, trade, transmission, and distribution may certainly be targeted as part of a strategy of hybrid war, as has already happened in Ukraine. Since the desynchronization and synchronization processes – regardless of whether the Continental or Nordic options are ultimately chosen – can create new political, strategic, and physical security vulnerabilities, Russia might opportunistically exploit them. For instance, Russia is capable of sabotaging both submarine and overland electricity infrastructure. Non-kinetic instruments – disinformation campaigns, political influence operations, and cyber-attacks – can also be deployed against those vulnerabilities and thus exploited for destabilization or coercion purposes.

Energy has long been Russia's favorite tool of coercion, though to date the focus of attention has been on sectors such as gas and oil.

- Many indicators show that Russia is preparing its infrastructure to be prepared to exit the BRELL agreement earlier than the Baltic states, which would allow Moscow to deploy coercive instruments to the electricity sector without causing damage to its own economic or security interests. Accordingly, the relative vulnerabilities to sabotage of critical electricity infrastructure linking the Baltic states to the Nordic or Continental areas, as well as the internal and external political resilience of the two areas – particularly of the key synchronization partners Finland or Poland – to Moscow's coercive pressure, will be of crucial importance in ensuring the security of the Baltic states as they pursue their own desynchronization efforts.

- From a security standpoint, the above considerations establish two aspects as critical. First is the presence of sufficient capabilities and effective cooperation frameworks to deter, detect, prevent, and respond to suspected acts of sabotage and/or to minimize the consequences of such acts. Second is sufficient political will, solidarity, firm relationships, and mutual trust among the countries involved to accept the geopolitical risks associated with synchronization and act in crisis circumstances – jointly when necessary – to protect infrastructure critical to synchronous functioning. The report explores these critical aspects by reviewing and assessing the external and internal political resilience of the Nordic and Continental areas, the physical security and resilience of the needed synchronization infrastructure, and cyber resilience. It discusses advantages and disadvantages of synchronization with those areas while also highlighting and evaluating various risks.

- Synchronization of the Baltic states to the Continental grid would provide the considerable advantage of joining the biggest and most reliable electricity system in Europe; however, it brings with it several serious challenges such as internal political dynamics in the region and differences in national energy policies. The political environment in the Visegrád Four (V4) countries, such as the rise of populist Euroskepticism, deterioration of the rule of law, and erosion of independent institutions – particularly in Hungary and Poland – could be a potential threat to trust-building with the Baltics and other EU Member States, while also endangering further support to the infrastructure projects by the European Commission. Russia's growing influence – exercised through internal political and economic actors in some of the V4 countries as well as in Germany – might potentially affect the behavior of these countries during a security crisis falling into the gray

area between war and peace, thereby undermining political cohesion and solidarity or disrupting further integration of European energy markets and infrastructure. Thus, this should also be a particularly serious concern.

Synchronization of the Baltic states to the Continental grid would provide the considerable advantage of joining the biggest and most reliable electricity system in Europe; however, it brings with it several serious challenges such as internal political dynamics in the region and differences in national energy policies.

- Due to its capabilities, overall security policy posture, and NATO membership, Poland should be seen as a country politically willing and militarily rather capable to confront Russia when faced with coercive measures, including those directed against its energy infrastructure. On the other hand, Poland's political relations with countries further "upstream" (particularly Germany) as well as "downstream" (Lithuania) should also be a matter of concern regarding political solidarity and a factor diminishing the external political resilience of the Continental area. For instance, in the event of a security crisis caused by Russia but falling short of outright war (and thus, not leading to the invocation of NATO's Article 5), still remaining unresolved tensions in Lithuanian-Polish bilateral political relations could hamper the timely and effective protection of critical infrastructure connecting the two countries. Should those relations improve – as some early signs suggest is happening – they nonetheless remain at risk of Russia's efforts to undermine them, e.g. through "active measures" targeted at ethno-linguistic minority issues.

Poland should be seen as a country politically willing and militarily rather capable to confront Russia when faced with coercive measures.

- While Poland acknowledges that its political decision to support synchronization is based on its desire to help the Baltic states break their remaining dependency on Russia, Warsaw is concerned by the slow emergence of a unified position among the Baltic states and sees this as a weakness that could be potentially exploited by Russia. At the same time, national energy market and internal political issues clearly dictate the Polish political approach to specific synchronization solutions, i.e. its refusal to consider building a second overland interconnector to the Baltic states. Its unwillingness to open up its electricity market to competition from other EU Member States has led Warsaw to constrain additional electricity infrastructure capacity on its borders, thereby helping to prevent cheaper foreign electricity, which jeopardizes domestic coal-based power generation, from reaching the Polish market. While, as noted, Poland does support synchronization, this support is seemingly based on the implicit condition that the flow of cheaper electricity imports from or via the Baltics be limited.

Warsaw is concerned by the slow emergence of a unified position among the Baltic states and sees this as a weakness that could be potentially exploited by Russia.

- The issue of Baltic synchronization is supported on political level in Hungary, Slovakia, and Czechia, but is not as high a priority for them as it is for Poland. For the public and private sector energy decision-makers in these countries, the synchronization process is a Polish and Baltic issue. Actors in these countries are primarily concerned with guaranteeing that the quality of the Continental grid is not compromised by synchronization. Accordingly, for them, the Baltic states – along with any other potential new entrants – need to fulfill all the requirements of membership. In contrast to Poland, Germany strongly endorses Baltic synchronization precisely because it aligns well with the country's energy policy interests and priorities. However, Berlin – like some Nordic

capitals – seems to be susceptible to Moscow's skillful political manipulation of the Kaliningrad isolation issue, and Russia's portrayal of itself as a victim of Baltic aspirations (especially in terms of economic costs and security of supply disruption).

- Synchronization with the Nordic area would be a more attractive choice for Estonia for many reasons – from mutual trust and shared values (at the political and operational levels) on the role of the state in the electricity market, and the appropriate level of transparency in governance, to the importance of moving towards smart grids that can best accommodate the increased use of renewables. On the other hand, the Nordic option would require much greater time (possibly extending the time horizon of synchronization well beyond 2030), further study, significantly larger financial investments and substantial deployment of political capital by the Estonian government to make it a reality.

In contrast to Poland, Germany strongly endorses Baltic synchronization precisely because it aligns well with the country's energy policy interests and priorities.

Synchronization with the Nordic area would be a more attractive choice for Estonia for many reasons.

  - Currently, attitudes in Nordic capitals to this option range from polite indifference in the case of Helsinki – on a political level, Finland is realistically only willing to support synchronization with Estonia if all needed investments are funded by other parties, e.g. Brussels and/or Tallinn – to skepticism in the case of Oslo and Stockholm. The latter in particular seems to be reluctant to "import" additional geopolitical risk to the Nordic area while seeing little benefit from doing so.

The Nordic option would require much greater time (possibly extending the time horizon of synchronization well beyond 2030), further study, significantly larger financial investments and substantial deployment of political capital.

  - Finland, for its part, continues to view energy trading primarily in economic rather than security terms, and while it is taking steps to improve the resilience of its national grid in the event of what it still sees as an unlikely Russian attempt to damage its infrastructure in a hybrid attack, it also sees no security (or indeed economic) benefit to synchronizing with the Baltic states.

- Meanwhile, in Vilnius, the ongoing Estonian consideration of the Nordic option and insistence on a two-line solution for joining the Continental area are viewed with outright incredulity and hostility, with senior officials bluntly stating that the delayed endorsement of synchronization via Poland using only the existing single-line LitPol Link interconnector endangers Baltic unity on other issues and projects. Lithuanian authorities seem to have a much greater sense of urgency in terms of national security when it comes to synchronization. They consider that their strategic interests – especially preventing electricity imports from the Astravyets Nuclear Power Plant in Belarus, which Vilnius deems highly unsafe – are closely aligned with Poland's desire to limit electricity imports from third parties outside the EU (that is, Russia/Belarus).

- The ability to deter and defend against a physical attack would be higher when synchronizing with the Continental grid for the following reasons:

  - In the maritime domain, surveillance, detection, and response to suspected hostile intent and action is much more complicated than on land due to more complex natural conditions, greater legal ambiguity, higher cost, and lower availability of defensive capabilities (including through collective security and defense frameworks), and other factors. The lack of such

maritime capabilities means that Estonia in particular cannot adequately ensure the protection of submarine cables in case they are physically threatened; moreover, it currently has neither the intentions nor the resources to develop such a capability. Given that the submarine interconnectors have overland sections as well, specific challenges related to overhead lines also apply, thereby increasing the amount of effort and cost required to protect and defend these cables.

- Any possible damage or disruptions in the overhead line(s) between Lithuania and Poland would also be easier to locate and faster to repair compared to the proposed interconnecting submarine lines between Estonia and Finland, where limited availability of repair ships, severe weather conditions, and/or harassment by Russia's military vessels could cause significant delay. Even if the location of the interconnector(s) in the Suwałki Gap could be seen as a vulnerability, the area is widely recognized as a strategic bottleneck between the Baltic states and the rest of Europe that must be protected in the event of a crisis and thus is afforded much higher attention in national and multinational security and defense planning, cooperation, and presence than the Gulf of Finland. However, resilience requires redundancy – in this case, a second interconnector – which Poland is reluctant to commit to building overland for a variety of reasons, including anticipated environmental impact, opposition from potentially affected local communities, economic cost and, implicitly, domestic market protectionism.

Resilience requires redundancy – in this case, a second interconnector – which Poland is reluctant to commit to building overland.

- The land domain is inherently easier for national security authorities to control. The persistent presence of military, security (border guard), and law enforcement personnel in the vicinity of the Suwałki Gap as well as growing investments in technical control measures on the external EU border with Russia and Belarus improve the odds of detecting and preventing any hostile activity (with the exception of the possible use of remotely controlled aerial drones across the international borders by hostile actors). Mobile rapid response land capabilities for security forces, supported by aerial assets, are also cheaper to develop, maintain, and scale up. They are also easier to operate than credible maritime control and response assets. Last, but not least, authorities have the full right to pursue, inspect, and detain suspicious vehicles and individuals, or even seal off entire areas of operation – neither of which is possible to the same extent at sea, at least outside the relatively small space defined as territorial waters.

- Because of heightened geopolitical tensions in the region, membership in military alliances has a relatively strong deterrent effect, giving the Poland-Lithuania connection an advantage over Finland-Estonia links. Despite their close defense cooperation with the Alliance, neither Sweden nor Finland are part of NATO – while the solidarity and mutual security clauses found in the EU's Lisbon Treaty are largely untested. The ability of Finland and/or Sweden to risk broader conflict escalation in the event of attacks on critical submarine infrastructure connecting with the Baltic states is thus rather questionable, especially in terms of their political will to confront hostile action, given that the impact of that action only marginally affects them, and that their response may lead to a direct military confrontation with Russia.

Because of heightened geopolitical tensions in the region, membership in military alliances has a relatively strong deterrent effect, giving the Poland-Lithuania connection an advantage over Finland-Estonia links.

- There are no significant differences between the cyber resilience levels of the Finnish and Polish transmission system operators (TSOs). Although both countries have seen national-level

improvements in the protection of critical infrastructure, Finland demonstrates a more effective whole-of-nation approach to cyber security than does Poland. Finland also has a better position in the Global Cyber Security Index 2017, a measure that not only evaluates critical infrastructure protection but also takes into account all national efforts to enhance cyber security. Looking at the two synchronous grids as a whole, on average, the Nordic countries rank higher than the Continental area members in the Global Cyber Security Index; this is also due to the prevailing culture of public-private, whole-of-society, and whole-of-government collaboration that can also be observed in the cyber security area.

Nordic countries rank higher than the Continental area members in the Global Cyber Security Index; this is also due to the prevailing culture of public-private, whole-of-society, and whole-of-government collaboration.

- From the broad and multidimensional perspective chosen for this report, there is no ideal solution. This stems, first, from the geographical fact that the Baltic states, whichever of the two directions they choose, will remain a small peninsula in a larger synchronous area, connected to that area via a single particular country – Finland or Poland – and via a particular geographical domain (sea or land) each of which has strengths and weaknesses. Second, this finding also flows from the fact that both Finland and Poland – as well as the countries further "upstream" in each synchronous area – have their own understanding of the situation and of their interests, which may not necessarily align either fully or even partially with the perspectives and interests of the Baltic states. Choosing either option entails equally difficult bargaining, compromises, and trust-building. Third, neither of the two areas is a paradise or a promised land; while they have their own distinct advantages, they also contain various deficiencies and risks across all of the dimensions considered in this report.

- The disadvantages of synchronization with either of the two alternatives pale in comparison to the unsustainability and risks of the status quo, that is, remaining in BRELL. The report concludes that, despite various disadvantages and risks in terms of external and internal political resilience as well as its lesser degree of cyber resilience, the Continental option is indeed a somewhat more optimal choice than the Nordic area. However, an important consideration is whether the connection of the Baltic states to the Continental area is sufficiently redundant and robust (i.e. has enough physical resilience) to ensure a strong connection. A one-line solution using only the existing LitPol Link interconnector exposes the Baltic states to a heightened risk of persistent disruption compared to a two-line solution. Such disruption would force the Baltic states to resort to isolated operation more frequently, impose economic costs on the three countries, and might be manipulated by Russia to amplify its negative political and psychological impact. On the other hand, turning down the opportunity of a one-line Continental solution could entail operating in an isolated Baltic area for a very protracted period of time – perhaps between 2020 (when Russia becomes ready to desynchronize) and 2030 (the earliest time when the Nordic alternative might be ready). This significantly prolongs the Baltic countries' window of vulnerability to coercion.

- The likelihood of implementing the two-line scenario is currently rather low in the short- to medium-term, given Poland's reluctance to accept it and Lithuania's strong insistence that a one-line solution is the cheapest and fastest means of pursuing synchronization. However, the odds of the two-line solution might be increased in the long term if Warsaw were provided more incentives to construct a second line by the EU, and if a concerted persuasion effort were mounted not only by the Baltic states but also by other political actors (especially the remaining members of the V4 group and Germany). The likelihood of the Nordic option is equally low, given the complete lack of enthusiasm for it among the Nordic partners, and is unlikely to increase – unless some compelling technical evidence emerges that a one-line scenario is impossible to sustain and unless a political consensus on a two-line solution to the Continental area fails to emerge, which would increase the likelihood of this scenario to medium.

- This leaves two other possibilities. First is the one-line scenario, which is more likely to be implemented if Estonia and Latvia acknowledge the degree of urgency felt in Lithuania, and if all three countries work towards a common understanding of – and mitigation plan for – the associated risks, including agreeing to pursue a two-line solution in the more distant future. Second is isolated Baltic operation by default. (The latter scenario was not examined in this report, as it is very clearly not an optimal solution from a geopolitical perspective, given that it contradicts the long-established strategic paradigm of the Baltic states – ever closer integration into European structures and avoiding being isolated and left on their own).

- As the Baltic states continue moving towards a firm agreement on the way ahead, they will have to think through and address various risks associated with the synchronization of their grids with the Continental area. They will have to work to ensure that the risks identified in the report are mitigated by means of a wide range of measures, such as:

  - maintaining strong situational awareness about Russia's measures directed against vulnerabilities of Western societies, states, and institutions in general – and against desynchronization from IPS/UPS and synchronization with the Continental grid in particular;

  - ensuring unity and close political as well as security cooperation among the Baltic states throughout the synchronization process;

  - continuously communicating and re-affirming the importance of successful synchronization from a security and socio-political stability point of view to their partners and allies;

  - restoring a genuine strategic partnership between Poland and Lithuania based on mutual trust and respect. Lithuania's claims to leadership on the synchronization project would sound more credible and dependable if they rested on a sound political and strategic partnership with Poland;

  - supporting the rule of law, transparent and effective governance, and adherence to shared values across the Continental area, especially in the countries of critical importance to synchronization;

  - enhancing physical protection measures and resilience in the Suwałki Gap (i.e. eventually constructing the second interconnector) and ensuring that critical infrastructure protection in this geographical area continues to be high among the national priorities both of Poland and Lithuania;

  - promoting a more salient role for the EU in such aspects as: the negotiations related to the synchronization process – including in relation to the Kaliningrad issue as well as in building support for implementing a two-line scenario; ensuring solidarity and integrity of crisis management by individual members in the situations short of war; strengthening national abilities, including in close cooperation with NATO, to manage hybrid threats against critical energy infrastructure;

  - working to support well-integrated common EU electricity markets (as part of the Energy Union) while facilitating the development of the EU as a Security Union, particularly with its emphasis on the protection of external borders and critical infrastructure, cyber security, and police and intelligence cooperation;

  - emphasizing the importance of cyber resilience of the electricity sector in the Continental grid and boosting the whole-of-nation and whole-of-alliance cyber security approaches across NATO and the EU;

- reaching out to the Nordic countries to discuss the technical and procedural aspects of utilizing the existing asynchronous interconnectors to ensure security of supply in the event that interconnectors to the Continental area become compromised;

- last, but not least, working to ensure their own national resilience across the board, so that the Baltic states do not become a geopolitical liability or security vulnerability in the eyes of their synchronization partners.

List of Abbreviations

AfD	*Alternative für Deutschland* [Alternative for Germany]
ANO	*Akce nespokojených občanů* [Action of Dissatisfied Citizens]
BRELL	Belarus, Russia, Estonia, Latvia, Lithuania
BSI	*Bundesamt für Sicherheit in der Informationstechnik* [Federal Office for Information Security]
CDU	*Christlich Demokratische Union* [Christian Democratic Union]
CEIP	Critical Energy Infrastructure Protection
CEO	Chief Executive Officer
CERCES	Centre for Resilient Critical Infrastructures
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CRATE	Cyber Range and Training Environment
CSDP	Common Security and Defense Policy
DDoS	Distributed Denial of Service
DNS	Domain Name System
EC	European Commission
EECSP	Energy Expert Cyber Security Platform
EE-ISAC	European Energy – Information Sharing & Analysis Centre
EEZ	Exclusive Economic Zone
ENISA	European Union Agency for Network and Information Security
ENTSO-E	European Network of Transmission System Operators for Electricity
EU	European Union
FCR	Frequency Containment Reserve
FOI	*Totalförsvarets forskningsinstitut* [Swedish Defense Research Agency]
HVAC	High-Voltage Alternating Current
HVDC	High-Voltage Direct Current
ICCP	Inter-Control Center Communications Protocol
ICT	Information and Communication Technology
IPS/UPS	Integrated Power System/United Power System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
JAMK	*Jyväskylän ammattikorkeakoulu* [Jyväskylä University of Applied Sciences]
JRC	Joint Research Center
JYVSECTEC	Jyväskylä Security Technology
kV	Kilovolt
LNG	Liquefied Natural Gas
LPL	LitPol Link
MIRT	Mobile Incident Response Team
MSA	Maritime Situational Awareness
MSB	*Myndigheten för samhällsskydd och beredskap* [Swedish Civil Contingencies Agency]
MW	Megawatt
NATO	North Atlantic Treaty Organization
NIMBY	Not-In-My-Back-Yard
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OT	Operational Technology
PCI	Projects of Common Interest
PESCO	Permanent Structured Cooperation
PiS	*Prawo i Sprawiedliwość* (Law and Justice)
PSE	*Polskie Sieci Elektroenergetyczne*

PST	Phase Shifting Transformer
R&D	Research & Development
SCADA	Supervisory Control and Data Acquisition
SFNTG	Swedish-Finnish Naval Task Group
SIEM	Security Information and Event Management
SNMG	Standing NATO Maritime Group
SNMP	Simple Network Management Protocol
SSDP	Simple Service Discovery Protocol
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TSO	Transmission System Operator
TW	Terawatt
UAV	Unmanned Aerial Vehicle
US	United States
UUV	Unmanned Undersea Vehicle
V4	Visegrád Four
VJTF	Very High Readiness Joint Task Force

Introduction

Emmet Tuohy
Tomas Jermalavičius
Anna Bulakh

In early 2017, ICDS began an investigation of the geopolitical and security aspects of what we call BRELLxit – desynchronization of the power grids of the Baltic states from IPS/UPS system and synchronization with either the Continental or Nordic areas of synchronous operation.[1] The Baltic countries' decision to opt for BRELLxit is obviously a political and geopolitical choice, given their discomfort with continued reliance on a hostile state (and its close ally) for the stability and security of their electricity systems. Since this is such a sensitive and vital area, the political uncertainty and geopolitical risks of status quo are simply deemed too high. Moreover, desynchronization will finally undo one of the last remnants of the legacy of Soviet occupation while further deepening integration with Europe – a symbolic and politically important step for the three nations that, as a region, already represent one of the most integrated corners of the continent given their membership in all European and transatlantic institutions.

Desynchronization will finally undo one of the last remnants of the legacy of Soviet occupation while further deepening integration with Europe.

However, much of the debate and analysis on desynchronization – especially on the choice between the two areas with which the Baltic states could synchronize – has focused on economic costs and benefits, security of supply questions, and technical aspects. The very issues that gave rise to BRELLxit in the first place – geopolitics, political risks, and national security concerns – are most noteworthy by their absence in the synchronization debate. They should be at the heart both of making this strategic decision and of managing its implementation. (Indeed, if purely technical arguments were most relevant, the most rational course of action might well be to keep BRELL intact and remain within the larger IPS/UPS system, while working to improve its governance and reliability). This report seeks to reinsert geopolitics into the discourse and examine the choice of synchronous areas from the security and political perspectives.

The key challenge for the Baltic states is that the desynchronization process has begun in a geopolitical environment that has deteriorated dramatically since the start of Russia's aggression against Ukraine in early 2014. Certainly, even before that point the three countries were far from untouched by various covert efforts by the Kremlin to subvert them, nor were they sanguine about Moscow's strategic methods and objectives – especially after the brief Russian war against Georgia in 2008. However, their relations with Russia reach new lows with each passing year, as the war in Ukraine's east rumbles on and discoveries of Kremlin meddling in democratic processes throughout Western countries continue to be made. The situation is now grave enough for the Western political, security and defense community to consider a conventional military attack on one or several NATO members by Russia as no longer outside the realm of the plausible – or possible. The Baltic states are now considered particularly vulnerable, as reflected in various military deterrence measures undertaken by the Alliance since the 2014 Wales and 2016 Warsaw summits.

The very issues that gave rise to BRELLxit in the first place – geopolitics, political risks, and national security concerns – are most noteworthy by their absence in the synchronization debate.

In this context, desynchronization and subsequent synchronization with the Continental or Nordic grids can become

[1] BRELL – Belarus, Russia, Estonia, Latvia, Lithuania – is an agreement signed between these countries in 2001 to maintain synchronous functioning within the IPS/UPS grid. In 2015, the Baltic states declared their intent to desynchronize from this grid by 2030 at the latest. In this report, the Continental and Nordic synchronous areas are often referred to as Continental and Nordic **areas** or Continental and Nordic **grids**.

the scene of moves taken as part of a broader geopolitical struggle. Furthermore new arrangements for the synchronous functioning of the Baltic grids, while eliminating the geopolitical and security vulnerabilities associated with BRELL, will inevitably bring about a new set of such vulnerabilities associated with the chosen area of synchronization. Those vulnerabilities can be leveraged and exploited by Russia to further its strategic goals vis-à-vis the Baltic states, the EU, and NATO. This report aims to map such vulnerabilities while providing some recommendations on mitigation approaches, primarily through the prism of resilience-building in various domains. It assumes that over the next decade, Russia will remain a geopolitical actor hostile to the West in general and the Baltic states in particular – and that neither the EU nor NATO will disappear. The key question answered in this work is as follows: which option for synchronization is more optimal from a geopolitical, political, and security perspective?

The Baltic states have been discussing synchronization options for a number of years. These options have included:

- Synchronization with the Continental area via Poland by using the existing overland interconnector from Lithuania, LitPol Link (known as the one-line scenario), and possibly building a second interconnector (the two-line scenario).

The emerging consensus supports pursuing the Continental option, with the main remaining bone of contention being whether a second interconnector must be built.

- Synchronization with the Nordic area via Finland by building several (at least three, but possibly up to five) new submarine interconnectors with Estonia. (The current Estlink 1 and Estlink 2 cables are not suited for synchronization purposes).

- Forming a synchronous functioning area of their own (the "Baltic island" scenario).

The emerging consensus supports pursuing the Continental option, with the main remaining bone of contention being whether a second interconnector must be built, or whether a one-line connection is sufficient instead. The Baltic states and Poland are expected to reach a political agreement on implementation by summer 2018, after completing several ongoing technical studies. The European Commission has made synchronization one of its key priorities – for example, including improvements necessary for BRELLxit on the latest biennial Projects of Common Interest (PCI) listing – and has been urging the Baltic states to move towards implementation as soon as possible. At the same time, some stakeholders in Estonia still believe that the Nordic option should not yet be discarded, thereby continuing to cause frictions with Lithuania – which leans strongly towards the Continental option.

The report examines the following dimensions of the Continental European and Nordic areas in order to determine the robustness of each synchronization option:

- **External political resilience**, or factors such as threat awareness (including appreciation among policymakers and operational-level officials of the security aspects of the electricity sector in general/synchronization in particular, as well as their sense that urgent action is needed); stance towards Russia and willingness to confront it in various domains (including energy security); bilateral relations with allies and partners as well as with common institutions (e.g. the EU); and national interests and political support to the Baltic states in their synchronization plans. Vulnerabilities, deficiencies, and failures in this dimension might potentially lead to dangerously misaligned national interests and jeopardize national or collective responses to Russia's general strategy or to its hostile actions;

- **Internal political resilience**, or factors pertaining to the strength of national institutions, socio-political cohesion and resilience to Russia's influence attempts through internal political, societal, or economic actors. As Keith W. Dayton points out "resilience comes from within a country, through rule of law, good governance, a competitive media system, checks and

balances, and transparent and functioning institutions".[2] Vulnerabilities, deficiencies, and failures in this dimension make trust, solidarity, and common approaches between the countries in the same synchronous operation area more difficult, especially in crisis circumstances;

- **Economic resilience**, looking at the cost-effectiveness of the synchronizing interconnectors, their impact on the security of electricity supply to industrial and household consumers, as well as technical aspects such as the functional reliability of the interconnectors and of the target grid in general. This dimension also considers development of electricity markets and national energy policies with regards to market integration, free trade, and climate change mitigation.

- **Physical resilience** of the infrastructure vital for synchronization, including redundancy of planned links, rapidity of recovery in case of damage, etc. This dimension deals with vulnerability to hostile kinetic action, capability of governments to prevent or respond to such action, as well as issues that make the development and use of this capability easier or, conversely, more complicated;

- **Cyber resilience** of the two synchronous areas, that is, indicators demonstrating readiness and ability to cope with cyber-attacks and cyber sabotage efforts directed against synchronous operation, power grid stability, or critical infrastructure more generally. This includes overall cyber security standards, organizational frameworks, and policies with regards to cyber security and incident management by transmission system operators (TSOs), critical infrastructure protection (CIP) authorities, and national governments, as well as the general "health" of cyberspace in the relevant country/synchronous area.

These dimensions are tightly inter-woven, of course: for instance, erosion of internal political resilience compromises external resilience; lack of economic resilience undermines internal political strength and cohesion; deficient physical and cyber security tests external and internal resilience, etc. However, for the sake of comparison, they are treated as distinct domains of equal weight and importance.

The main concern is whether the Baltic states are about to commit themselves politically to a synchronization option with serious deficiencies in some dimensions of resilience.

Based on the research findings, in the overall conclusions each area is assigned a score on a five-point scale, with the scores then added to make a final determination as to which option is more optimal. The main concern is whether the Baltic states are about to commit themselves politically to a synchronization option with serious deficiencies in some dimensions of resilience. Similarly, any further consideration of the Nordic alternative should also reflect its potential shortcomings in terms of resilience. The "Baltic island" scenario, however, has been excluded from the report, as it very clearly contradicts a long-established strategic paradigm of the Baltic states – ever closer integration into European structures and avoiding being isolated and left on their own.

In the Continental area, research efforts for this report focused on Poland as well as a few countries "upstream" (Germany and the Visegrád Three – Czechia, Slovakia, Hungary); in the Nordic area, the main focus was on Finland and Sweden, the two countries with existing electricity connections to the Baltic states, with Norway and Denmark providing additional insights and perspectives. The Baltic states – Estonia at one end, and Lithuania at the opposite – were also covered by the report's authors. The research sought to ascertain the current state of play in those countries and regions across the above-mentioned dimensions, as well as to understand their policy positions, assessments and perspectives on the issues pertaining to synchronization. A series of semi-structured interviews, meetings and e-mail communication exchanges was conducted with foreign, security, defense, and energy policymakers, policy analysts,

[2] Keith W. Dayton, "Director's Letter", *per Concordiam* 8:2 (2017): 4, accessed October 12, 2017, http://perconcordiam.com/perCon_V8N2_ENG.pdf.

and practitioners (primarily at TSOs, but also representatives of security, defense, and energy agencies) from various capitals – in total 66 individuals (see Annex A for their affiliations). Most of these meetings and interviews were held on condition of non-attribution to allow candid and open sharing of knowledge and arguments. Open sources – policy and strategy documents, statements, news reporting, academic/policy analyses & research reports, as well as open databases & indices – provided further materials for assessment. In one particular aspect (cyber resilience), part of the analysis relies on the responses to a survey questionnaire administered to a TSO.

The report does not dive deeply into economic aspects of the synchronization choices, pointing to existing analyses – especially the European Commission's (EC) Joint Research Centre's (JRC) study, released in 2017 – as a backdrop to its own assessments. It acknowledges, however, the emerging consensus based on the JRC conclusions that, from the perspectives of cost, time, security of supply, and technical feasibility, synchronization of the Baltic states with the Continental area is more optimal. However, it notes that there are still lingering doubts in Estonia and Latvia as to whether the Nordic option should be completely off the table. It is hoped that the findings of this report will either help guide policymakers in managing, in an enlightened and strategic manner, the risks associated with implementing the Continental option – should all sides begin taking concrete steps towards pursuing it in 2018 – or contribute towards a more informed discussion regarding the wisdom of pursuing the Nordic option, should it become more widely discussed due to a breakdown in the ostensibly existing political consensus about the Continental option.

Chapter I of the report looks into why and how BRELLxit and Baltic synchronization relates to the Kremlin's strategic playbook, and, consequently, reasserts the importance of geopolitical and security perspective on the subject. Chapters II and III consider the external and internal political as well as economic resilience and vulnerabilities of the Nordic and Continental areas, in turn, with the former also casting a critical look at the search for consensus among the Baltic states. Chapters IV and V analyze physical and cyber resilience, respectively. The report closes with conclusions about which of the synchronous areas represents the most optimal choice, while also making some recommendations about how to mitigate potential pitfalls related to that option.

Chapter I

Moscow's Games: Grand and Petty

Tomas Jermalavičius
Yuri Tsarik
Julia Vainio

In 2009, when Russia temporarily cut off gas supplies to large swathes of Europe due to a dispute with Ukraine, the EU realized that ensuring its energy security required more than just hosting discussions but instead demanded urgent action, notably via diversification of energy sources, suppliers, and supply routes. This was at a relatively early geopolitical stage, when Russia was still – despite its war against Georgia in 2008 – perceived as a "partner" in many quarters across the EU and NATO. In the wake of Russia's aggression against Ukraine in 2014 – resulting in the annexation of Crimea and an ongoing war in the Donbas region – this perception was replaced by a view of Russia as an adversary and a geopolitical threat. Russia's hostile intent towards the established European and global security order is no longer regarded as fiction or paranoia, and the continent's security discourse has become very much driven by a focus on what is often termed as a "hybrid war" waged by the Kremlin regime against the pillars of this order.

Russia's hostile intent towards the established European and global security order is no longer regarded as fiction or paranoia.

This chapter aims to analyze Russia's strategy and modus operandi in the current geopolitical environment to ascertain what role the energy sector – and more specifically, the Baltic states' decision to go ahead with BRELLxit and synchronize with either the Continental or Nordic grids – can play in Russia's grand game. It rests on the assumption that the nature of the regime in Moscow – as well as the way it defines and pursues its fundamental geopolitical interests – will not change radically over the coming decade. The chapter begins by examining the Kremlin's foreign policy playbook and how power grids fit into it. It then considers the measures that Russia is implementing to limit or eliminate its own vulnerability to BRELLxit – and, perhaps, to prepare to utilize power grids and Baltic synchronization in its hostile geopolitical maneuvering. Finally, it articulates the rationale for why and how Russia *would* exploit this issue, from petty punishment to grander strategic coercion to destabilization as a pathway to something much worse and more sinister.

Russia is a revisionist power that is waging a sustained campaign to overturn the established post-Cold War order and erode the multilateral institutions and norms underpinning it.

1. Moscow's Playbook and Power Grids

The Kremlin's geopolitical goals have been much analyzed over the last few years. There is a broad consensus in political and analytical circles across the entire West that Russia is a revisionist power that is waging a sustained campaign to overturn the established post-Cold War order and erode the multilateral institutions and norms underpinning it.[3] It is generally understood that Russia seeks to reassert itself as a "great power" and secure recognition of its sphere of influence – particularly in its close neighborhood but

[3] See, for instance, Ingmar Oldberg, "Is Russia a status quo power?", *UIPaper,* No 1, 2016, https://www.ui.se/globalassets/butiken/ui-paper/2016/is-russia-a-status-quo-power---io.pdf (accessed September 8, 2017); Aaron L. Friedberg, *The Authoritarian Challenge: China, Russia and the Threat to the Liberal International Order* (Tokyo: The Sasakawa Peace Foundation, 2017), http://www.spf.org/jpus-j/img/investigation/The_Authoritarian_Challenge.pdf (accessed October 2, 2017); or Riccardo Alcaro, *West-Russia Relations in Light of Ukrainian Crisis* (Rome: Edizioni Nuova Cultura & Istituto Affari Internazionali, IAI, 2015), http://www.iai.it/sites/default/files/iairp_18.pdf (accessed September 8, 2017).

also beyond – in which other powers defer to Moscow's interests. Edward Lucas quotes an unnamed Russian official some 17 years ago defining the country's aim as ensuring that, in this sphere of influence, "nothing happens that we don't know about, and nothing happens that we don't like…."[4] The problem to Moscow lies in the fact that principal Western political, security, and economic institutions do not necessarily approve of the ways in which Russia responds to things that it "doesn't like." They consequently mount some resistance, whether in the form of economic sanctions or changes to military posture and force positioning. Therefore, Moscow's strategy includes efforts to divide Western institutions – primarily the EU and NATO – to weaken their effectiveness in standing up to Russia's revisionist policies and coercive actions. As Stefan Meister puts it, "its aim is nothing short of paralyzing and sabotaging the decision-making processes of EU and NATO, organizations that depend on consensus, by influencing politics within the individual member states."[5]

In the Kremlin's geopolitical dossier, the Baltic states are certainly a special case (even if not as "special" as, for instance, Ukraine or Belarus).

In the Kremlin's geopolitical dossier, the Baltic states are certainly a special case (even if not as "special" as, for instance, Ukraine or Belarus). Their restored independence and integration into the West came to be seen by Moscow as a lamentable geopolitical loss that conflicts with its national interests and great power ambitions.[6] The fact that countries that were once occupied by (and forcibly incorporated into) the Soviet Union are now part of what the Kremlin deems competing, hostile political and military alliances serves, in its view, as unwelcome evidence of Russia's weakness and "humiliation" at the hands of the West.[7] In the best-case scenario for the Kremlin, this loss is remedied, with the Baltic states falling back into Moscow's sphere of influence if not under its direct control. In a less fulfilling scenario for the Kremlin, Russia grudgingly accepts that the Baltic countries' status as members of NATO and the EU prevent it from re-asserting direct control. Even in the latter scenario, however, Russia is still likely to seek to destabilize the Baltic states in general, while more specifically working to weaken their ties with other Western countries in order to blunt the "success story" narrative and demonstrate that membership in NATO and the EU does not really deliver security and stability unless Moscow's interests are taken into account. As Agnia Grigas notes, "Russian influence in the Baltics aims to constrain their independence and undermine the political, economic, and civilizational choices they have made."[8]

Russia is still likely to seek to destabilize the Baltic states in general, while more specifically working to weaken their ties with other Western countries in order to blunt the "success story" narrative.

Concurrently, membership of the Baltic states in the EU and NATO might be interpreted in Moscow as an opportunity to target these organizations and undermine them from within; this could be done by creating situations involving the Baltic states that would severely test the solidarity, cohesion, and unity of either organization, thus hampering their ability to act. In this line of geopolitical analysis, Russia is pursuing a far greater prize

[4] Edward Lucas, *The Coming Baltic Storm: Baltic Sea Security Report* (Washington DC: Center for European Policy Analysis, 2015), 12, http://cepa.org/sites/default/files/styles/medium/Baltic%20Sea%20Security%20Report-%20(2).compressed.pdf (accessed September 8, 2017).

[5] Stefan Meister, *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign* (Washington DC: Transatlantic Academy, 2016), 7, http://www.transatlanticacademy.org/sites/default/files/publications/Meister_IsolationPropoganda_Apr16_web_0.pdf (accessed September 8, 2017).

[6] See James Greene, "Russian Responses to NATO and EU Enlargement and Outreach", *Chatham House Briefing Papers,* June, 2012, 5-6, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/0612bp_greene.pdf (accessed September 8, 2017).

[7] See Michael Crowley, "Putin's revenge", Politico, December 16, 2016, https://www.politico.com/magazine/story/2016/12/russia-putin-hack-dnc-clinton-election-2016-cold-war-214532 (accessed September 5, 2017).

[8] Agnia Grigas, "Legacies, Coercion and Soft Power: Russian Influence in the Baltic States", *Chatham House Briefing Paper,* August, 2012, 2, http://irsociety.org/wp-content/uploads/2014/09/Legacies-Coercion-and-Soft-Power-Russian-Influence-in-the-Baltic-States.pdf (accessed September 8, 2017).

than just re-asserting influence or control over the Baltic states (which would merely be a welcome side effect); instead, Kremlin's regime is acting to exploit perceived weaknesses and imperfections in the Baltic states and elsewhere to advance its broader objective of weakening the EU and NATO as its geopolitical opponents. The Baltic states, like any other members of the two organizations with potential vulnerabilities, can in this view serve the Kremlin as instruments of its effort to undermine the trust and consensus required for NATO and the EU to operate effectively.[9]

Kremlin's regime is acting to exploit perceived weaknesses and imperfections in the Baltic states and elsewhere to advance its broader objective of weakening the EU and NATO as its geopolitical opponents.

Whether the strategy is a "personal," even petty, game directed specifically against the Baltic states, or part of a broader effort to undermine the West using these countries simply as instruments, it is clear that the Kremlin's so-called "hybrid war" campaign against the Baltic states operates almost continuously.[10] This is not surprising, given that persistence is one of the characteristic features of such campaigns: as Christopher Chivvis points out, "The reality of hybrid war is ever-changing intensity of conflict. Hybrid war strategies are always underway, although at certain moments they may become more acute and intense or cross over into conventional combat operations."[11] Its targets include the liberal democratic political and social order in the Baltic states as well as societal cohesion and economic stability of these countries, their international reputation and bilateral relations with allies and partners, as well as the legitimacy, effectiveness, and even domestic popularity of their economic, social, foreign, defense, and other policies.[12] One of the areas where the Baltic states are being challenged by Moscow is energy security, as the countries have sought to decrease their dependence on Russia – in terms of both supplies and infrastructure – and integrate with the energy markets and systems of the rest of the EU.[13] The Baltic states clearly recognize that the Kremlin will not cease exploring, probing, creating, or exploiting various vulnerabilities in political, societal, economic spheres of life or in their relationships with their allies and partners. In all these areas, trust, common values, consensus, and cooperation are principal assets – and thus important targets of Russia's strategy.

Kremlin's so-called "hybrid war" campaign against the Baltic states operates almost continuously.

The Kremlin deploys a very broad array of instruments of statecraft in its hybrid war campaign against the Baltic states as well as further afield. Those include: economic sanctions and trade restrictions; energy supply disruptions; disinformation and cyber warfare; political and economic corruption and influence-building; support to various

One of the areas where the Baltic states are being challenged by Moscow is energy security, as the countries have sought to decrease their dependence on Russia.

[9] See, for instance, U.S. Army Asymmetric Warfare Group, Ambigous Threats and External Influences in the Baltic States. Phase 2: Assessing the Threat, November, 2015, https://info.publicintelligence.net/AOWG-ThreatsBalticStates.pdf (accessed September 12, 2017).

[10] See U.S. Army Asymmetric Warfare Group, Ambiguous Threats and External Influences in the Baltic States.

[11] Christopher S. Chivvis, *Understanding Russian "Hybrid Warfare" And What Can Be Done About It* [Testimony presented before the House Armed Services Committee] (Santa Monica: RAND Corporation, 2017), 2, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf (accessed September 8, 2017).

[12] See, for example, Henrik Praks, *Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics – the Case of Estonia* (Rome: NATO Defense College, 2015), https://www.icds.ee/fileadmin/media/icds.ee/failid/Henrik_Praks_-_Deterring_and_Defeating_Russia_s_Ways_of_Warfare_in_the_Baltics.pdf (accessed September 8, 2017).

[13] Simon Hoellerbauer, "Baltic Energy Sources: Diversifying Away from Russia", *Baltic Bulletin: Foreign Policy Research Institute*, June 14, 2017, https://www.fpri.org/article/2017/06/baltic-energy-sources-diversifying-away-russia/ (accessed September 12, 2017).

political and societal movements, including extremists and Russian-speaking minorities; "lawfare"; military threats and violations, etc.[14] In some cases, Russia acts openly – albeit often under a variety of false pretexts – but in many others, it uses clandestine measures to mask its intent and make attribution more difficult/deniability more plausible; such measures include the use of proxies such as sympathetic political and societal actors or organized crime (including cybercrime) groups, as well as intelligence assets.[15] The result is what is often termed "gray zone" conflict, which is "best understood as activity that is coercive and aggressive in nature, but that is deliberately designed to remain below the threshold of conventional military conflict and open interstate war."[16]

Manipulation, subversion, sabotage, and destabilization—that is, measures falling short of war—are the preferred ways of deploying the instruments of state power at the Kremlin's disposal.

Manipulation, subversion, sabotage, and destabilization – that is, measures falling short of war – are the preferred ways of deploying the instruments of state power at the Kremlin's disposal. However, it is equally important to note that Moscow combines those instruments in a comprehensive, dynamic, and flexible way and is not shy to use its military power if necessary – all in order to seize and maintain the initiative while locking in a strategic advantage. The Kremlin already has a rather solid record of taking bold geopolitical risks (its annexation of Crimea and intervention in Syria being prime examples) and is bound to generate surprises at various inflection points. Thereby it will continue creating situations in which its geopolitical opponents are caught off guard, kept off balance, and unable to respond in a coherent, effective, and legitimate way. This approach is sometimes referred to as hitting the "chaos button," that is, creating controlled periods of chaos that confuse and weaken the opponent.[17] Failure to recognize and understand the Kremlin regime's modus operandi increases the risk that one may be subject to unpleasant surprises, or may lead one to overlook and underestimate vulnerabilities that Russia is already secretly probing.

Failure to recognize and understand the Kremlin regime's modus operandi increases the risk that one may be subject to unpleasant surprises.

Russia's use of the energy sector as a conduit for strategic coercion has been recognized for a long time.

Russia's use of the energy sector as a conduit for strategic coercion – defined as "the deliberate and purposive use of overt threats to influence another's strategic choices" – has been recognized for a long time.[18] In particular, oil and gas supplies have served as potent tools in raising the costs for (or extracting concessions

[14] See a succinct list in Edward Lucas, "The Kremlin's 20 Toxic Tactics", *Europe's Edge,* October 30, 2017, http://cepa.org/EuropesEdge/The-Kremlins-20-toxic-tactics (accessed November 1, 2017).

[15] See Keir Giles, *Russia's 'New Tools' for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power* (London: Chatham House, 2016), 27-46, https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf (accessed September 8, 2017); Orysia Lutsevych, *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood* (London: Chatham House, 2016), https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-04-14-agents-russian-world-lutsevych.pdf (accessed September 8, 2017); or Mark Galeotti, *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe* (London: European Council on Foreign Relations, 2017), http://www.ecfr.eu/page/-/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf (accessed September 8, 2017).

[16] Hal Brands, "Paradoxes of the Gray Zone", Foreign Policy Research Institute, February 5, 2016, https://www.fpri.org/article/2016/02/paradoxes-gray-zone (accessed September 9, 2017).

[17] See Flemming Splidsboel Hansen, *Russian Hybrid Warfare: A study of disinformation* (Copenhagen: Danish Institute for International Studies, 2017), 10, http://pure.diis.dk/ws/files/950041/DIIS_RP_2017_6_web.pdf (accessed August 16, 2017)

[18] Lawrence Freedman, "Introduction" in *Strategic Coercion: Concepts and Cases,* editor Lawrence Freedman (Oxford: Oxford University Press, 1998), 3.

from) opponents, as well as in punishing them for lack of compliance with Russia's demands and interests. Writing as early as 1998, Elaine Holoboff concluded: "It is clear…that Russia has not hesitated to use oil as a mechanism of diplomacy, and that on a number of occasions this has taken the form of coercive acts directed against its neighbors."[19] One good example is the closure (for "repairs") of the oil export pipeline from Russia to Lithuania in 2006 when the latter refused to sell its oil refinery to a Kremlin-friendly oil corporation (the pipeline is still being "repaired" as of 2018).[20] The targets of the Kremlin – especially the Baltic states – have been undertaking various steps to diversify their energy supply sources and routes and to limit Russia's influence in European energy markets. The electricity sector and the critical energy infrastructure (CEI) that supports it have received much less attention as a potential arena for Russia's hybrid war than the gas or oil sectors.[21] This could be because, until recently, Russia did not have a significant history of using electricity as a geopolitical tool; moreover, at least in the Baltic states, only Lithuania has been highly dependent on imports of Russian electricity – due to the closure of the Ignalina Nuclear Power Plant in 2009. Russia's own dependence on IPS/UPS grid stability obviously plays a role as well.

The electricity sector and the critical energy infrastructure (CEI) that supports it have received much less attention as a potential arena for Russia's hybrid war than the gas or oil sectors.

However, due to its critical importance to the functioning of society, the electricity sector has already proven to be an attractive target during intra-conflict coercion in other theatres of Russian action, as physical attacks on the infrastructure of the power supply systems in Luhansk and Donetsk regions of Ukraine demonstrate. According to a report from the NATO Energy Security Centre of Excellence, several power plants, substations, and power lines came under targeted fire on multiple occasions, leading to over a thousand power outages in the Donetsk region alone.[22] These were mainly caused by damage to the 35-110 kV power lines during the first year of the conflict. There were also several reported incidents in which Russian proxy fighters obstructed infrastructure repairs by firing on repair teams. These attacks might not have been undertaken for tactical military advantage, but instead for the strategic objective of undermining societal and economic resilience.

The electricity sector has already proven to be an attractive target during intra-conflict coercion in other theatres of Russian action, as physical attacks on the infrastructure of the power supply systems in Luhansk and Donetsk regions of Ukraine demonstrate.

Kinetic attacks aside, cyber-attacks on the electricity distribution system of Ukraine using "BlackEnergy3" malware caused a large-scale blackout in December 2015 and affected more than 200,000 consumers. Investigators suspected a Russia-linked group of hackers – initially Fancy Bear, then Sandworm Team – as perpetrators of this cyber-attack.[23] While putting Ukraine's government and society under more strain in the ongoing conflict, it

[19] Elaine M. Holoboff, "Bad Boy or Good Business? Russia's Use of Oil as a Mechanism of Coercive Diplomacy" in *Strategic Coercion: Concepts and Cases*, ed. Lawrence Freedman (Oxford: Oxford University Press, 1998), 209.

[20] "Russia Won't Re-Open Oil Pipeline, Lithuania Says", *Reuters,* October 11, 2007, http://uk.reuters.com/article/lithuania-russia-oil/russia-wont-re-open-oil-pipeline-lithuania-says-idUKL1159854520071011 (accessed October 5, 2017).

[21] As an illustration of the amount of attention devoted to electricity supply as opposed to gas and oil, see F. Stephen Larrabee et al, *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures* (Santa Monica: RAND Corporation), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1305/RAND_RR1305.pdf (accessed September 8, 2017)

[22] Oleksandr Sukhodolia, Dmytro Bobro, Vytautas Butrimas, Jaroslav Hajek, and Sergii Karasov, *Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine* (Vilnius: NATO Energy Security Centre of Excellence (ENSEC COE), 2018 [forthcoming]).

[23] Donghui Park, Julia Summers, Michael Walstrom, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks", *The Henry M. Jackson School of International Studies (University of Washington),* October 11, 2017, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/ (accessed October 31, 2017).

also served as a harbinger of the future use of cyber tools to destabilize and exert coercive pressure, including by targeting critical energy infrastructure.[24]

Although this report does not consider vulnerabilities during a protracted military conflict like that currently experienced by Ukraine in the Donbas region, Russia's willingness to target electricity infrastructure in such conflicts (whether directly or via proxies) suggests that for Moscow, this vital infrastructure is fair game for action designed to destabilize and coerce opponents. Low-risk, low-cost, low-intensity attacks on CEI, such as destroying substations or power lines (see Chapter IV) or conducting paralyzing cyber-attacks on the grid, would test the Baltic states and their allies and partners while keeping the situation in the ambiguous "gray zone" of conflict. Less ambitiously, various "active measures" such as support to the environmental activists and "not-in-my-backyard" (NIMBY) activists opposed to infrastructure development projects (e.g. electricity interconnectors), disinformation campaigns to discredit those projects, and political influence-peddling to obstruct their progress provide ways for Moscow to derail or slow down BRELLxit by the Baltic states.

2. Entering the Danger Zone?

There are some indications that the electricity grids of the Baltic states could become an appealing target in Russia's strategy – as a means of raising the political and economic costs and reducing the benefits of BRELLxit for the Baltics as well as their allies and partners, or as an instrument of putting pressure on the region's stability, cohesion, and solidarity. Russia has continuously opposed the Baltic states' aspirations to leave the UPS/IPS synchronous area, citing both the economic unsuitability of the project as well as its concerns over stability of electricity supplies to the Kaliningrad region. However, as early as 2015, in practice if not in rhetoric, the Russian government accepted the prospect of BRELLxit as a reality and commenced activities designed to reduce its own vulnerabilities once it takes place. Those activities include:

Russia has continuously opposed the Baltic states' aspirations to leave the UPS/IPS synchronous area.

- expanding generation and transmission capacities in its North-West and Central united energy systems in order to turn the North-Western Federal District into a net producer of electricity by 2030;
- modernizing the transmission grids within the Kaliningrad and Pskov regions;
- equipping the Kaliningrad region with dual-redundancy power generating capacities (constructing 4 new fossil-fuel generating stations with a total output of 1 GW);
- ensuring dual-redundancy gas supplies to the Kaliningrad region via sea (constructing an LNG terminal with a total annual import capacity of 2 billion cubic meters [bcm] of gas; it should be noted that thanks to modernization, the total gas consumption in the region will decrease from 1.3 bcm/year to 1 bcm/year due to increased efficiency);
- expanding natural gas storage capacities in Northwest Russia to ensure supplies to St. Petersburg, especially during winter.

While most of these plans have already been reviewed in our previous study, Russia's plans in the Pskov region merit renewed attention.[25] On June 9, 2016, the Board of Directors of Rosseti, the state-owned grid operator, headed by Minister of Energy Alexander Novak, adopted a number of "strategic decisions" (as they were termed in the official press

[24] See, for instance, Jason Healey and Michelle Cantos, "What's next for Putin in Ukraine: Cyber escalation?" in *Cyber War in Perspective: Russian Aggression against Ukraine,* ed. Kenneth Geers (Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2015), 153-158, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Healey_Cantos_17.pdf (accessed October 31, 2017).

[25] See Emmet Tuohy, Anna Bulakh, and Yuri Tsarik, *Desynch or Sink – A Political Analysis of Baltic Electricity Desynchronization.* (Tallinn: International Centre for Defense and Security, 2017), https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Analysis_Desynch_or_Sink_Tuohy-Bulakh-Tsarik_May_2017.PDF (accessed August 1, 2017).

release).[26] These will enable the company to accomplish a number of objectives, including implementation of a federal-level investment project in the Pskov region that will maintain stable electricity supplies to consumers in the event of Baltic states' desynchronization. These decisions were later integrated into the 2016–2025 investment program of the North-West inter-regional transmission grid company.[27] The program includes plans for the massive reconstruction of overhead transmission lines, security improvements, and the modernization of defect detection systems, information collection and transmission systems, communication channels, and other elements.

Moscow is clearly eager to be fully prepared for BRELLxit four to five years before the Baltic states are ready themselves.

Relations in the energy sphere will instead continue to serve the Kremlin's wider strategy towards the Baltics, Central Europe, and the EU as a whole, rather than the other way around.

The project's cost is estimated at 3 billion rubles (approximately €43 million). The timeline is aligned with Russia's other plans in the region; that is, it includes intensive spending from 2016–2021, but provides for zero spending from 2022–2025. This is just another illustration of the pre-emptive nature of Russia's plans with regard to desynchronization. Moscow is clearly eager to be fully prepared for BRELLxit four to five years before the Baltic states are ready themselves – thereby giving the Kremlin a freer hand beginning in 2020 to exploit the situation more strategically and without undermining Russia's own energy security. As one Nordic TSO expert noted, "should Russia desynchronize well ahead of the Baltic states, I would not want to be in the shoes of someone in Vilnius, Riga, or Tallinn."

3. Power to Coerce through Power Grids

Russia's policies in the Baltic region are designed with political rather than economic goals in mind. As the interviewed experts from Russia and Belarus (see Annex A) believe, while implementation of BRELLxit might further strain Moscow's economic relations with the Baltic states (as well as the EU), it will not define and drive Russia's overall political conduct in the region. Relations in the energy sphere will instead continue to serve the Kremlin's wider strategy towards the Baltics, Central Europe, and the EU as a whole, rather than the other way around.

Punishing the Baltic states for their desynchronization aspirations would be in line with Moscow's established policy of demonstrating that any attempt to end a critical dependency on Russia inevitably has consequences.

How could disrupting the desynchro-nization process and undermining its outcomes advance Russia's broader strategic goals? First of all, punishing the Baltic states for their desynchronization aspirations would be in line with Moscow's established policy of demonstrating that any attempt to end a critical dependency on Russia inevitably has consequences; such retaliation would in Moscow's view serve as a deterrent to other states considering similar actions while being of domestic propaganda value inside Russia

[26] "Совет директоров ПАО «Россети» принял ряд стратегических решений" [The Board of Directors of Rosseti adopted a number of strategic decisions], Rosseti Россети, June 10, 2016, accessed August 1, 2017. http://www.rosseti.ru/press/news/?ELEMENT_ID=26881&sphrase_id=301177.

[27] "Приказ Министерства энергетики Российской Федерации «Об утверждении изменений, вносимых в инвестиционную программу ПАО «МРСК Северо-Запада», утвержденную приказом Минэнерго России от 30.11.2015 № 906»" [Decree of the Ministry of Energy of the Russian Federation "On the approval of changes made to the investment program of the public JSC 'IDGC North-West', passed by the decree of the Ministry of Energy of Russia No 906 on November 30, 2015], IDGC North-West МРСК Северо-Запада, December 16, 2016, accessed August 1, 2017. http://www.mrsksevzap.ru/cs/Satellite?blobcol=urldata&blobheader=application%2Funknown&blobheadername1=Content-Disposition&blobheadername2=MDT-Type&blobheadervalue1=inline%3B+filename%3DInvestitcionnaia_programma_na_2016-2025_gody.rar&blobheadervalue2=abinary%3B+charset%3DUTF-8&blobkey=id&blobtable=MungoBlobs&blobwhere=1384344669352&ssbinary=true.

as well. Second, causing costly and frequent breakdowns and other failures in the wake of synchronizing with the Continental or Nordic grids would steadily undermine the reputation of the Baltic states' governments domestically and internationally, putting additional pressure on their economic systems (e.g. through the higher costs of having frequently to operate in an isolated mode).[28] This would be instrumental in promoting a sense of instability, insecurity and incapability of coping with crisis in the Baltic states, thereby eroding public trust of these societies in their governments while undermining the legitimacy of their policies – specifically those of confronting Russia in general and of desynchronization in particular. The popular discontent created or magnified by such efforts could further be utilized by Moscow to strengthen its political position in the Baltic states by, for example, meddling in elections.

A mix of overt and covert measures against the synchronization project and future functioning of the Baltic states' grid as part of the chosen synchronous area could potentially strain their mutual relations as well as relations with other allies and partners.

Third, a mix of overt and covert measures against the synchronization project and future functioning of the Baltic states' grid as part of the chosen synchronous area could potentially strain their mutual relations as well as relations with other allies and partners (e.g. Poland or Finland). This is particularly plausible if those allies and partners do not come to appreciate the importance of the power grid interconnectors to the Baltic states' security, do not prioritize their protection, and/or do not act with a sense of urgency in geopolitical crisis situations affecting the Baltic states. If timed carefully to coincide with a downturn in bilateral relations e.g. between Poland and Lithuania, such measures would place an even greater strain on political solidarity. A serious solidarity failure, in turn, would foster a sense of abandonment and isolation in Baltic societies and endanger the political cohesion of NATO and/or the EU. Indeed, relations among the Baltic states themselves could become a target, with the Kremlin creating the image of the Baltics as indecisive, disunited, and unable to cooperate effectively – as described in Chapter II.

It would be entirely in keeping with Moscow's existing playbook to prepare the soil in Warsaw or Helsinki, or perhaps even farther afield (Stockholm or Berlin) so that the policy positions and crisis behaviors of those nations in a narrowly synchronization-related or even a broader and more multi-dimensional political crisis fit with the Kremlin's expectations and interests. Such "shaping operations" could include clandestine political influence-building to disrupt crisis decision-making as well as various efforts to diminish the value of the Baltic states in the eyes of the publics and political elites of those nations. In addition to reducing the perceived benefits of synchronizing with the Baltic states, such operations would also seek to influence perceptions of the political, economic and security costs – thereby making efforts undertaken on the Baltics' behalf appear too high, and therefore acceptance of a Russian "solution" to such a crisis more likely. In short, it would be reasonable to expect that Moscow will seek to steer various capitals into believing that it is not worth "importing" additional geopolitical risk by accepting synchronization with the Baltic states or, even if they *do* accept it, that it would still not be worth maintaining the synchronous links during a potential future security crisis in the region.

It would be reasonable to expect that Moscow will seek to steer various capitals into believing that it is not worth "importing" additional geopolitical risk by accepting synchronization with the Baltic states.

In the run-up to desynchronization, the issue of Kaliningrad seems to be emerging as an

[28] See Chapter IV concerning an isolated (asynchronous) mode operation of the Baltic states' grids.

example of the kinds of issues used in such influence campaigns. As pointed out earlier in this chapter, Russia is undertaking measures to mitigate the impact of desynchronization on the exclave. Yet, the Kremlin might be eager to create a false perception of the potential adverse economic impact in order to reduce political will for synchronization with the Baltic states. The fact that concern about the issue of Kaliningrad was raised in conversations with this report's authors in various capitals (e.g. Berlin, Stockholm) shows that there is already some potential to exploiting this instrument either to obstruct desynchronization or to exact a steep(er) price for it.

4. One-Time Shot, or Part of a Bigger and Sinister Game?

It is, of course, possible to imagine a scenario whereby Russia would take no major steps to prevent or derail BRELLxit or undermine synchronous functioning of the Baltic grid with the Continental or Nordic grids. It would simply keep developing its energy systems assuming that BRELLxit will, sooner or later, become a reality. "Let's wait and see what happens next" seems to be the general stance in various Russian and Belarusian policy circles on the BRELLxit issue at the moment. In this crisis-free scenario, we could expect only some "huffing and puffing" from Moscow, to register its dissatisfaction and maintain the appearances of geopolitical cleavage (a few years ago Russia complained about the potential costs of up to €2.5bn, the impact on the Kaliningrad region, and a lack of consultation by the Baltic states), but no real action to subvert or derail BRELLxit.[29]

If Russia does decide to take such actions, one potential example would be a one-time physical attack on the individual interconnectors by clandestine means; however, according to the experts interviewed for the current report, this attack would not create enough physical disruption to make such an attack worthwhile.[30] This is mainly for two reasons: first, by the time Baltic synchronization to either grid is completed, the resilience of the Baltics' own electricity system already needs to be great enough to withstand partial or even complete disconnection from other synchronous areas for a certain period of time.[31] Second, the risk that a one-time attack would escalate into a broader conflict is too high to merit doing so solely for the sake of harming the Baltic synchronization project.[32] "Active measures" against the Baltic synchronization project are more likely and could include less abrasive but potentially equally disruptive means such as disinformation campaigns, political manipulation, and cyber-attacks. In fact, cyber-attacks were identified by some interviewed experts as both as more likely and more fruitful. The cyber domain would be a very suitable medium for attacks in which a coercive message can be delivered with a reasonable degree of plausible deniability, due to the attribution problems inherent in cyberspace.[33]

"Active measures" against the Baltic synchronization project are more likely and could include less abrasive but potentially equally disruptive means such as disinformation campaigns, political manipulation, and cyber-attacks.

[29] Anca Gurzu, "Baltics threaten to unplug Russian region", *Politico,* April 11, 2015, https://www.politico.eu/article/baltics-threaten-to-unplug-russian-region-power-kaliningrad-electricity-interconnectors-lithuania-poland-sweden/ (accessed August 20, 2017).

[30] Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[31] Heiki Jakson, former NATO expert on critical energy infrastructure, interview, Helsinki, August 16, 2017; Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[32] Miguel Simões, OF-3/PAO, and Andrew Camp, OF-4/ J2X CI/ HUMINT, NATO Force Integration Unit Lithuania, interview, Vilnius, August 31, 2017.

[33] According to the majority of the interviewed experts, cyber-attacks would be easier to conduct from afar, they leave less traces and usually require less work force compared to physical attacks. Cyber-attacks could also be conducted easier than physical attacks by other than state-controlled actors. However, this would be dependent on the chosen target, expertise of the perpetrator and the resources available. Cyber resilience of the two synchronous areas / grids is compared in Chapter V. Experts: Experts from the Ministry of Foreign Affairs of Lithuania, interview, Vilnius, June 13, 2017; Heiki Jakson, former NATO expert on critical energy infrastructure, interview, Helsinki, August 16, 2017; Communications Department of Litgrid, interview, Vilnius, June 13, 2017; Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

However, there **are** reasons why the Kremlin *would* be willing to carry out a one-time attack: to highlight a new vulnerability of the Baltic states (and thereby indicate the willingness and ability to exploit it when the need arises); to deliberately raise the stakes in the event of a simultaneous acute spike in geopolitical tensions in North-East Europe, in order to sow confusion or acquire leverage; or simply to distract attention from other vectors of strategic action in the Baltic region or elsewhere. While less likely than non-kinetic "active measures", and while likely to cause more of a nuisance than a massive disruption, the possibility of such a "one-time shot" attack cannot therefore be entirely excluded. Its psychological impact would be strongest if the targeted physical link between the Baltic states and the new synchronous area is weakest (that is, if the single overhead line to Poland is the only link to the rest of a synchronous operation area).

While less likely than non-kinetic "active measures", and while likely to cause more of a nuisance than a massive disruption, the possibility of a "one-time shot" attack cannot be entirely excluded.

At the more extreme end of the range of potential crisis scenarios, a series of physical strikes against synchronization infrastructure would not just be a one-time attack, but be part of a larger, more comprehensive campaign aimed at the large-scale, severe destabilization of the region. Of course, the possibility that Russia will resort to using such escalated tactics very much depends both on its internal political developments as well as on the opportunity perceived by the Kremlin in a more global or at least broader regional context, e.g., if the regime starts preparing to undertake more conventional aggression and sees the need to prepare the way for it in non-military domains first. This more extreme scenario might include (but would not be limited to) the following activities:

- acts of cyber sabotage (not confined only to CEI);
- acts of physical sabotage of critical infrastructure on land and at sea;
- sparking protests among ethnic minorities in the Baltic states (and possibly Poland);
- financing and orchestrating violent activities of radical activists;
- activating influence agents in domestic politics to muddle, obstruct, and delegitimize crisis decision-making;

Targeting critical energy infrastructure and future synchronization of the Baltic states, particularly when "bundled" with other tools of coercion, "adds value" to the adversary's broader strategy in a variety of ways.

- initiating cuts in energy (electricity, gas) supplies to the Baltic states;
- stepping up the scale and intensity of its disinformation campaign;
- conducting large-scale military maneuvers around the Baltic states – including in the vicinity of vulnerable areas connecting them with neighboring EU countries (e.g. in the Suwałki Gap connecting Lithuania and Poland, or in the Gulf of Finland between Finland and Estonia).

At the more extreme end of the range of potential crisis scenarios, a series of physical strikes against synchronization infrastructure would be part of a larger, more comprehensive campaign aimed at the large-scale, severe destabilization of the region.

This is a scenario in which more than one synchronous link might come under kinetic attack – as opposed to a one-time blow against a single interconnector. It highlights that targeting critical energy infrastructure

and future synchronization of the Baltic states, particularly when "bundled" with other tools of coercion, "adds value" to the adversary's broader strategy in a variety of ways. Unlikely as it might sound at the moment – given that it would represent a conventional military attack on a NATO ally – this scenario has to feature in crisis planning, preparedness and mitigation, much the same as prudent military defense planning always addresses the worst-case (i.e. conventional war) scenario without fully expecting it to become reality.

Conclusion

Although often downplayed or even overlooked, the electricity sector – including its physical infrastructure – is vulnerable to many of the tricks in Moscow's playbook and is becoming part of its repertoire of coercion and hybrid war. This does not necessarily mean that Russia will definitely choose to pursue the desynchronization issue – and the attendant vulnerabilities for the Baltic states – as a matter of policy. Nevertheless, given Russia's general modus operandi in the region as well as the specific preparations it is making for Baltic desynchronization, it should not come as a surprise that exploiting BRELLxit could become one of the planks of Moscow's strategy towards the Baltic states and, by extension, Europe.

The odds are too high and the field too vital to the national security of the Baltic states to leave it to hope and expectation that Moscow will "play nice" and that power grids will somehow remain immune to geopolitics, coercion, and hybrid war games, whether petty or grand.

Despite the ostensible political inertia and drift with regard to BRELLxit-related strategic opportunities in Moscow's current thinking, Baltic desynchronization efforts could be turned by the Kremlin into a major political issue literally overnight. This could be done either to derail desynchronization or simply to make it more costly – the latter being a gesture of petty retaliation not out of character given Moscow's practice in relations with its neighbors. Likewise, tampering with the process of desynchronization and future functioning of the Baltic states as part of the Continental or Nordic grids could become yet another instrument in a complex "hybrid" toolbox of the Kremlin to advance its broader strategic aims. Which way it goes will depend mostly on both internal political developments in Russia and on evolutions in the regional and global context; accordingly, anticipating the characteristics of various scenarios, let alone attaching any specific degree of likelihood to them, is very difficult. What is within the "art of the possible" is to map the potential vulnerabilities and work to mitigate or eliminate them.

It is thus necessary to underscore the point that resilience and integrity – of political institutions and crisis management decision-making, of bilateral relations, trust and solidarity in crisis situations, and of electricity systems and markets as well as of the infrastructure linking them – are important parameters in weighing the choices and designing future steps and threat mitigation measures by the Baltic states, whichever option is chosen for synchronization. The benefits and risks associated with each option – Continental or Nordic – is the subject of the remainder of this report. It is clear though that the odds are too high and the field too vital to the national security of the Baltic states to leave it to hope and expectation that Moscow will "play nice" and that power grids will somehow remain immune to geopolitics, coercion, and hybrid war games, whether petty or grand.

Chapter II

Stopping at the Water's Edge? Baltic (Dis)unity and the Nordic Option

Emmet Tuohy

Politics, as the American saying goes, stops at the water's edge. Popularized by Sen. Arthur Vandenberg (R-Mich.), whose isolationist views changed rather abruptly after the bombing of Pearl Harbor, it has traditionally meant that even significant political differences at home should not affect the pursuit of major international projects overseas – such as the founding of NATO, which owed much to Vandenberg's efforts. While the Baltic states may not form a single political unit like the United States, they are far too often perceived as a monolithic entity by other countries even in the Baltic Sea region, not to mention in Brussels, Washington, or further afield. Even if this perception is of course quite unjustified given the quite different cultures, histories, languages, and – perhaps most of all – energy security situations of the three countries, it continues to fuel frustration with the lengthy period of time it often takes for Riga, Tallinn, and Vilnius to agree on issues such as the preferred option for electricity desynchronization.

Politics, as the American saying goes, stops at the water's edge.

But can policymakers in the three capitals follow Vandenberg's advice, and keep their differences on desynchronization confined to the shores of the Baltic? Or is there a possibility that they will fail to reach a final agreement in the time that they have available – thereby endangering not only the project of synchronizing with other European Union countries, but even the continued future of links among themselves? To answer these questions, however, one must review what the current options are for the Baltic countries and assess the benefits and risks – both (geo)political and economic – of the most controversial of those options: the choice to synchronize with the Nordic countries.

Can policymakers in the three capitals keep their differences on desynchronization confined to the shores of the Baltic? Or is there a possibility that they will fail to reach a final agreement in the time that they have available – thereby endangering not only the project of synchronizing with other European Union countries, but even the continued future of links among themselves?

1. Defining the Water's Edge: Synchronization Options and The Baltic Debate

1.1 To Agree or Not to Agree?

Released just ahead of a May meeting in Tallinn of the prime ministers of Poland and the three Baltic states to discuss electricity synchronization, our previous study concluded by noting that there remained "some difference of opinion" among the countries about which desynchronization option was best.[34] Unfortunately, neither that meeting – explored in more detail below – nor other negotiations in the ensuing months brought much clarity to the debate. At times, in fact, clarity has been so lacking that casual – or

[34] Emmet Tuohy, Anna Bulakh, and Yuri Tsarik, *Desynch or Sink: A Political Analysis of Baltic Electricity Desynchronization* (Tallinn: International Centre for Defense and Security, 2017), 14, https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Analysis_Desynch_or_Sink_Tuohy-Bulakh-Tsarik_May_2017.PDF.

indeed, even not-so-casual – observers would be forgiven for concluding that there was no longer a debate at all. For instance, after the meeting, Lithuanian prime minister Saulius Skvernelis declared that "After a decade of no decision, a decision in principle has been adopted," giving rise to headlines such as "Baltics Agree on Grid Synchronization Via Poland."[35]

However, less than a month later, Elering CEO Taavi Veskimägi noted in an interview with Bloomberg that the three countries had "yet to agree" on an option.[36] Estonian prime minister Jüri Ratas' acceptance of synchronization via Poland was "conditional" on the construction of two separate links between Poland and Lithuania, whereas Lithuania preferred to pursue synchronization via the existing single link. For Veskimägi and a "wide consensus" of those in Estonia the "only way to synchronize with Central Europe is by *two* separate routes between Lithuania and Poland," the Elering executive concluded that "a link-up to Nordic systems remains an option." [37]

Seemingly undermining that wide consensus ahead of a meeting with his Latvian, Lithuanian, and Polish counterparts in Vilnius in October, however, Riigikogu (Estonia's parliament) EU Affairs Committee chairman Toomas Vitsut declared that the Continental European option was "more cost-effective and more reliable from a security of supply perspective."[38] When asked about whether there was any contradictions, an Estonian official argued that "we've been quite clear all along with Poland and our Baltic partners" about supporting two lines, not one, for the Continental option, while another public servant separately pointed out that the Nordic option was "just a scenario analyzed by the [EU] Joint Research Center, and never an official goal" of the Estonian government.

Lithuania has been unambiguous and quite forceful in its position in favor of one goal – the Continental option – in both private discussions and public statements.

By contrast, Lithuania has been unambiguous and quite forceful in its position in favor of **one** goal – the Continental option – in both private discussions and public statements. In interviews with the author, Lithuanian officials from across the country's governing institutions argued consistently that the Nordic option is worse "from an operational, technical, security, and cost" perspective when compared to the Continental choice for synchronization, underscoring that "the fact we are now approaching the 10-year anniversary of deciding about synchronization options is unacceptable."

Meanwhile, in public, the message is unchanged. For example, foreign minister Linas Linkevičius declared in a meeting with European Commission first vice-president Frans Timmermans that Vilnius is "ready to take on the role of a leader in this matter," adding that existing studies (as reviewed below) "have shown that the most cost-effective and efficient way" of synchronizing is through Poland. This moreover was not the sole occasion on which Lithuania has made its case with EU officials at the highest levels; for instance, Lithuanian President Dalia Grybauskaitė has also reportedly directly lobbied Commission President Jean-Claude Juncker on the importance of choosing the Continental option.[39]

Unfortunately, the same sense of urgency that prevails in Lithuania on synchronization does not yet exist in the other two Baltic states.

[35] "Baltics Agree on Grid Synchronization Via Poland", *The Baltic Times*, May 10, 2017, https://www.baltictimes.com/baltics_agree_on_grid_synchronization_via_poland/ (accessed November 4, 2017).

[36] Ott Ummelas, "Baltics Need Own Grid as Russia Pulls Power Plug, Elering Says", *Bloomberg News*, July 4, 2017, http://www.taaviveskimagi.ee/2017/07/balti-riikide-elektrisus-teemi-sunkroniseerimisest-euroopaga-intervjuu-bloomberg-ile-08-06-2017/ (accessed November 4, 2017).

[37] Taavi Veskimägi, "Varustuskindluse tagab toimiv regionaalne energiaturg" [security of supply is ensured by a functioning regional energy market], presentation at the Elering Security of Supply conference, Tallinn, Estonia, June 6, 2017; Ummelas, "Baltics Need Own Grid".

[38] "Vitsut arutab Balti ja Poola kolleegidega transpordi ja energeetika küsimusi" [Vitsub discusses with the Baltic and Polish colleagues transport and energy issues], Riigikogu, October 1, 2017, accessed November 4, 2017, https://www.riigikogu.ee/pressiteated/euroopa-liidu-asjade-komisjon-et-et/vitsut-arutab-balti-ja-poola-kolleegidega-transpordi-ja-energeetika-kusimusi/.

[39] Aili Vahtla, "Minister: Lithuania Ready to Take Lead in Baltic Power Grid Synchronization", *ERR News*, October 2, 2017, http://news.err.ee/633806/minister-lithuania-ready-to-take-lead-in-baltic-power-grid-synchronization (accessed October 3, 2017).

In part, this disparity is not entirely a new phenomenon.[40] Due in part to the lack of electricity generating capacity in contrast to Estonia (with its oil shale resources) or Latvia (with its hydro power stations) after the EU-mandated closure of the Ignalina nuclear power plant in 2009, Lithuania has made energy security a core institutional priority for the past decade. However, it does not automatically follow that the other two states are ignoring the issue. In Estonia's case, in addition to commissioning the current report in order to facilitate informed decision-making on synchronization options, Elering has proposed strengthening the three countries' ability to function as an electricity island "in order to win some more time" to reach an agreement.[41]

Unfortunately, the same sense of urgency that prevails in Lithuania on synchronization does not yet exist in the other two Baltic states.

1.2 Nordic countries: waiting and seeing?

Although certain key officials in ministries and transmission system operators (TSOs) are following the topic, in general there is relatively little attention to the Baltic synchronization debate in the countries belonging to the Nordic synchronous area (that is, Denmark, Finland, Norway, and Sweden, though only part of the former's territory is part of the area; the Jutland peninsula is synchronized to Continental grid). To the extent that they are concerned at all, the Nordic countries have focused on market and security of supply aspects, with the foreign and security policy dimensions being virtually absent – in large part because, as officials argued in interviews, "the topic simply does not affect us: it's an issue for the Baltic states."

In general there is relatively little attention to the Baltic synchronization debate in the countries belonging to the Nordic synchronous area.

Thus, to the extent that they are concerned at all, the Nordic countries prefer for an agreement to be reached among the Baltic states before committing to – let alone moving ahead with preparations for implementing – the Nordic option. On a political level, some countries prefer not even to *discuss* this option; as the Norwegian Ministry of Petroleum and Energy stated, "given the ongoing process and results within the BEMIP initiative" towards identifying the best conditions for the Continental option, "the ministry prefers not to give an assessment of…the option of synchronizing with the Nordic instead of Continental synchronous areas at this point in time."[42] With varying degrees of cautiousness, Danish, Finnish, and Swedish officials expressed a willingness to offer "support" to whatever choice the Baltic states make – even though all of them pointed out that the Continental option was the most cost-effective one. Former Svenska Kraftnät CEO (and ex-minister of defense) Mikael

To the extent that they are concerned at all, the Nordic countries prefer for an agreement to be reached among the Baltic states before committing to – let alone moving ahead with preparations for implementing – the Nordic option.

[40] For instance, Lithuania established a separate Ministry of Energy in 2008, while by contrast Latvia and Estonia cover energy security issues through relatively small departments within the Ministry of Economics and Ministry of Economic Affairs & Communications respectively. See Giedrius Česnakas, "Energy Security Cooperation in the Baltic States: Lessons for the South Caucasus Region" in J. Novogrockiene and E. Siaulyte, eds., *Addressing Emerging Security Risks for Energy Networks in [the] South Caucasus* (Amsterdam: IOS Press, 2017), 3.

[41] Merike Rebane, "Elering: Baltikumi energiavõrgu autonoomset võimekust tuleks tugevdada" [Elering: The Baltic energy grid's autonomous capacity needs to be strengthened], *Raamatupidamisuudised,* September 20, 2017, http://rup.ee/uudised/majandus-ja-ari/elering-baltikumi-energiav-rgu-autonoomset-v-imekust-tuleks-tugevdada (accessed November 1, 2017).

[42] Ministry of Petroleum and Energy, electronic correspondence with the author, October 20, 2017.

Odenberg summarized the prevailing official view as follows: "we don't want to be an obstacle, and will not offer great opposition" to a final Baltic decision in favor of the Nordic option.[43]

As the next chapter shows, Continental European area countries such as Slovakia and Hungary share similar views: that is, while not greatly affected by or enthusiastic about synchronization, they still express a willingness to support whatever decision the Baltic states reach at the negotiating table. But what *are* the options being considered, exactly?

1.3 What's on the Table: Current Synchronization Options

It is not the purpose of the current report to provide detailed economic and technical analyses of the options for synchronization; such work has already been conducted by the Nordic TSOs and the European Commission's Joint Research Center (which produced a main study in 2016 and a final document, containing recommendations and an executive summary, in June of this year).[44]

The Joint Research Center's final document lists three main options for the Baltic countries after BRELLxit: first, operation as a single area not synchronized with *any* neighboring countries (an option not seen as economically viable or politically desirable, and therefore not considered in this report); second, the Nordic option, which will require the construction of "new alternating current undersea cables between Estonia and Finland," – three, according to the Nordic TSO study and the experts interviewed by the author – and finally, the Continental option, via either the existing LitPol Link 1 doubled overhead line (hereinafter "LPL1"), or via both LitPol Link1 and a second Lithuania-Poland connection, known as LitPol Link 2 (the "LPL2") (see also Annex B).[45]

The current cost projections for the two options under consideration are, as per the JRC's figures, €900 million for LPL1, €770-€960 million for LPL2, and €1.36-€1.41 billion for the Nordic option.

Given the well-established and extremely positive reputation of the Nordic countries the benefits of relying on these states rather than others for the future security of one's critical infrastructure projects seems almost unnecessary to point out.

2. Looking Admiringly Across the Water's Edge: (Geo)political Advantages of the Nordic Option

Given the well-established and extremely positive reputation of the Nordic countries for corruption-free societies and for stable, consensus-based political systems – to the extent that even the creator of the award-winning political drama television series *Borgen* feels compelled to acknowledge that "Danish coalition politics… sounds absurdly boring" – the benefits of relying on these states rather than others for the future security of one's critical infrastructure projects seems almost unnecessary to point out.[46] Moreover, the idea of fostering these ties is not an old one in the Estonian political context.

[43] Mikael Odenberg, former CEO, Svenska Kraftnät, interview with author, Stockholm, Sweden, September 25, 2017

[44] Energinet, Fingrid, Statnett, Svenska Kraftnät, *Impact of Baltic Synchronization on the Nordic Power System Stability* (Sundbyberg, Sweden: Svenska Kraftnät, November 2016), http://www.svk.se/siteassets/om-oss/rapporter/impact-of-baltic-synchronization-on-the-nordic-power-system-stability.pdf (accessed November 5, 2017); Artus Purvins, Ettore F. Bompard, Anna Mutule, et al, *The Baltic Power System between East and West Interconnections: First Results from a Security Analysis and Future Work* (Luxembourg: Publications Office of the European Union and European Commission's Joint Research Center, 2016); Arturs Purvins, Tao Huang, Shaghayegh Zalzar, et al, *Integration of the Baltic States into the EU Electricity System: A Technical and Economic Analysis – Final Report (Executive Summary)* (Luxembourg: Publications Office of the European Union and European Commission's Joint Research Centre, 2017), https://publications.europa.eu/en/publication-detail/-/publication/8d3b7da2-562e-11e7-a5ca-01aa75ed71a1 (accessed November 5, 2017).

[45] Purvins et al, *Integration of the Baltic States*, 3.

[46] The Nordic countries regularly occupy (nearly) all of the top spots in the Transparency International annual corruption rankings. See "Corruption Perceptions Index 2016," Transparency International, January 25, 2017, accessed November 5, 2017, https://www.transparency.org/news/feature/corruption_perceptions_index_2016; Jasper Rees, "Why the World Fell for Borgen", *The Daily Telegraph*, December 13, 2013, http://www.telegraph.co.uk/culture/tvandradio/10491255/Why-the-world-fell-for-Borgen.html (accessed November 5, 2017).

In his famous 1999 speech "Estonia as a Nordic Country," then-foreign minister (and later President) Toomas Hendrik Ilves pointed to similarities in technological innovation, political transparency, and even professional culture in arguing against the conception of Estonia as inherently "post-Communist." Even two decades ago, the UK and Nordics served as the main destination for Estonian exports and leading source of foreign direct investment, which "makes perfect sense – we understand each other, we can do business."[47]

Mutual trust and shared values are quite apparent among Estonia and its northern neighbors both at the strategic and operational levels.

Especially when looking at the electricity sector, Ilves' words ring true 18 years later. Not only have the markets been fully integrated under the Nord Pool Spot market – with trading flows having steadily risen after the completion of the Estlink 1 and 2 asynchronous cables between Finland and Estonia – but mutual trust and shared values are quite apparent among Estonia and its northern neighbors both at the strategic and operational levels. [48]

First, while they sometimes do undertake projects for social reasons (for example to ensure lower prices to consumers in areas far from major population centers), in general the Nordic countries have a much more compatible attitude towards the role of the state in electricity markets than does, for example, Poland, given the latter's policy objective (as explained in more detail in the next chapter) to prioritize its domestic market over international trading. While it is indeed true, as the author has previously argued, that both Estonia and Poland stand out within the European Union as uniquely dependent on fossil fuel usage for generating electricity – and have lobbied to reduce the impact of EU climate policy on their domestic oil shale and coal industries respectively – Estonia remains committed to implementing climate targets in the long term.[49]

Why does this ideological difference matter to synchronization? Essentially, as an Estonian official explained, "since Poland is more protectionist, if there's a sudden price spike it is more likely to curtail exports so as to keep prices lower at home," whereas "we, or the Finns, would be more likely to let things continue," viewing higher prices as an incentive to spur further investment in, for example, energy efficiency.

In addition to shared values about the need for TSOs to be non-political and transparent in their operation – and about the importance of implementing EU regulations – the Nordic countries also have a similar approach to Estonia on the need to invest in, and support the development of, smart-grid technology. First, such smart grids can better handle the challenges associated with greater use of renewable energy sources (which generate power more intermittently than fossil-fuel plants), and thus allow the region to better meet its goal of meeting stronger renewables targets and adapting to a reformed EU Emissions Trading System (ETS) when it is introduced. Second, as Taavi Veskimägi has observed, since Denmark, Norway, and Finland share Estonia's vision of making the region into a global leader in the digitalization of electricity systems, this is one reason why synchronizing with the Nordic countries will create more value than

The Nordic countries also have a similar approach to Estonia on the need to invest in, and support the development of, smart-grid technology.

[47] Toomas Hendrik Ilves, "Estonia As a Nordic Country", speech at the Swedish Institute of International Affairs, December 14, 1999, http://vm.ee/en/news/estonia-nordic-country (accessed October 30, 2017).

[48] See Emmet Tuohy and Kristiina Visnapuu, *Nord Pool Spot and the Baltic Electricity Market: Difficulties and Successes at Achieving Regional Market Integration* (Tallinn: International Centre for Defense and Security, June 2015), https://www.icds.ee/publications/article/nord-pool-spot-and-the-baltic-electricity-market-difficulties-and-successes-at-achieving-regional-m/ (accessed November 8, 2017).

[49] Emmet Tuohy, "Polluter or Partner: Estonian Energy Security & Climate Policy", presentation at the European Climate Policies vs. Energy Security Strategy of Member States: Concerns and Contradictions conference, College of Europe, Warsaw, Poland, January 26, 2015.

synchronizing with Central Europe."[50] However, as the next sections explore in further detail, the extent to which this additional value exists is not perceived the same way by Estonia's Nordic partners across the water.

3. Blocked at the Water's Edge? (Geo) Political Risks of the Nordic Option

Of course, like any society in our current universe, the Nordic countries are far from being political utopias. To take one point in particular – while anti-immigration/Euro-skeptic sentiment is far less salient in Nordic domestic politics than in the Visegrád countries – a factor explored in much more detail in the next chapter – it has still increasingly become relevant in the region. To take just one country, Sweden, as an example, there an anti-immigration party has established itself as the 2nd-most-popular nationwide in polls leading up to next year's parliamentary election; while explanations differ as to the cause of its rise, even in 2015 observers noted that the "party's electoral success prompted hasty political horse trading among other parties intent on keeping extremists as far from the levers of power as possible, which in turn prompted allegations that Sweden's political establishment was subverting the democratic process."[51]

Of course, like any society in our current universe, the Nordic countries are far from being political utopias.

Despite the 2009 Declaration of Solidarity, which expresses the country's willingness to provide (and receive) help in time of crisis, and despite its more recent tentative steps to improve its work with NATO (it signed a host-nation support agreement in 2016), Sweden (along with Finland) is still militarily non-aligned.[52] While the two countries are highly supportive of new efforts to facilitate security cooperation within the European Union, in neither Stockholm nor Helsinki is there much *awareness of*, let alone serious contingency planning for, the possibility that the Baltic states might actually invoke the collective defense clause of the EU's Lisbon Treaty. Finally, it should be noted that even in Sweden, Russian efforts to develop and extend its influence have become the source of growing concerns.[53]

While doubts about political resilience are important, the biggest risk stems from the fact that the Nordic countries simply do not support synchronization enough to invest their own resources in completing it – at least without convincing evidence that it is the only option for the Baltic states, or without proof that it offers unique benefits to their own systems and economies. The latter is not provided by the Nordic TSO study which concludes that the technical benefits to the Nordic area of Baltic synchronization are, at best, minimal.

Moreover, there is considerable geopolitical risk above all from Finland, the country which is most important to the Nordic option; due to the limitations of current technology, it is the only Nordic state to which synchronous connectors can currently be constructed from the Baltic states. In general, Finland still sees energy mostly in economic rather than security terms; while Finland is taking steps to improve the resilience of its *own* grid, and continues to work on countering hybrid threats, the context

[50] Taavi Veskimägi, "EL-i puhta energia paketi kaudu saab Eesti tõusta energiasüsteemide digitaliseerimise globaalseks liidriks" [Through the EU's clean energy package, Estonia can become aglobal leader in the digitization of energy systems], *Eesti Päevaleht* , June 20, 2017, http://epl.delfi.ee/news/arvamus/taavi-veskimagi-el-i-puhta-energia-paketi-kaudu-saab-eesti-tousta-energiasusteemide-digitaliseerimise-globaalseks-liidriks?id=78619782 (accessed November 4, 2017).

[51] "Anti-immigrant Sweden Democrats Move into Second Place in Polls," Reuters, March 23, 2017, https://www.reuters.com/article/us-sweden-politics/anti-immigrant-sweden-democrats-move-into-second-place-in-polls-idUSKBN16U1NS (accessed November 5, 2017); Michael Booth, "Stop the Scandimania: Nordic Nations Aren't the Utopias They're Made Out to Be", The Washington Post, January 16, 2015, https://www.washingtonpost.com/opinions/stop-the-scandimania-nordic-nations-arent-the-utopias-theyre-made-out-to-be/2015/01/16/8f818408-9aa0-11e4-a7ee-526210d665b4_story.html (accessed November 5, 2017).

[52] See Michael H. Clemmesen, "On Baltic Views of the Swedish Declaration of Solidarity," in *Friends in Need: Towards a Swedish Strategy of Solidarity with Her Neighbors* (Stockholm: Royal Swedish Academy of War Sciences, 2012); Charles Duxbury, "Sweden Ratifies NATO Cooperation Agreement", *The Wall Street Journal*, May 25, 2016, https://www.wsj.com/articles/sweden-ratifies-nato-cooperation-agreement-1464195502 (accessed November 20, 2017).

[53] Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case", *Journal of Strategic Studies* 40:6 (October 2017): 773-816.

of its past and ongoing energy and political relationships with its eastern neighbor remain cause for concern.

The Nordic countries simply do not support synchronization enough to invest their own resources without convincing evidence that it is the only option for the Baltic states, or that it offers unique benefits to their own systems and economies.

In the recent *past,* the lengthy battles with (and within) Finland over the location of the EU-supported regional liquefied natural gas (LNG) terminal and Balticconnector pipeline between Estonia and Finland should disabuse observers in the Baltic states of any lingering notions

While Finland is taking steps to improve the resilience of its own grid, and continues to work on countering hybrid threats, the context of its past and ongoing energy and political relationships with its eastern neighbor remain cause for concern.

that Helsinki automatically will be easier to work with than Warsaw as a key partner on a major series of energy infrastructure projects. To take one example from the Balticconnector case, the Finnish state-owned company Gasum – which had "no incentive to change," as the author noted in an interview, due to its profits in trading with Russia – suddenly refused to participate in the project despite years of involvement in the planning process, declaring that it was "not commercially viable."[54] This in turn forced the Finnish government to step in and create a new company to serve as Elering's partner and assure continued EU funding. To this past example should be added the present example of Finland's active cooperation with the Russian state enterprise Rosatom in completing a nuclear power plant at Hahnikivi: when asked about the political implications of this deal, Finnish officials are remarkably complacent, citing the fact that it is a joint venture with a majority-Finnish-owned company (Fennovoima) as evidence for why the project should not raise any security concerns.

3.1 "The End of Regional Cooperation as We Know It"?

After the above-mentioned May prime ministerial meeting in Tallinn, it was perceived at least in Vilnius that *all* energy issues among the Baltic countries had been settled. Not only did Estonian prime minister Jüri Ratas reportedly acknowledge that synchronization would take place via Poland, but "Lithuania offered no opposition" to EU support for the Estonian Paldiski liquefied natural gas (LNG) terminal project – at least before "the political winds shifted," as the Lithuanian academic Giedrius Česnakas argues.[55] Currently, the Paldiski project financing decision remains "on hold until consultations [among] the prime ministers" are completed.[56]

Even if in theory the two issues are not interrelated, it might well be the case in practice that for Estonia to generate more favorable political winds – which unlike actual weather patterns, tend not to be random – it may have to offer a concession on one in order to attain its objectives on the other. If not, it could be "the end of regional cooperation as we know it," as one official anonymously noted; for example, Rail Baltic(a) or even work together on defense matters could be affected – providing fertile ground for the use of "active measures" by the countries' neighbors, as suggested in previous chapter of this report.

If no agreement is reached, in the end, the downside political risk is far from negligible. For instance, the chairman of the Lithuanian parliament's energy committee argued in September that, "given how events are unfolding, it's time for Lithuania to prepare for

[54] Richard Martyn-Hemphill, "Finland, Estonia to Lobby Brussels for Gas Linkup", *The Baltic Times,* October 10, 2017, https://www.baltictimes.com/finland__estonia_to_lobby_brussels_for_gas_linkup/ (accessed November 20, 2017).

[55] Giedrius Česnakas, lecturer, Vytautas Magnus University, interview by author, Vilnius, Lithuania, July 28, 2017.

[56] "Estonia to Likely Support Alexela in Paldiski LNG Terminal Dispute", *The Baltic Times,* August 31, 2017-September 27, 2017, 7.

Plan B" and synchronize with the Continental area by alone, "without tying itself to Latvian and Estonian energy plans."[57] The longer they persist, the greater the likelihood that divisions among the Baltic countries can be exploited by outside powers. Moreover, *if* Estonia decides to insist on the Nordic option, it will have to spend considerable financial and political capital, as well as time, on winning over doubters not only in Vilnius but in the Nordic countries themselves – as the technical difficulties reviewed in the next section suggest.

The longer they persist, the greater the likelihood that divisions among the Baltic countries can be exploited by outside powers.

4. Too Far to the Water's Edge? Economic/Technical Disadvantages and Risks of the Nordic Option

As already noted earlier in this chapter, outright preference for the Nordic option is rare among policymakers even in Estonia, to say nothing of the potential partner countries in either the Nordic or the Baltic regions. This is not simply due to the (geo)political factors outlined above; as both previous studies and our own research findings indicate, there are legitimate drawbacks to the Nordic area *as such,* in addition to the cost and other issues associated with connecting to it.

Outright preference for the Nordic option is rare among policymakers even in Estonia, to say nothing of the potential partner countries in either the Nordic or the Baltic regions.

None of the major studies on the topic – not the JRC report, not the Nordic TSO study, and not even a non-public 2013 report commissioned by the Baltic TSOs from Gothia Power – conclude that this is the most effective option for synchronization.[58] Even the more optimistic Elering Security of Supply Report 2017 noted only that the existing studies indicated that the Nordic option was "possible."[59]

Why? First, for the most common reasons cited: cost and time. By any measure, the undersea cables needed to implement the Nordic option – assumed in the Nordic TSO study to be three 220 kV AC lines with a projected capacity of 250 MVA each – are simply more expensive to construct, and thus make the Nordic option considerably pricier than either version of the Continental option. Moreover, they will also take longer to construct and require more study before they can be implemented.

Second, the three lines cannot be used simultaneously for market trading and synchronization purposes – unlike any of the connections in the Continental scenario. As Jussi Jyrinsalo of Fingrid explained in Tallinn last year, the existing DC Estlink 1 and 2 cables will continue to be utilized as they are now, but for synchronization to take place, the AC lines will be used *only* for "system support, [which is] needed in case of dimensioning faults on either side."[60]

Third, strictly from a technical electricity point of view, the Nordic system is smaller and "less safe" than that of Continental grid. Its frequency quality is weaker (that is, it experiences greater and more significant deviations

[57] Aili Vahtla, "Lithuania Mulling Power System Synchronization without Estonia, Latvia", *ERR News,* September 13, 2017, http://news.err.ee/618274/lithuania-mulling-power-system-synchronization-without-estonia-latvia (accessed November 5, 2017).

[58] See "The Baltic States' Integration to the EU Internal Electricity Market", Elering, accessed November 20, 2017, https://elering.ee/baltic-states-integration-eu-internal-electricity-market.

[59] Elering, *Eesti elektrisüsteemi varustuskindluse aruanne 2017* [Estonian electricity system security of supply report] (Tallinn, 2017): 14.

[60] A dimensioning fault is the largest loss of power generating capacity that a system might face; it is accordingly designed (dimensioned) to withstand it and maintain normal operation. In the event that the Visaginas nuclear power plant is ever constructed in Lithuania, the size of this fault will be seven (!) times larger than at present. See Jussi Jyrinsalo, "Baltic Synchronisation towards Nordics: Is It a Real Alternative?", presentation at Elering Security of Supply Conference, Tallinn, Estonia, June 7, 2016, 6.

above/below the 50Hz target) and, in the words of one Nordic official, it is less stable (that is, it has declined over time) than that of the Continental grid. One Nordic TSO official even warned the author in an interview that Nordic "consumers are used to dealing with frequency instability, but yours may not be," warning that there could be issues as Baltic industries adjust to the greater oscillation and other unpredictability of the Nordic grid. Moreover, this issue is expected to get worse, both for the existing Nordic area members – especially as nuclear power plants in Sweden are decommissioned (with four to go offline in 2020 and others projected to reach the end of their service lifespan in 2040.) Furthermore, as competition strengthens within Nord Pool Spot, as another Nordic official predicts, Baltic generating capacity will be outmoded and taken offline – thereby further weakening even the combined system.

Fourth, Estonia (and the other Baltic states) in this scenario would be connected not to the heart of the Nordic network, but to its weakest point – Finland, which is relatively isolated with only two synchronous connections to the rest of the Nordic area countries, though more are being planned. (On this point it should be noted that the Baltic states would become the weakest part of the Continental area in the same sense, given that only one or two connections are likely to be used to implement that option).

Estonia (and the other Baltic states) in this scenario would be connected not to the heart of the Nordic network, but to its weakest point – Finland.

Fifth, unlike with the Continental grid – to which many countries, most recently Turkey, have successfully synchronized – no state has *ever* before joined the Nordic area; accordingly, as experts noted in interviews with the author, "we don't even know exactly what we will have to do," although revisions to e.g. the Nordic network code and operating practices will likely be included. Finally, even though officials in each of the Nordic capitals stressed the relative ease of reaching agreement among such a small group of countries sharing cultural and political values, even this comparative advantage should not be overstated. For example, a recent dispute between Finland and Denmark on one side and Sweden and Norway on the other – about whether rules for balancing reserves should be set at the national level – entered public view, with the Finnish TSO noting that its counterparts' proposal "seems completely incomprehensible."[61]

Unlike with the Continental grid – to which many countries, most recently Turkey, have successfully synchronized – no state has ever before joined the Nordic area.

Getting Across the Water's Edge: Conclusions

Ultimately, to get across the existing divide among the countries concerned, some compromise will be needed. But what kind?

First, one issue is to consider "LPL1Plus," or another "hybrid" option involving initial synchronization via the existing LitPol Link followed by an additional cable for security of supply purposes. Such a link could run either from Poland to Lithuania or even, as reportedly suggested by Riga, from Latvia to Sweden. While this might ensure quicker agreement among the Baltic states – and might attract EU support, as "another cable to Sweden means more than just more electricity supply" but also political unity, as one former Lithuanian competition authority official put it[62], Sweden's unwillingness to construct another trans-Baltic cable (NordBalt 2) because of the considerable domestic

[61] "The proposal regarding a new balancing model made by the Swedish and the Norwegian transmission system operators conflicts seriously with Finland's national decision-making power and the goals of the European Union", Fingrid, June 9, 2017, accessed November 20, 2017, http://www.fingrid.fi/en/news/announcements/Pages/The-proposal-regarding-a-new-imbalance-settlement-model-conflicts-seriously-with-Finland%E2%80%99s-national-decision-making-power-.aspx.

[62] Former Lithuanian government official, correspondence with author, November 2, 2017.

investments required and weaker economic case given the recent completion (and incomplete utilization) of NordBalt 1 – "we can't be building a new cable every year," as one Swedish figure noted ironically – means, as well as the weaker economic case, that this may not be the most workable compromise in the end.

For now, while the reader might conclude from the information presented in this chapter that it is clearly best for the Baltic states not to cross the water's edge and synchronize instead via Poland, no synchronization option is risk-free – as the next chapter explains in further detail.

Chapter III

The Continental Option: Low-Hanging Fruit or Poisoned Chalice?

Anna Bulakh
Nolan Theisen

In principle, the countries that belong to the Continental synchronous area support the Baltic states' desire for BRELLxit and their joining the Continental grid. After all, some current Continental area member countries have been in a similar situation not long ago; in 1995, the Visegrád countries and in 2004, Bulgaria and Romania completed the task of investing and upgrading their physical networks while updating the procedures and methods of network operation in order to qualify to make the transition from IPS/UPS to the Continental grid.

The process of joining Continental area is well established and will work no differently for the Baltic countries.

In this sense, the process of joining Continental area is well established and will work no differently for the Baltic countries. Once they formally initiate the process within ENTSO-E, the pan-European association of electricity transmission system operators, they then assume the responsibility of meeting the strict standards of the Continental area – a process that is typically expected to take three to five years. In this light, the current target date for Baltic synchronization of 2025 (see previous chapter) is not far off, explaining the growing sense of urgency. However, as with any decision of such magnitude involving so many countries, it is not simply a matter of rhetorical political solidarity; instead, the impact of Baltic membership in Continental area should be evaluated by each country in terms of perceived and actual costs and benefits across multiple dimensions.

This chapter will review the current perspective of five Continental area countries – the Visegrád Four (V4; Czechia, Hungary, Poland, and Slovakia) as well as Germany – on the prospect of Baltic synchronization to the Continental grid in general and the 1- or 2-line options in particular, taking into consideration several factors including political landscape, market integration and trade, regional and energy security, technical capacity, and investment. The question is whether this is a proverbial "low hanging fruit" ripe for being picked up with lesser effort or risk (and at lower cost) than the alternative Nordic option, as some analyses suggest. Or could it, due to various aspects often not directly associated with synchronization, turn into something which contains a significant risk of eventually becoming, for the Baltic states, a poisoned chalice?

1. Potential Advantages

1.1 Geopolitical landscape

As has been previously noted in this report, the Baltic region's current link to Russia represents a potential source of leverage for coercive action by the Kremlin. Moscow is gradually turning Kaliningrad from a liability into an asset. The resulting degree of strategic vulnerability requires the Baltic states to identify and approach allies within the Continental area in order to develop a risk-mitigation strategy based on maintaining political resilience while ensuring security of supply as well as effective functioning of the market.

Even though political perceptions of the Visegrád countries have largely been shaped of late by their move towards questioning not only past governments' more EU-friendly narratives but even the very rationale for deeper European integration, the Continental synchronous area may still be the most effective source of like-minded allies for the Baltic states as they seek to counter potential Russian adverse actions.

While Poland – the country that would serve as the connecting point for synchronization between the Continental area and the Baltic states – has adopted an assertive attitude towards Russia, the other members of the Group – Czechia, Hungary, and Slovakia – have taken a much more neutral stance. As with the Baltics, Poland has demonstrated very strong political will in resisting the Russian challenge by supporting EU sanctions, investing in its own defense capabilities, and pushing for a strong NATO presence on the Alliance's eastern flank (including in the Baltic states).[63] Shared borders with Russia (the Kaliningrad region) and Belarus make Poland an obvious target for Russian aggression, whether military or otherwise. Poland's lead role in the fight against the Nord Stream 2 project – part of Moscow's ongoing campaign to leverage its energy exports to the EU for political purposes – is just one example of how Warsaw's strategic thinking regarding threats in the region is similar to that of the Baltic states.

Poland has demonstrated very strong political will in resisting the Russian challenge by supporting EU sanctions, investing in its own defense capabilities, and pushing for a strong NATO presence on the Alliance's eastern flank.

Poland's assertive stance on Russia and its strong bilateral relations with the United States provide strong incentives for many of the country's neighbors to seek closer cooperation with Warsaw. Earlier, Poland had demonstrated greater commitment to EU integration, striving to assume a more important place in Europe's policy engine (including through such formats as the Weimar Triangle with France and Germany). Today the current Polish government has modified its priorities, putting a Poland-centric agenda front and center – including in regional cooperation. It is advancing a regional format, called the Trimarium or Three Seas Initiative – which promotes Poland's pivotal geopolitical role in the region between the Adriatic, Baltic, and Black Seas and seeks to strengthen connectivity, cooperation, and solidarity across this region.[64] Warsaw seems to appreciate that, despite NATO's prominence and primacy in managing Russia as a military threat, more regional and European unity and solidarity (e.g. in energy, trade, or sanctions policy) is necessary to counter Russian revisionism.

It is equally important to note Germany's political recognition of Russia's challenge to the EU and to the European security order. Berlin's firm position is one of the main pillars in sustaining Europe's response to Kremlin aggression in Ukraine, and Germany has become one of the key contributors to NATO's military deterrence measures and Enhanced Forward Presence by taking the lead of one of the multinational units deployed to the Baltic states. Together with France, Germany has been part of the core engine driving European integration forward – including in political, security, defense, and economic affairs. Successful Franco-German cooperation is obviously one of the key ingredients of the EU's robust external action and is bound to remain such in the future, especially after the exit of the UK from the Union.[65]

Berlin's firm position is one of the main pillars in sustaining Europe's response to Kremlin aggression in Ukraine, and Germany has become one of the key contributors to NATO's military deterrence measures and Enhanced Forward Presence.

[63] Piotr Buras and Adam Barcel, "An Unpredictable Russia: the Impact on Poland", *European Council on Foreign Relations*, July 15, 2016, http://www.ecfr.eu/article/commentary_an_unpredictable_russia_the_impact_on_poland (accessed September 5, 2017)

[64] See Grzegorz Lewicki, "The Three Seas Initiative will strengthen Europe", *Visegrad Insight,* July 3, 2017, http://visegradinsight.eu/the-three-seas-initiative-will-strengthen-europe/ (accessed September 5, 2017).

[65] See Kaitlin Lavinder, "Are France and Germany the last hope for the EU?", *The Cipher Brief,* June 28, 2017, https://www.thecipherbrief.com/are-france-and-germany-the-last-hope-for-the-eu (accessed September 2, 2017); Pierre Briançon and Joshua Posaner, "Angela Merkel and Emmanuel Macron rekindle German-French romance", *Politico,* July 13, 2017, https://www.politico.eu/article/angela-merkel-and-emmanuel-macron-rekindle-german-french-romance/ (accessed September 5, 2017).

1.2 Energy security and market

Synchronization with the Baltics – and the resulting further physical and commercial integration of national electricity markets – is broadly advantageous not just for the Baltic states themselves (which have, understandably, driven the project forward) but for the V4 countries and Germany individually. These states will gain additional frequency reserves and balancing opportunities in the form of new and diverse sources of generation. Certainly, at the same time, the expanded synchronous area opens national systems to new risks and vulnerabilities; these will be examined in the next section. From an economic perspective, open trade under perfect competition allows for the most efficient outcomes that increase net social welfare through price convergence, even though winners and losers emerge across countries and sectors depending on several relative market characteristics. Nonetheless, integration provides overall benefits to (Central) European consumers; frequency-support generating capacity will be shared among a larger population, while electricity will be traded on a more competitive basis – thereby translating into lower prices.

In terms of energy security, the Visegrád countries, Germany, and the Baltic states together have a relatively clear underlying shared interest: synchronization is understood on all sides to represent the further strengthening of cooperation.

In terms of energy security, the Visegrád countries, Germany, and the Baltic states have a relatively clear underlying shared interest: synchronization is understood on all sides to represent the further strengthening of cooperation. However, this understanding is at times only superficial. Officially, Poland supports the European Commission's vision, as reviewed in our study, for eliminating this remaining Baltic energy island. Originally the plan was to have LitPol Link upgraded by 2025, the same target date for supplemental network investments to be made in Northeast Poland whether or not the Continental synchronization option for the Baltic is chosen. However, Poland does not perceive the 2-line option as being in its national interest (see section 2.3 below for more detail).

Germany fully supports the European Commission's drive towards creating a single European energy market. It is thus evident that German market interests are generally contradictory to those of Poland.

Germany, on the other hand, as a proponent of open markets that stands to benefit from greater commercial electricity trading, supports the second line as it will boost trade capacity and market access. In fact, according to the interviewed experts (see Annex A) the issue positively aligns with a political priority for Berlin, since it would help provide new export opportunities that would fuel the growth of its renewable energy sector. This in turn incentivizes the construction of new cross-border infrastructure, solidifying robust direct physical connections to the Nordic grid, its Visegrád neighbors, and, by extension, the Baltics. Germany thereby fully supports the Commission's drive towards creating a single European energy market. It is thus evident that German market interests are generally contradictory to those of Poland; in the specific Baltic synchronization context, these differences are reflected in Berlin's support for the construction of LPL2; while it recognizes that the doubled lines along the LPL1 route would be sufficient for synchronization purposes, the one-line option would restrict available net transfer capacities for trading purposes – something that would not be in Germany's interest.

Outside of Poland – the only V4 country that shares a land border with the Baltic states – the issue of Baltic synchronization is largely perceived as peripheral and inconsequential at least in terms of direct effects on the other V4 states. For Slovakia and Hungary, synchronization is of no apparent importance; it does not register as a political priority, will

not materially affect their networks, and is not perceived to offer any opportunities for national energy companies. While acknowledging in interviews that they have no national interest in the Baltic synchronization decision as such, both Hungarian and Slovak officials explicitly express a willingness to support the process once the Baltic states initiate it within ENTSO-E in order to bring about more energy trading, deeper market integration, and improved security of supply for all parties. Czech officials offer similar views, while also being more interested in potential new market opportunities created by the synchronization and integration processes.

For Slovakia and Hungary, synchronization is of no apparent importance; it does not register as a political priority, will not materially affect their networks, and is not perceived to offer any opportunities for national energy companies.

In principle, members of the Continental synchronous grid will stand to benefit from improved security of supply and market integration from synchronization without themselves incurring any direct network costs. Outside of Poland, a second line to bolster both trade and security of supply is welcomed. The unilateral support of synchronization among Continental area members provides the Baltic states an opportunity to focus specifically on advocating the second link, perhaps leveraging this majority in order to push Warsaw into changing its position.

2. Potential Risks and Disadvantages

2.1 External and Internal Political Resilience

While the synchronization of the Baltic states to the Continental synchronous area provides considerable advantages in joining the largest electricity system of the European Union, it brings with it more than just the market or technical challenges addressed later in this chapter. In addition, political and security dynamics in the region, Russian influence, and differences in national energy policies have the potential to have a negative impact on the synchronization process and its outcomes.

Bilateral relations in the Continental area have some serious weak points through which political cohesion can be disrupted. Poland and Germany are going through yet another rough patch in bilateral relations. Differences in interpreting history, managing their economic relations, handling their approach to Russia in energy, and – most of all – managing the influx of refugees and economic migrants have nearly drained the reservoir of mutual trust and respect between Berlin and Warsaw.[66] Poland's relations with another heavyweight of Europe, France, also became tense with a new administration taking over in Paris and reproaching Warsaw over the issues of democratic values and European solidarity.[67] Meanwhile tensions between Warsaw and Vilnius over perceived mistreatment of the Polish minority population in Lithuania essentially led to the implosion of the close "strategic partnership" forged during the 1990s and to the growth of mutual distrust and disrespect.[68] For both sides, this relationship is a strategic necessity, especially given the

Bilateral relations in the Continental area have some serious weak points through which political cohesion can be disrupted.

[66] See Matthew Karnitschnig and Jan Cienski, "Warsaw's EU spat stalls German-Polish engine", *Politico.eu,* January 14, 2016, https://www.politico.eu/article/warsaws-eu-spat-stalls-german-polish-engine-poland-government-media-law/ (accessed September 2, 2017), and also Adam Balcer and Paweł Zerka, *Hard Love, Actually: Polish-German Relations and a 'Multi-Speed' Europe – a View from Warsaw* (Warsaw: WiseEuropa, 2017), http://wise-europa.eu/wp-content/uploads/2017/03/170323-Hard-Love-actually.pdf (accessed September 5, 2017).

[67] See Tsvetelia Tsolova and Pawel Sobczak, "In stinging attack, France's Macron says Poland isolating itself in Europe", *Reuters,* August 25, 2017, https://www.reuters.com/article/us-france-centraleurope/in-stinging-attack-frances-macron-says-poland-isolating-itself-in-europe-idUSKCN1B5128 (accessed September 2, 2017).

[68] "Dialogue of the deaf between Vilnius and Warsaw", *The Economist,* February 10, 2012, https://www.economist.com/blogs/easternapproaches/2012/02/poland-and-lithuania (accessed September 2, 2017).

grave threat that Russia poses to the common stability of the entire region.[69] Some current tentative steps towards improving bilateral political relations are in their early stages – in February 2018, Polish president paid an official visit to Vilnius for the first time in seven years – but they will not move far and fast enough without sustained political will on both sides to resolve their differences.[70]

Most disconcerting from the perspective of political resilience is the crisis developing in slow motion between the EU authorities in Brussels and the national authorities of several Visegrád countries.

However, most disconcerting from the perspective of political resilience is the crisis developing in slow motion between the EU authorities in Brussels and the national authorities of several Visegrád countries. Baltic desynchronization is emerging as a priority European project at a time of considerable political tensions on the continent. The refugee and migration crisis has created or exacerbated stark divisions within the EU, with challenges to the idea of European solidarity coming particularly from the V4 countries – which have found themselves in often severe and direct confrontations with Germany. Recent political actions taken by Budapest and Warsaw, allegedly in defiance of EU core principles, has given rise to a European political crisis and increased uncertainty about future cohesion of the EU.[71] A set of laws giving Polish politicians control over the country's court system is only one in a series of contentious legal reforms being pursued by the ruling Law and Justice party (PiS) that have widened the divide between Warsaw and Brussels and prompted the latter to invoke Article 7 to initiate procedures regarding potential violation of the EU Treaty.[72]

The Polish government's attempts to interfere with and gain control over institutions that are supposed to remain impartial and/or independent are not confined to judiciary. The trend has also affected Poland's defense sector: A large number of top military officers left their posts in protest over alleged overt political interference by the government into the competencies of the military command.[73] New media legislation, giving the government full powers to appoint and dismiss the management of the public broadcaster, is another example of how the ruling party disregards some of the fundamental principles underpinning liberal democracies – in this instance, independent media and pluralism.[74] The enactment of this law was referred to as "wholly unacceptable in a genuine democracy."[75] The path taken by the ruling party in Poland creates uncertainty about the country as a reliable partner in various EU projects, should its confrontations with Brussels become a highly disruptive and unsustainable "new normal."[76]

Yet despite all the above, Poland is not even the most vigorous promoter of Euroskepticism of all the member states in the Continental area –

[69] See Marius Laurinavičius, "Time for a reset of Polish-Lithuanian relations?", *Europe's Edge,* December 10, 2015 (accessed September 2, 2017).

[70] "Lithuanian PM hails progress in relations with Poland", *The Baltic Course,* August 17, 2017, http://www.baltic-course.com/eng/baltic_states/?doc=132292 (accessed September 5, 2017).

[71] Heather Grabbe and Stefan Lehne, "Defending EU Values in Poland and Hungary", *Carnegie Europe*, September 4, 2017, http://carnegieeurope.eu/2017/09/04/defending-eu-values-in-poland-and-hungary-pub-72988 (accessed September 18, 2017); Andrew Rettman, "Hungary veto sets scene for EU battle on Poland", *EUObserver,* December 21, 2017, https://euobserver.com/justice/140385 (accessed December 21, 2017).

[72] Daniel Boffey, "EU Will Hit Poland with Deadline to Reverse Curbs on Judicial Freedom", *The Guardian*, July 23, 2017, https://www.theguardian.com/world/2017/jul/22/eu-will-hit-poland-with-deadline-to-reverse-curbs-on-judicial-freedom (accessed September 10, 2017).

[73] Matthew Day, "Mass exodus of Polish army's top ranks in protest over political interference from government", *The Telegraph*, February 17, 2017, http://www.telegraph.co.uk/news/2017/02/17/mass-exodus-polish-armys-top-ranks-protest-political-interference/ (accessed September 15, 2017).

[74] Roy Greenslade, "Polish president urged not to sign controversial media law", The Guardian, January 7, 2016, https://www.theguardian.com/media/greenslade/2016/jan/07/polish-president-urged-not-to-sign-controversial-media-law (accessed September 15, 2017); Nate Schenkkan, "PiS uses media control to bring Poland to heel", Emerging Europe, July 19, 2017, http://emerging-europe.com/voices/voices-politics/pis-uses-media-control-to-bring-poland-to-heel/ (accessed September 15, 2017).

[75] Roy Greenslade, "Polish journalists protest at state control of public broadcasting", *The Guardian,* January 11, 2016, https://www.theguardian.com/media/greenslade/2016/jan/11/polish-journalists-protest-at-states-control-of-public-broadcasting (accessed September 15, 2017).

[76] Piotr Buras, "Europe and Its Discontents: Poland's Collision Course with the European Union", *European Council on Foreign Relations*, September 2017, http://www.ecfr.eu/page/-/ECFR230_-_EUROPE_AND_ITS_DISCONTENTS_-_POLANDS_COLLISION_COURSE_WITH_THE_EU_.pdf (accessed September 18, 2017).

that title is arguably best awarded to Hungary. Over more than ten years in power, the ruling Fidesz party has managed to undermine the independence of public institutions and erode civil society to a degree not seen elsewhere in the EU.[77] This has set Budapest on a collision course with Brussels on a number of occasions, with little signs that the government is willing to shift its position on the importance of preserving the integrity of those institutions. Prime Minister Viktor Orbán's government has dismantled constitutional checks and balances and consolidated control over the state-owned media.[78] Moreover, the government's dissemination of xenophobic, anti-immigration propaganda may violate Article 2 of the EU's Lisbon Treaty, which calls for unity based on respect for democracy, equality, non-discrimination, and tolerance.[79] Furthermore, its law restricting foreign funding for NGOs in order to limit the influence of "foreign agents" is strongly reminiscent of the similar legislation enacted by Russia in 2012.[80]

Poland is not even the most vigorous promoter of Euroskepticism of all the member states in the Continental area – that title is arguably best awarded to Hungary.

Consistent efforts by the governments and ruling parties of both countries to subject various public entities and institutions to full political control are justified by the pretexts of fighting corruption and administrative incompetence on the one hand, or undoing politicization by their predecessors on the other. Sometimes this might indeed be the case, but the overall character and impact of such policies sends a worrisome message to Poland's neighbors and strategic partners in the Baltic states, which may be entering yet another mutually dependent partnership – of synchronous electricity systems. While national governments are entirely acting within the scope of their powers to establish strategies for the energy and infrastructure sectors, including TSOs, the "rule book" of ENTSO-E prescribes the full independence of TSOs in managing their operations (including their response to emergencies) free of political and governmental interference.

Polish and Hungarian governments have already demonstrated that they are not afraid of alienating their EU partners or Brussels and enduring some isolation, should their domestic political imperatives and agendas demand it.

Most of the interviewed experts insisted they would find it highly unlikely, even unthinkable, that the Polish or Hungarian governments would ever violate this "rule book," given that they would find themselves completely isolated in the ENTSO-E community and would draw serious sanctions. On the other hand, both the Polish and Hungarian governments have already demonstrated that they are not afraid of alienating their EU partners or Brussels and enduring some isolation, should their domestic political imperatives and agendas demand it. It is plausible, even if not at the moment accepted as probable, that the "unthinkable" might well become a reality, especially under the pressures of a security crisis. Such a development might not necessarily harm the Baltic states: a geopolitically conscious government sensitive to the threats emanating from Russia and cognizant of its modus operandi – such as in

[77] See Norwegian Helsinki Committee, *Full-fledged democracy under attack in Hungary,* September 30, 2013, http://www.osce.org/odihr/106129?download=true (accessed September 15, 2017); Bojan Bugarič, *Protecting Democracy and the Rule of Law in the European Union: The Hungarian Challenge* (London: The London School of Economics and Political Science, 2014), http://www.lse.ac.uk/europeanInstitute/LEQS%20Discussion%20Paper%20Series/LEQSPaper79.pdf (accessed September 15, 2017); Eszter Zalan, "MEPs vote to start democracy probe on Hungary", *EUobserver,* May 17, 2017, https://euobserver.com/political/137943 (accessed September 15, 2017).

[78] Philip Stephens, "Viktor Orban's Hungary Crosses to Europe's Dark Side", *The Financial Times*, July 12, 2017, https://www.ft.com/content/2032f1c2-66e5-11e7-8526-7b38dcaef614 (accessed August 20, 2017).

[79] "The Lisbon Treaty, Article 2", accessed August 21, 2017, http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-1-common-provisions/2-article-2.html.

[80] "Russia: Government vs. Rights Groups, Human Rights Watch", Human Rights Watch, September 8, 2017, accessed September 10, 2017, https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle; Yasmeen Serhan, "Hungary's Anti-Foreign NGO Law", *The Atlantic*, June 13, 2017, https://www.theatlantic.com/news/archive/2017/06/hungarys-anti-foreign-ngo-law/530121/ (accessed August 21, 2017).

present-day Poland – might be able to support emergency management by the TSOs in ways consistent with the geopolitical situation. On the other hand, if such a government is compromised by Russia's influence and/or prioritizes own political, economic or security interests over solidarity with the Baltic states, the outcome could be rather unpleasant for the latter.

As far as the other analyzed countries are concerned, Slovakia is also not immune to anti-EU right-wing, nationalist, and populist forces. Two far-right parties, SNS and LSNS, made it into parliament in the 2016 elections. Yet in contrast to Budapest and Warsaw, Bratislava is still open to building a stronger relationship with Berlin – as is Prague. The wide range of liberal parties in Czechia relative to other countries in the region helps it to maintain a pro-EU and generally pro-Western consensus.[81] However, the fact that the populist Euroskeptic incumbent President Miloš Zeman, who openly propagates pro-Kremlin views, was re-elected for the second term in office attests to the strength of anti-EU and Russia-friendly sentiment in the country.[82] While Germany has been the last stronghold against rising anti-EU rhetoric in the region, its September 2017 elections were also shaped in part by Euroskepticism; after its srong performance at the polls, the nationalist Alternative for Germany (AfD) will now have a considerable voice in federal politics and will be the main opposition party in Bundestag.[83]

The growth in Euroskeptic populist sentiment in the region is significant for Baltic synchronization for two reasons: first, the rise of Euroskepticism might undermine support of EU-funded regional projects in general; and second, as described in the next section, anti-Western, anti-EU parties often either adopt a narrative sympathetic to the Kremlin or align themselves with Russia openly.[84] This can in turn help reshape a country's approach on issues of importance to Russia – including economic relations with the Baltic states, of course – in the Kremlin's favor. Both factors undermine the internal and external political resilience of the region, erode trust and solidarity, and raise questions about states' ability or willingness to act to assist their neighbors in crisis conditions.

First, the rise of Euroskepticism may undermine support of EU-funded regional projects in general; and second, anti-Western, anti-EU parties often either adopt a narrative sympa-thetic to the Kremlin or align themselves with Russia openly.

For the Baltics, the calls for so-called "pragmatic softening" of Russia policy in the region with which the Baltic states plan to synchronize raise questions about the scale of Kremlin influence.

2.2 Russian Influence

For the Baltics, the calls for so-called "pragmatic softening" of Russia policy in the region with which the Baltic states plan to synchronize raise questions about the scale of Kremlin influence. Clearly, the rise of populism is beneficial to the Kremlin's strategic goal of fragmenting and weakening the EU; moreover, if the mutual interests of Visegrád and German political and business leaders are forged by a degree of interdependence with Russia, the Baltics

[81] Benjamin Cunningham, "5 Takeaways from Slovakia's Elections", *Politico*, June 3, 2016, http://www.politico.eu/article/slovakia-fico-asylum-migrants-elections-nazi-nationalists/ (accessed July 25, 2017); Benjamin Cunningham, "Visegrád's Illusory Union", *Politico*, September 6, 2016, http://www.politico.eu/article/poland-hungary-czech-republic-slovakia-Visegrads-illusory-union-bratislava-summit-eu-migration-orban-fico-sobotka-szydlo/ (accessed July 25, 2017).

[82] Veronika Špalková and Jakub Janda, *Activities of Czech President Miloš Zemanas the Kremlin's Trojan Horse* (Prague: European Values, 2018), http://www.europeanvalues.net/wp-content/uploads/2018/01/Activities-of-Czech-President-Milo%C5%A1-Zeman.pdf (accessed January 29, 2018).

[83] Anne Applebaum, "Germany's Election Gives the Country a Reality Check", *The Washington Post*, September 27, 2017, https://www.washingtonpost.com/news/global-opinions/wp/2017/09/24/germanys-election-gives-the-country-a-reality-check/?utm_term=.d6b0bbac00cd (accessed October 5, 2017).

[84] Marcin Zaborowski, "Poland's inward turn", *Visegrad Insight*, January 8, 2018, http://visegradinsight.eu/polands-inward-turn/ (accessed January 8, 2017); Gustav Gressel, *Fellow Travellers: Russia, Anti-Westernism, and Europe's Political Parties* (London: European Council for Foreign Relations, July 2017), http://www.ecfr.eu/page/-/ECFR225_-_FELLOW_TRAVELLERS1.pdf (accessed October 5, 2017).

could be left as a political island of resistance to the Kremlin. As stated above, far right and Euroskeptic rhetoric in these (and other) EU member states aligns in most cases with pro-Russian sentiment. This is not a coincidence; in each election, the Kremlin strives to bring a sympathetic group of *Putinverstehers* ("Putin Whisperers" or literally "Those Who Understand Putin") to power.[85]

The growing Euroskeptic and far-right movements in the Visegrád countries and Germany open the door for greater Russian influence.

As the Baltic states pursue BRELLxit, the growing Euroskeptic and far-right movements in the Visegrád countries and Germany open the door for greater Russian influence, whether by supporting these political forces rhetorically, or by developing closer ties with these movements' leaders or sympathizers in the political establishment. According to reports, the AfD leadership has developed direct contacts with powerful figures in Moscow; the party's top leaders have traveled to meet with United Russia (Putin's political party) on several occasions.[86] Not coincidentally, it received exceptionally positive coverage by Russian media outlets during the election campaign, securing about a third of the party's support from Russian speaking voters. It is significant that the Russian-speaking minority in Germany – part of the Kremlin's "Russian world" – now has a sympathetic party in the German parliament, and with it the ability to influence mainstream policies. And even though Angela Merkel secured a fourth term in office, her Christian Democratic Union (CDU) and its Bavarian sister party fell short of an outright majority; accordingly, it must now form a new coalition that might bring more *Putinverstehers* into her administration, figures who lobby for a closer relationship with Russia by promising to "manage" Putin as they secure greater profits for German business.[87]

It is significant that the Russian-speaking minority in Germany—part of the Kremlin's "Russian world"—now has a sympathetic party in the German parliament.

The national security risk posed by pro-Kremlin radicals and political sympathizers in Slovakia is among the highest in the region. The relations between Slovak and Russian extremist groups go beyond simply spreading anti-EU/NATO narratives to include active organizational cooperation – including paramilitary training – with Russian officials and fellow extremists.[88] Meanwhile, in Hungary, the second-largest (and most anti-EU) party in parliament – Jobbik – allegedly receives financial support from Russia and together with Orbán's ruling Fidesz party, actively channels Russian interests.[89] The winner of the Czech parliamentary elections, billionaire and media mogul Andrej Babiš, the leader of the antiestablishment party Action of Dissatisfied Citizens (ANO, or "Yes," in its Czech abbreviation), is not only openly critical of the EU and NATO but has also been accused

The national security risk posed by pro-Kremlin radicals and political sympathizers in Slovakia is among the highest in the region.

[85] Lóránt Győri, Péter Krekó, Jakub Janda, and Bernhard Weidinger, *Does Russia interfere in Czech, Austrian and Hungarian elections?* (Budapest: Political Capital, 2017), http://www.politicalcapital.hu/pc-admin/source/documents/western_experiences_eastern_vulnerabilities_20171012.pdf (accessed October 24, 2017).

[86] Simon Shuster, "How Russian Voters Fuelled the Rise of Germany's Far-Right", *Time*, September 25, 2017, http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/ (accessed October 24, 2017).

[87] Cornell Overfield, "Built to Last: Coalition Formation and German-Russian Relations after the Election", *Foreign Policy Research Institute*, October 2, 2017, https://www.fpri.org/article/2017/10/built-last-coalition-formation-german-russian-relations-election/ (accessed October 8, 2017).

[88] Grigorij Mesežnikov and Radovan Bránik, *Hatred, Violence, and Comprehensive Military Training: The Violent Radicalisation and Kremlin Connections of Slovak Paramilitary, Extremist, and neo-Nazi groups* (Budapest: Political Capital, 2017), http://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_country_study_SK_20170428.pdf (accessed July 25, 2017).

[89] Dániel Hegedűs, *The Kremlin's Influence in Hungary: Are Russian Vested Interests Wearing Hungarian National Colors?*, Berlin: DGAP, 2016, https://dgap.org/en/article/getFullPDF/27609 (accessed June 12, 2017).

of links to Russia.[90] As finance minister, Babiš had underwritten a record-breaking loan to a Russian company, owned by a close friend of Putin, at a time when Western countries have imposed sanctions.[91] In Poland, however, "the options for direct Russian political influence are limited, and the Kremlin mainly employs soft power due to the fact that the Polish government, political establishment, and societal attitudes are firmly unfavorable towards the Kremlin."[92] Russia's tools of political influence in Poland seem to be confined to the fringe groups rather than affecting the mainstream parties, or the current government.

Neither Hungary's Orbán nor Slovakia's Fico have tried to conceal either their deep economic ties with or favorable approaches toward Russia.

Neither Hungary's Orbán nor Slovakia's Fico have tried to conceal either their deep economic ties with or favorable approaches toward Russia. Both countries rely on Russian nuclear fuel as well as gas and oil supplies while openly questioning sanctions against Moscow.[93] Hungary has significantly increased its dependency on Moscow after reaching three key business deals: on the Paks Nuclear Power Plant with Rosatom, on gas supplies with MET, and on modernization of subway cars for Line 3 of the Budapest Metro. These agreements were reached at a detrimental cost to the state budget, and allegedly involve high-level political corruption linked to Russia.[94]

Slovakia depends heavily on Russian oil, gas, and nuclear fuel as well as energy technology in order both to operate and modernize its existing plants and plan future ones.[95] Its national budget relies extensively on revenue from transit fees for Russian gas, thereby helping to shape the ambiguous position of its left-wing government towards Russia. Czechia almost agreed to Russia's bid to construct the planned Temelín nuclear power plant, though the tender was later canceled due to a lack of transparency.[96] While EU countries have gradually been diversifying away from Russian gas, Moscow has been able to maintain an energy foothold through nuclear energy. Rosatom has won many fuel supply tenders in Central and Eastern Europe in the last 10 years; overall, nuclear power accounts for 27% of the EU's electricity generation, with 131 plants operational in 16 countries.[97]

Ironically, it is Germany that supports the growth of Russian gas dominance in European market. Berlin's silence towards the concerns about Nord Stream 2 raised by its EU allies will benefit neither Germany nor regional energy security. What is particularly striking is the very deep penetration of German energy and political circles by those with close ties to Russia. Russia has recruited senior German politicians like former chancellor Gerhard Schröder, who took a position as chairman of the board of the Nord Stream pipeline project. The Eastern Committee of the German Federation of Industry is the main lobbying

What is particularly striking is the very deep penetration of German energy and political circles by those with close ties to Russia.

[90] "Politico Server: Babiš is Most Powerful Man in Czech Republic", *Prague Daily Monitor*, October 30, 2015, http://www.praguemonitor.com/2015/10/30/politico-server-babiš-most-powerful-man-czech-republic (accessed August 29, 2017).

[91] Gabriel Meyer, "Putin Hiding Under a Czech Candle", *Daily Caller*, January 12, 2015, http://dailycaller.com/2015/12/01/putin-hiding-under-a-czech-candle (accessed August 20, 2017)

[92] Lukasz Wenerski and Michal Kacewicz, *Russian Soft Power in Poland: The Kremlin and pro-Russian organisations* (Budapest: Political Capital, 2017), 9, http://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_country_study_PL_20170428.pdf (accessed August 26, 2017).

[93] "EU Should Drop Russia Sanctions, Slovak PM Says after Meeting Putin", Reuters, August 26, 2016, http://www.reuters.com/article/us-ukraine-crisis-slovakia/eu-should-drop-russia-sanctions-slovak-pm-says-after-meeting-putin-idUSKCN1111A1 (accessed August 26, 2017)

[94] Hegedűs ,"The Kremlin's Influence in Hungary",

[95] Jakub Groszkowski, "Prime Minister Fico's Russian card", *OSW*, July 2015, https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-07-01/prime-minister-ficos-russian-card (accessed August 25, 2017).

[96] Christian Kvorning Lassen, "Russian Liaisons with the Czech Republic", *Charter 97*, May 16, 2016, https://charter97.org/en/news/2016/5/16/204504/ (accessed August 26, 2017).

[97] Kenneth Rapoza, "How Washington Is Fighting For Russia's Old Europe Energy Market", *Forbes*, May 2016, https://www.forbes.com/sites/kenrapoza/2016/05/17/washingtons-european-energy-security-boondoggle (accessed July 30, 2017); "Nuclear Power in the European Union", World Nuclear Association, accessed September 10, 2017, http://www.world-nuclear.org/information-library/country-profiles/others/european-union.aspx.

organization for pro-Russian business interests as well as for German companies operating in Russia. A number of Russia-Germany forums, e.g., the Petersburger Dialogue (funded mostly by the German foreign ministry) and the German-Russian Forum (financed mainly by the business community), were created to transfer Western values eastwards to post-Soviet Russia; however, today, they may well work the other way around. Established platforms for Russia-Germany engagement provide Russia with access to Germany's business and political decision-makers that can later be exploited to dampen "enthusiasm" in Berlin for synchronization with the Baltic states.

The region has become a major playground for Russia's influence operations.

The region has become a major playground for Russia's influence operations. By supporting far-right movements and developing closer business ties with political and business leaders, the Kremlin has been able to penetrate the decision making of EU member states themselves. This level of influence can assist Russia in shaping negotiations on synchronization. Both Euroskeptic populist movements and pervasive Russian influence in the Continental area create a risk that, at some point, the Baltic states will find themselves in the situation of critical dependency on countries with compromised political systems that are unable or unwilling to co-operate in a security crisis engineered by Moscow. Thus, the question is ultimately whether the Visegrád group and Germany, given these above factors, can be sufficiently resilient internally and externally in order to deal with overt and covert interference – including with the synchronization process.

2.3 Energy Markets: National(ist) Challenges

While questions about resilience in the face of external political influence and increased Euroskepticism create uncertainty for the Baltics in potential confrontations with Russia, the same trends affect the decisions made on the technical, financial, environmental, and security side of synchronization – and thus, the resilience of energy markets. A complex political environment – one also shaped by protectionist Polish energy policy – might leave national interests above regional solidarity. The issue of the second synchronization interconnector with the Baltic states (see Chapter II) is a case in point. Poland has pledged to undertake the necessary technical measures from its side to ensure synchronization, though (as explained in the previous chapter) it will reportedly not consider anything beyond the one-line option – in part because these additional options will expand trading capacity. Warsaw does not seek to open its energy market, and instead protects its coal and lignite generating capacity from cheaper foreign imports. In fact, Poland wants to increase the utilization of its coal assets, and the construction of a second line facilitating commercial flows is inconsistent with its energy strategy.

A complex political environment – one also shaped by protectionist Polish energy policy – might leave national interests above regional solidarity.

Warsaw does not seek to open its energy market, and instead protects its coal and lignite generating capacity from cheaper foreign imports.

Meanwhile Germany's national gas and electricity policies adversely impact its Visegrád (and, albeit to a far lesser degree, its Baltic) neighbors and cannot be entirely separated from negotiations over synchronization. The ongoing saga surrounding Nord Stream 2 is a well-documented case in point, while loop flows caused by Germany's *Energiewende* (transition towards a low-carbon energy system), more specifically as result of insufficient domestic transmission capacity to deliver renewable energy supplies from north to south, have been a constant source of frustration for Poland and Czechia. The unscheduled flows through those countries between German regions limit the net transfer capacity available for their commercial operations and have caused

serious disruptions, notably in the summer of 2015, when the load factor overwhelmed Poland's system.

The short-term solution is a coordi-nated phase shifting transformer (PST) investment project between the German and Polish TSOs, Hertz50 and PSE; the project envisions the installation of four PSTs by 2020, thereby assuring some measure of control over these sporadic cross border power flows. The first PST – located at the Mikulowa substation – began operation in the summer of 2016.

Accordingly, the nature of Polish and German energy markets and policies will present additional complexity to the synchronization negotiations, whether directly or indirectly. Poland remains firmly opposed to any second line that exposes its electricity market, while it perceives that Germany is profiting at its expense due to the ongoing loop flow issues that affect the trading Berlin continues to advocate. While they may be about technical issues, these are political positions and ultimately affect the future political partnerships among the countries concerned; accordingly, the importance of political trust should not be neglected.

The nature of Polish and German energy markets and policies will present additional complexity to the synchronization negotiations, whether directly or indirectly.

Conclusion

Given the complexity of the economic, political, security, and technical factors affecting their synchronization decision, that Baltic states do need to recognize that while they gain strategic advantages by choosing to synchronize with the Continental area, they also face some serious risks as a result. Certainly, choosing the Continental option means joining a synchronous area as large as the one the Baltic states are leaving, thereby ensuring security of supply. The Continental area is also more coherent, as few members are not part of both the EU and NATO (and the ones that are not, for instance, NATO members – like Austria or Switzerland – are much further "upstream" from the Baltics' link to the Continental grid.)

The Continental area includes states that have the stamina (such as Poland) and resources (Germany) to stand up to Russia's coercive and destabilizing strategies.

Moreover, the Continental area includes states that have the stamina (such as Poland) and resources (Germany) to stand up to Russia's coercive and destabilizing strategies. Poland in particular is a strong supporter of Baltic synchronization as a geopolitical imperative to reduce its exposure to Russia. The area also contains two countries – Germany and France – that are key drivers of closer European integration and whose cooperation with each other and with European institutions still (for better or for worse) underpins so much of the common action taken by the EU. The importance of this tandem will be ever more salient in the field of European security and defense in the coming years, as CSDP begins to fulfill its potential. Last, but not least, this is the area where the greatest potential for energy market integration lies.

Choosing the Continental synchronous area also carries with it a degree of exposure to internal political uncertainty and risks associated with the political developments in this area, which may eventually spread to the geopolitical realm and undermine political solidarity between the countries. As

Choosing the Continental synchronous area also carries with it a degree of exposure to internal political uncertainty and risks associated with the political developments in this area, which may eventually spread to the geopolitical realm and undermine political solidarity between the countries.

demonstrated in this chapter, the growth of Euroskeptic movements in the Continental area undermines resilience to existing and potential Russian influence operations as well as to coercive action the Kremlin might choose to undertake. The Euroskeptic populists align themselves, in many cases, with Russian foreign policy interests, increasing the political risks to the synchronization process in particular and to regional security in general. The area also contains a collection of some of the most fraught bilateral political relations (the Poland-Germany and Poland-Lithuania relationships being of notably critical importance to the Baltics) as well as some of the most Euroskeptic national governments with a penchant for removing checks and balances in governance and undermining the independence and political impartiality of public institutions. As for the economic cohesion and resilience of the area, Poland's ongoing "battle" against free and integrated electricity markets and clean energy does not serve as a great source of optimism for the future.

The disadvantages discussed in this chapter may not necessarily spill over into the synchronization relationship: at present, day to day functioning of the Continental area shows that broader political and geopolitical turbulence so far has not disrupted its successful management. Even while exhibiting political changes causing dismay among many other European partners, the behavior of neither Budapest nor Warsaw has cast doubt on the strength of their commitments to collective defense within NATO framework. Poland's strong stance vis-à-vis Russia and ability to view energy issues in a geopolitical context are particularly noteworthy. Many of the disadvantages described here may well prove to be temporary, applicable to the broader context only in the short or medium term; accordingly, they could largely disappear in ten years or so.

The Continental option seems to represent easy low-hanging fruit for Baltic synchronization. However, if internal political and economic resilience dynamics do not improve—even deteriorate—this option may well prove to be a poisoned chalice.

However, the longevity of the present political regime of "illiberal democracy" in Hungary is indicative of how entrenched such political forces can become over time. Tensions and fissures created by their ideologies and actions are already threatening to have an existential impact on the EU as such. As Steven Erlanger and Marc Santora put it, "The growing conflict between the original Western member states of the bloc and the newer members in Central and Eastern Europe is the main threat to the cohesion and survival of the European Union. It is not a simple clash, but a multibannered one of identity, history, values, religion and interpretations of democracy and 'solidarity.'"[98] Also, we are already observing how considerations flowing from a protectionist energy policy agenda can determine how many synchronous links may be built between the Baltic states and the rest of the Continental grid. The operation of this grid – especially of its members close to the Baltic states – has not yet been tested by a severe security crisis engineered by Russia.

The longevity of the present political regime of "illiberal democracy" in Hungary is indicative of how entrenched such political forces can become over time. Tensions and fissures created by their ideologies and actions are already threatening to have an existential impact on the EU as such.

In the end, the Baltic states should not only aim to make the most *cost-effective* choice for synchronization, but also the most sustainable and strategically viable one. The latter means that in addition to system stability and security of supply, the synchronization option will also have

[98] Steven Erlanger and Marc Santora, "Poland's nationalism threatens Europe's values, and cohesion," *The New York Times,* February 20, 2018, https://www.nytimes.com/2018/02/20/world/europe/poland-european-union.html (accessed February 21, 2018).

to rely on an internally and externally resilient political and energy market environment that can guarantee effective regional and European cooperation in the event of security-related crises. In many regards, the Continental option seems to represent easy low-hanging fruit for Baltic synchronization. However, if internal political and economic resilience dynamics do not improve – or worse, deteriorate – this option may well prove to be a poisoned chalice, forcing some very sharp dilemmas on the Baltic states in the future: such as between speaking up about the threats to political values that bind NATO and the EU together, or staying silent out of immediate security considerations.

Chapter IV

Hanging by a Thread? Physical Security of Synchronization Links

Julia Vainio
Artūras Petkus
Tomas Jermalavičius

One critical dimension that should be considered is the potential kinetic threats to the lines that will synchronize the Baltic countries to their chosen area. This chapter analyzes the possible physical threats to each synchronization option – and the capabilities by the relevant players to manage these threats, including by means of multilateral responses.

One critical dimension that should be considered is the potential kinetic threats to the lines that will synchronize the Baltic countries to their chosen area.

Beginning with a description of both existing and needed interconnector infrastructure, the chapter reviews vulnerabilities and resilience of this infrastructure before then discussing the current – and required – response capabilities and frameworks. The chapter then closes with some conclusions on the preferable synchronization option from a physical security perspective.

1. Infrastructure

As outlined earlier in this report, the Baltic states are synchronized with the IPS/UPS power system on the basis of the BRELL agreement with Russia and Belarus – meaning that their grid frequency and frequency containment reserves (FCRs) are both currently maintained from Moscow.[99] Four 300-330 kV overhead power lines connect Estonia and Latvia to mainland Russia; two similar lines connect Lithuania to Kaliningrad. There are also four 300-330 kV overhead lines and one 750 kV overhead line connecting Lithuania to Belarus.[100]

In addition to its synchronous connections with UPS, the Baltic states also have asynchronous interconnections with both the Nordic and the Continental grids. These include three HVDC (High-Voltage Direct Current) submarine links to the Nordic power system and one HVAC (High-Voltage Alternating Current) overhead line to the Continental grid (see Annex B). The former cannot be used for synchronization, which is based on the frequency of alternating current within the grid and therefore requires HVAC lines to achieve. Therefore, synchronization with the Nordic area would, as noted in Chapter II, require three additional submarine HVAC cables to be built between Estonia and Finland – the only possible such connection, as current technology does not enable the construction of HVAC cables long enough to connect the Baltic states and Sweden.

Of the three HVDC links to the Nordic system, two connect Estonia and Finland: Estlink-1, a 350-megawatt (MW) cable 105 km in length connecting the Harku and Espoo converter stations in Estonia and Finland respectively, and the 650 MW, 175-km-long Estlink-2 between the stations at Püssi (Estonia) and Anttila (Finland).[101] Both are jointly owned by Elering and Fingrid. The third – one of the longest HVDC submarine cables in the world – is the 700 MW NordBalt line between Lithuania and Sweden; when its land part of the cables is included, the total length of the system is 450 km. The converter stations are located in Klaipėda, Lithuania, and Nybro, Sweden.

[99] Frequency containment reserves (FCR) are electricity production assets used to maintain the frequency within a given system; gas turbines and coal plants are some examples of FCRs used for emergencies (i.e. in the event a power plant or interconnector unexpectedly goes offline), as they can quickly increase or decrease production as needed.

[100] See "ENTSO-E Map", ENTSO-E, accessed June 23, 2017, https://www.entsoe.eu/map/Pages/default.aspx. The 750 kV LT-BY overhead line is rarely utilized.

[101] Converter stations are facilities that transform AC into DC or vice versa.

Each submarine cable laid is unique in its design. They usually consist of several different parts, such as copper conductors, insulation, and armor beddings. Construction techniques vary according to manufacturer and seabed conditions. The cables are usually laid one to two meters below the seabed, though there are exceptions – such as with NordBalt. Due to the stony bedrock on the Swedish coast, during the laying period this cable was covered with over 65,000 tons of rubble and gravel to protect it from damage by ships.[102] In general, cables are adequately protected by the seabed itself – at least according to prevailing practice; there are thus no safety nets or other similar additional protective measures. An iron cage or safety net might also prove counterproductive and damage the cable if itself moved by an external object such as an anchor.

Both Estlink-1 and NordBalt cables have a so-called "black start" capability, in which the converters for each cable on the Baltic side can work to start up parts of its network after a total blackout.

In general, submarine power cables can be up to 300 millimeters in diameter. Depending on the structure of the power cable, connecting joints are located a few kilometers apart on land, while for the undersea sections the average distance between joints varies between 30-50 km and can even reach 100 km. Both Estlink-1 and NordBalt cables have a so-called "black start" capability, in which the converters for each cable on the Baltic side can work to start up parts of its network after a total blackout.[103] In the Estonian case, this feature can be used to provide supportive power to selected generating facilities, thereby enabling them to resume total or at least partial production within minutes.[104]

However, there are some reservations over how well this feature could be utilized in a crisis.[105]

If the Baltic states choose the Nordic option, as explored in Chapter II, at least three new cables would be needed between Finland and Estonia. More specifically, as proposed in the main JCR report, these could take the form of two 220 kV power cables from Loviisa (Finland) to Püssi as well as one 220 kV cable from Espoo to Harku.[106] So far, the general objective for the asynchronous connections from other EU countries to the Baltic states has been to provide trading capacity. However, once the Baltic states synchronize with another synchronous area, they will not only operate their systems on that region's frequency, but also apply its common rules – such as how to divide power reserves and how to regulate voltage. For example, as of now, Fingrid and Elering have no contractual agreements on providing each other with reserve capacity via Estlink 1 and 2.

Once the Baltic states synchronize with another synchronous area, they will not only operate their systems on that region's frequency, but also apply its common rules – such as how to divide power reserves and how to regulate voltage.

In addition to the three undersea cables mentioned above, there is one further asynchronous interconnection between the Baltic states and the rest of the EU: the 163-km-long HVAC overhead line LitPol Link between – Alytus, Lithuania and Ełk, Poland. The height of the line is on average 60 meters above ground level; however, in forested sections, towers are 100 meters high to avoid the need for tree cutting.[107] The current capacity of the

[102] Communications Department of Litgrid, interview, Vilnius, June 13, 2017.

[103] "ABB NordBalt", ABB, accessed June 28, 2017, http://new.abb.com/systems/hvdc/references/nordbalt.

[104] L. Ronström, M. L. Hoffstein, R. Pajo, and M. Lahtinen, "The Estlink HVDC Light Transmission System", presented at "Security and Reliability of Electric Power Systems", CIGRÉ Regional Meeting, Tallinn, Estonia, June 18-20, 2007, https://library.e.abb.com/public/c9f4e1c6068fb-993c125731d004612b2/Estlink%20HVDC%20Light%20transmission%20system.pdf (accessed June 28, 2017).

[105] Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[106] Arturs Purvins et al, The Baltic Power System Between East and West Interconnections: First Results from a Security Analysis and Future Work (Luxembourg: European Union Joint Research Centre, 2016), doi: 10.2790/411653, 23-26, http://publications.jrc.ec.europa.eu/repository/bitstream/JRC100528/reqno_jrc100528_pdf.pdf (accessed July 2, 2017).

[107] "Summary," LitPol Link, accessed July 2, 2017, http://www.litpol-link.com/about-the-project/summary.

link is 500 MW, set to be raised to 1000 MW by 2020.[108] Since it connects countries in different synchronous areas, the interconnection requires an HVDC back-to-back converter, which enables both market flow electricity as well as emergency reserves to be transferred in both directions.

Unlike the HVDC submarine cables, as noted in previous chapters, the existing LitPol Link line can indeed be used to synchronize the two areas. The European Network of Transmission System Operators for Electricity (ENTSO-E) plans to conduct a dynamic study to determine whether synchronization via only one interconnection would be sufficient to guarantee resilience and to ensure the provision of the necessary emergency reserves.[109] As Heiki Jakson argued in an interview for this report, LitPol Link interconnection capacity can be increased to at least 2000 MW; this could be solved via two additional 500 MW connections between Lithuania and Poland.[110] Technically, in the event that the Continental option is chosen, the then-redundant converter could be utilized, with small modifications, on the Belarusian or Russian borders; however, this is of course dependent on the political decision to continue power trading with those countries after BRELLxit.[111]

ENTSO-E requires each region to perform tests in which, before synchronizing with other grids, they demonstrate the ability to manage as an isolated synchronous area for a short period of time.

ENTSO-E requires each region to perform tests in which, before synchronizing with other grids, they demonstrate the ability to manage as an isolated synchronous area for a short period of time. Such tests would also be required of the Baltic states before their synchronization to either grid. The experiments normally take place over a few weeks both in winter and summer seasons.[112] The Baltic states are preparing for their next isolated operation test, which has been recommended for summer of 2019.[113] However, the Baltic states have been able to operate in an isolated mode for brief periods even before the construction of interconnections outside the BRELL area.[114] In fact, the Estonian electricity system underwent this type of isolated mode testing several times between 1995 and 2009.[115]

2. Vulnerabilities and Resilience

Disturbances to the electricity grids are not only related to malicious or systemic threats. According to ENTSO-E data, there were over 1,800 grid disturbances in the Nordic (including Iceland) and Baltic countries in 2015, which is about average for any given year.[116] In most cases the disturbances were caused by either natural forces or by accidents. Most frequent were breakdowns or defects in technical equipment such as substations or overhead lines. There were a few cases of third-party action, such as in the case of the biggest disturbance to take place in Lithuania in 2015, when a tree was cut down, tripping a transmission line and resulting in the temporary disconnection of five substations. This one incident alone caused more than one-third of the total lost electricity

[108] "Electricity Link LitPol Link", Ministry of Energy of the Republic of Lithuania, accessed July 2, 2017, https://enmin.lrv.lt/en/strategic-projects/electricity-sector/electricity-link-litpol-link.

[109] Experts from the Ministry of Foreign Affairs of Lithuania, interview, Vilnius, June 13, 2017.

[110] Heiki Jakson, former NATO expert on critical energy infrastructure, interview, Helsinki, August 16, 2017.

[111] Experts from the Ministry of Foreign Affairs of Lithuania, interview, Vilnius, June 13, 2017; Communications Department of Litgrid, interview, Vilnius, June 13, 2017.

[112] Arūnas Molis and Justinas Juozaitis, "Baltic Plug Into [the] European Electricity Network: Perspectives of Success", *Humanities and Social Sciences Latvia* 25:1 (Spring-Summer 2017), 34, https://www.lu.lv/fileadmin/user_upload/lu_portal/apgads/PDF/Humanities_and_social_sciences_2017_1__internetam.pdf (accessed July 12, 2017).

[113] "Isolated Operation Study: The Isolated Operation of the Baltic States", Elering, accessed July 5, 2017, https://elering.ee/en/isolated-operation-study-isolated-operation-baltic-states.

[114] Heiki Jakson, interview.

[115] These tests were conducted in 1995, 1997, 2001, 2006 and 2009. See Elering, *Eesti elektrisüsteemi varustuskindluse aruanne 2017* [Estonian electricity system security report] (Tallinn, 2017), 22, https://elering.ee/sites/default/files/public/Elering_VKA_2017.pdf (accessed September 30, 2017).

[116] "Disturbances" are further defined as "outages, forced or unintended disconnections, or failed reconnections because of faults in the power grid. See Fingrid, *Nordel's Guidelines for the Classification of Grid Disturbances*, August 2009, http://www.fingrid.fi/fi/voimajarjestelma/voimajarjestelmaliitteet/S%C3%A4hk%C3%B6n%20toimitusvarmuus/2015/Nordel_Guidelines_Classification_Grid_Disturbances_2009.pdf (accessed July 2, 2017).

in Lithuania that year.[117] Furthermore, the HVDC interconnections between Finland and Estonia have also suffered some disturbances. In 2015, for instance, 11 minor incidents affected Estlink-1, while four occurred with Estlink-2 – one of which lasted for some 18 days.[118] Since its inauguration, problems with outages have also affected NordBalt.[119] These facts underscore the importance of redundancy to ensuring the overall resilience of a power grid. If the one-line Continental option is chosen for synchronization, dependence on one interconnection increases the risk that the Baltic states would have to frequently resort to "island mode," i.e., isolated asynchronous operation, to cope with disturbances, which would inflict higher economic costs on the three countries. The likelihood of those higher costs would be reduced with a second interconnector. In a similar vein, a resilience approach based on redundancy requires three or more submarine lines for the Nordic option.

In case of physical disruption of the interconnectors, the ability of local generating capacity to meet demand not only on a primary or secondary reserve basis, but also on a tertiary reserve basis is critical to preventing the effects of a disruption from being more severe than originally imagined.[120] The need for generation adequacy is also recognized by the TSOs in the region: according to Litgrid, primary reserves would have to reach 2000 MW by 2025 for the Baltic states to operate in isolated mode.[121] This is an unrealistic amount of primary reserves for the region to maintain, while the required amount to operate in synchronous mode (with either the Nordic or Continental areas) would be considerably smaller.[122]

Physical attacks on the synchronizing interconnectors might occur in multiple ways:

- Transmission substations could be hit by kinetic strikes delivered by, for instance, long-range artillery, aircraft or, more stealthily, by Unmanned Aerial Vehicles (UAVs) laden with explosives;[123]
- Substations could also be destroyed by saboteurs planting explosives inside;
- Transmission towers could be taken down either by surreptitiously-placed explosives, or by explosives delivered by UAVs;
- Submarine cables could be cut or damaged using a range of means – from ships' anchors (bringing the benefit of greater plausible deniability) to explosives planted with the help of unmanned undersea vehicles (UUVs).

Some modes of physical attack could be conducted with clandestine approaches, masking either the intent or perpetrator (or both). Accordingly, it is of paramount importance to ensure effective surveillance and control of the maritime environment (both surface and subsurface) in the case of submarine cables, as well as of land borders, coastlines, territories, and airspace adjacent to critical infrastructure, in the case of overhead lines.

It is of paramount importance to ensure effective surveillance and control of the maritime environment (both surface and subsurface) in the case of submarine cables, as well as of land borders, coastlines, territories, and airspace adjacent to critical infrastructure, in the case of overhead lines.

[117] ENTSO-E, *Nordic and Baltic Grid Disturbance Statistics 2015* (Brussels, 2016), 11-12, https://www.entsoe.eu/Documents/SOC%20documents/Nordic/HVAC2015_2016_12_01.pdf (accessed August 20, 2017).

[118] ENTSO-E, *Nordic and Baltic HVDC Utilitisation and Unavailability Statistics 2014* (Brussels, 2015), https://www.entsoe.eu/Documents/Publications/SOC/Nordic/HVDC_Report_DISTAC_2015_10_27.pdf (accessed August 20, 2017).

[119] "Lithuania-Sweden Power Link Offline Again Due to Cable Fault", *The Baltic Course*, February 14, 2017, http://www.baltic-course.com/eng/energy/?doc=127621 (accessed 20 August 2017).

[120] Primary frequency containment reserves must be operational within 30 seconds; secondary reserves, within 15 minutes, and tertiary reserves, within 12 hours.

[121] Daivis Virbickas, "Baltic Generation Adequacy 2017–2032," Litgrid, presentation, June 1, 2017, http://www.litgrid.eu/uploads/files/dir377/dir18/17_0.php, (accessed June 20, 2017); Experts in the Ministry of Foreign Affairs, Lithuania, 13.6.2017.

[122] Communications Department of Litgrid, interview, Vilnius, June 13, 2017.

[123] The Lithuanian Armed Forces have been authorized to shoot down such UAVs, however. "Lithuanian Military Allowed to Shoot Down Unwanted Drones", *Delfi*, September 13, 2017, https://en.delfi.lt/lithuania/defence/lithuanian-military-allowed-to-shoot-down-unwanted-drones.d?id=75744453 (accessed September 21, 2017).

In recent years, the strategic importance of submarine cables has become a securitized issue. So far, the presence of Russian naval ships near international fiber optic cables has caused Western countries to suspect Russia has been preparing to damage these cables purposefully in the event of escalating geopolitical confrontation or outright war.[124] Sabotage to submarine cables can also be conducted without clear evidence of military involvement. A trade, fishing, or research vessel equipped with the necessary means such as UUVs on board – or even just anchors long enough to sever the cables – could in all likelihood remain above a submarine cable for enough time to inflict damage without prompting suspicion, let alone a response from the cable's owners or from authorities responsible for critical infrastructure protection.

The threat does not end with damage to the cables; there is also a risk of interference with repair efforts as well. A partial precedent exists already. During the laying of the NordBalt cable inside Lithuania's exclusive economic zone (EEZ) in March-April 2015, Lithuanian authorities reported three incidents in which Russian warships sought to disrupt the laying of the cable by ordering all civilian vessels to change course and abandon the area. The interference was ostensibly justified by naval exercises of the Russian Baltic Sea Fleet taking place in the approximate location at the time. However, the incidents accentuated political tensions in the region, as Lithuania responded by sending its own warship to the area.[125] Even though the Russian commands to civilian vessels were later deemed to have been executed according to international norms, these orders can at best be seen as existing within a "gray zone" of international law – one that can be exploited against ships deployed to identify and repair future damage to the cables as well.

The approximate – but not exact – locations of interconnector cables are usually displayed on nautical charts to help prevent any disturbances to the connections. According to an expert working on international security and defense issues, there is a widespread consensus that Russia knows the exact routes of the submarine cables connecting the Baltic states to Finland and Sweden.[126] The interviewed experts did concur universally that the risk of a malicious attack is low at present.[127] However, Russia's demonstrated modus operandi in this domain highlights the significant vulnerability of submarine cable infrastructure to asymmetric action by a hostile actor.[128] Should Moscow's strategic goals (see Chapter I) at some particular future point favor such action, this vulnerability could be exploited by Russia.

There is a widespread consensus that Russia knows the exact routes of the submarine cables connecting the Baltic states to Finland and Sweden.

Submarine power cables have another drawback relative to overhead power lines in one other area of resilience: speed of recovery. If a cable is disabled, it might take anywhere from a month to four months or more to put it back in operation.

Submarine power cables have another drawback relative to overhead power lines in one other area of resilience: speed of recovery. If a cable is disabled, it might take anywhere from a month to four months or more to

[124] "Russia a 'risk' to undersea cables, defence chief warns", *BBC News,* December 15, 2017, http://www.bbc.com/news/uk-42362500 (accessed December 15, 2017).

[125] Andrew Higgins, "Increasingly Frequent Call on Baltic Sea: 'The Russian Navy is Back' ", *The New York Times,* June 10, 2015, https://www.nytimes.com/2015/06/11/world/europe/intrusions-in-baltic-sea-show-a-russia-challenging-the-west.html (accessed August 10, 2017).

[126] Jussi Voutilainen, CDR/Finnish Navy, former Defense Attaché of Finland to Estonia, Latvia and Lithuania, interview, Tallinn, June 16, 2017.

[127] Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017; Jussi Voutilainen, interview.

[128] On submarine cables as an attractive target in a hybrid warfare campaign, see Martin Murphy, Frank G. Hoffman, and Gary Schaub Jr., *Hybrid Maritime Warfare and the Baltic Sea Region* (Copenhagen: Centre for Military Studies, 2016), 15-17, http://cms.polsci.ku.dk/publikationer/hybrid-maritim-krigsfoerelse/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf (accessed August 1, 2017).

put it back in operation.[129] There are several reasons for this disparity. First, there are only a limited number of cable repair ships available in the world; they are not in the Baltic region on standby in case of an accident or attack. Second, given their less accessible location, it is simply harder to identify the exact location of any problem with undersea cables than with overhead lines. Third, rough seas or adverse weather conditions – especially given the often-harsh winters in the region – can delay repairs further or even prevent them entirely during a given season. Fourth, since as mentioned above, each submarine cable has its own unique design, there is a limited amount of spare lengths of cable or other spare parts available to fit that design; they are generally set aside for pre-planned repairs.[130] For strategic reasons, the spare parts for NordBalt, for example, are stored in Sweden.[131] These aspects make the interconnectors vulnerable to exploitation of the aforementioned legal "gray zone" at sea – for instance, to obstruct and impede the movement of inspection/repair vessels in international waters – thereby extending repair timeframes even further.

Looking at the Continental option, a particular concern is that the synchronization line(s) would run through the so-called Suwałki Gap.

Submarine interconnectors also have cable lines on the ground that connect them to the converter stations on each side. Even though the converter stations and the overhead wires are protected by modern surveillance equipment, including camera surveillance systems and monitoring through SCADA systems, they are still subject to attack – and an accurate and debilitating strike on a converter station or HVAC substation on land would inflict larger damage than a direct kinetic strike on submarine cables. By disabling a substation, one would be able to potentially disrupt the flow of electricity to two or more regions normally connected by it. Such an attack could inflict maximum damage if conducted during periods of peak consumption, when the interconnectors are utilized to their maximum capacity.[132]

Looking at the Continental option, a particular concern is that the synchronization line(s) would run through the so-called Suwałki Gap – an area of land, less than 100 km wide, on the border of Poland and Lithuania between Russia (Kaliningrad) and Belarus. It is the only land connection between the Baltic states and the rest of the EU; if it were seized militarily, then traffic between the Baltics and the rest of Europe – including perhaps the electricity flows as well – would be severed.

Despite the JRC study conclusions holding that it might be possible to synchronize even with just one overhead line, there is pressure from Estonia and Latvia for another line to be built from Lithuania to Poland. If the other proposed line were built offshore, as suggested by some interviewees, it would have to cross Russian territorial waters or at least the Russian EEZ (not to mention that this might be technologically impossible due to the cable length; see Annex B). While it is legally possible to lay submarine cables in the Russian EEZ, this would require not only Russian permission – which is unlikely to materialize – but also raises questions about the wisdom of having vitally important submarine cables run through the EEZ and territorial waters of a geopolitical adversary. If such a line were built on land through the Suwałki Gap, it would only enhance the resilience of the Baltic electricity system under circumstances short of war.[133] In case of an act of war (i.e. a direct military attack cutting off the Baltic states by seizing the Gap), the number of interconnectors would not matter, as they could all be severed. However, another overhead line would provide for more resilience (in terms of redundancy) for synchronization in peacetime and in crisis situations short of war, while also providing increased commercial trading capacity in the region.

In terms of Russia's measures short of war (hybrid warfare or non-linear techniques), the

[129] Communications Department of Litgrid, interview, Vilnius, June 13, 2017; Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[130] Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[131] Communications Department of Litgrid, interview, Vilnius, June 13, 2017.

[132] Senior expert on power system planning, Fingrid, interview, Helsinki, June 15, 2017.

[133] Miguel Simões, OF-3/PAO, and Andrew Camp, OF-4/ J2X CI/ HUMINT, NATO Force Integration Unit Lithuania, interview, Vilnius, August 31, 2017.

Suwałki Gap still poses certain challenges. First, since it lies in close proximity to international borders with Russia and Belarus, its infrastructure is within relatively easy reach of clandestine activities from the territories of those countries (e.g. cross-border infiltrations by special forces, use of medium range UAVs or low-flying helicopters, etc.). Given the difficulties in detecting and tracking low-flying UAVs, for instance, this poses as serious challenge to the national authorities in charge of critical energy infrastructure protection (CEIP). Second, since both Poland and Lithuania are members of the passport-free Schengen Area, their mutual border in the Suwałki Gap is an internal EU border; consequently, it is a lower surveillance priority for national border guard services, and per the Schengen Agreement, border guard/customs services are generally only allowed to make spot checks – not regular controls – of people or goods crossing the frontier, with temporary exceptions possible during e.g. major international summits. Accordingly, this freedom of movement within the Schengen area makes it possible to prepare and conduct a physical attack against synchronization infrastructure without even having to cross a fully monitored international boundary in the vicinity of the Suwałki Gap; Russia has existing intelligence, organized crime, and other networks already established – and cultivated by its security services – within the Schengen Area. Last, but not least, the presence of a Belarusian ethnic minority near the Suwałki Gap in northeast Poland provides a plausible – albeit currently not very likely – avenue for hostile action against the interconnectors and substations under the pretext and cover of a "disaffected popular revolt", which is part of Moscow's hybrid war repertoire (see Chapter I).

Another overhead line would provide for more resilience (in terms of redundancy) for synchronization in peacetime and in crisis situations short of war, while also providing increased commercial trading capacity in the region.

Russia has existing intelligence, organized crime, and other networks already established – and cultivated by its security services – within the Schengen Area.

To a varying degree, however, these concerns could also be extended and applied to the overland part of submarine links between Estonia and Finland. For instance, overhead lines and substations linking the proposed submarine HVAC lines to the Baltic grid in North-East Estonia and South-East Finland would be rather close to Russia's border (as well as to the extensive Estonian and Finnish coastline which can be penetrated by seaborne special forces); on the Estonian side, it would lie in the area with a high Russian-speaking population. Furthermore, thanks to the membership of both Estonia and Finland in the Schengen Area, they would be exposed to the similar risks associated with the freedom of movement inside this area as just outlined regarding the Suwałki Gap. Thus, submarine interconnectors, in addition to the threats and physical protection issues associated with the unique maritime domain as outlined in this section, are *also* subject to the same vulnerabilities as land-based infrastructure, thereby effectively multiplying the range of measures required to respond to them. Analyzing such responses – whether those currently possible or those planned for the future – is the subject of this chapter's next section.

Submarine interconnectors, in addition to the threats and physical protection issues associated with the unique maritime domain, are also subject to the same vulnerabilities as land-based infrastructure, thereby effectively multiplying the range of measures required to respond to them.

3. Responses

Addressing vulnerabilities, managing risks, and responding to various threats to critical infrastructure, as well as managing consequences of failure and restoring the functioning of this infrastructure, is usually the responsibility of its owners. Governments often establish a framework for risk and threat assessment (e.g. by imposing legal obligation on private sector providers of vital services to prepare an assessment methodology, etc.) as well as capabilities that are owned and operated by state authorities. At the same time, governments perform national level threat assessments that eventually drive their own planning, prioritization, and resource allocation to deal with risks and threats to specific parts of national critical infrastructure. If synchronizing interconnectors are not included as a top priority in the future national assessments and plans of the countries concerned – Finland and Estonia at one end or Poland and Lithuania at another – then the availability of government-owned and government-operated surveillance and protection capabilities may be inadequate or absent altogether.

If synchronizing interconnectors are not included as a top priority in the future national assessments and plans of the countries concerned then the availability of government-owned and government-operated surveillance and protection capabilities may be inadequate or absent altogether.

In the maritime domain, international legal norms – such as the freedom to lay, maintain, and repair cables even outside a country's 12 nautical mile (22km) territorial limit – generally do protect submarine power connections. There are also obligations to impose criminal and civil penalties if the cables are intentionally harmed. International cables are also given special status for telecommunications, power, or military uses.[134] These legal norms specifically imply that in a possible malicious attack scenario, the relevant parties are entitled to defend their power cables even by physical means. However, this is contingent upon their capability and determination to do so.

The Baltic Sea has high volume of maritime traffic, which makes the surveillance and control of the surface area above the submarine lines harder, especially in international waters.

The Baltic Sea has high volume of maritime traffic, which makes the surveillance and control of the surface area above the submarine cables harder, especially in international waters. Maritime security in the Baltic Sea in general has long been identified as one of the areas requiring more investment in national and regional capabilities as well as more cooperation. A unified and coherent maritime security management system with situational awareness data and intelligence fully and freely shared among different civilian and military agencies – both within and among nations – is still an aspiration rather than a reality, despite regional cooperation initiatives such as SUCBAS (Sea Surveillance Cooperation Baltic Sea).[135] Sub-surface situational awareness is deemed to be adequate in Finland and Sweden, but lacking in the Baltic states – including in Estonia where maritime surveillance capabilities and interagency cooperation in this field are clearly insufficient.[136] Also, often information generated by the military sources is classified at the national level and not shared with other littoral states – even security partners.[137] There is a joint project by Latvia and Lithuania to improve Maritime Situational Awareness (MSA), but it is currently

[134] Jennifer Snyder and Neil Rondorf, "About Submarine Power Cables", International Cable Protection Committee, November 2011, https://www.iscpc.org/documents/?id=1755 (accessed August 2, 2017).

[135] Experts of the Estonian Defense Forces, interview, August 28, 2017.

[136] See Jaan Murumets, *Eesti Merejulgeolek: Uuringu raport* [Estonia's Maritime Security: Research Report] (Tartu: Estonian National Defense College, 2015), http://www.ksk.edu.ee/wp-content/uploads/2016/12/ossasional_5_avalik_veeb.pdf (accessed November 13, 2017).

[137] Jussi Voutilainen, interview.

in the very early stages. Estonia plans to join this effort, as its MSA capabilities have been identified as a critical shortfall in national defense planning process; however, it will require a new government-level impetus for increasing and combining civil security and military resources and will take at least another five to ten years to produce some tangible results.[138]

The naval capabilities of Estonia and Finland to protect synchronizing submarine cables or respond to suspicious activity possibly directed at submarine infrastructure are relatively low.

The naval capabilities of Estonia and Finland to protect synchronizing submarine cables or respond to suspicious activity possibly directed at submarine infrastructure are relatively low. Estonia's navy consists of only three mine countermeasure vessels (and due to personnel shortages as well as routine repairs, these cannot all be deployed simultaneously), thereby placing the onus of any potential military response in international waters on Finland. Finnish naval forces include two coastal brigades, eight patrol gunships with guided missiles, two offshore mine layers, four inshore mine layers, and three mine countermeasure vessels.[139] Finland is also renewing its fleet in the coming decade, and is ordering four new corvette vessels. These need to be able to defend against threats from surface ships, aircraft, and submarines while also being able to lay mines.[140] In recent years, Finland and Sweden have also increased their joint response capability. Annual joint naval exercises between the countries are held with the aim of establishing a Swedish-Finnish Naval Task Group (SFNTG) by 2023. As a bilateral tool, the SFNTG will be used for different levels of crisis prevention and management in maritime environments with a focus on military approach.[141]

There are no concrete plans to expand Estonian naval capabilities within the next ten years, as development priorities are focused on the land forces.[142] Indeed, the nation is at risk of losing even its existing small naval capability once the existing platforms reach the end of their service lifetimes.[143] Estonia and the other two Baltic states are almost fully reliant, in military terms, on NATO's maritime capabilities in the event of a military crisis. However, the Alliance has its own capability gaps in this domain, and its peacetime presence in the Baltic Sea is quite cursory.[144] A continuous NATO's peacetime maritime presence in the Gulf of Finland is unlikely at the moment. Even if the new emphasis on countering the Russia threat in the Baltic Sea leads to an increased NATO presence in the Gulf of Finland, peacetime rules

Estonia and the other two Baltic states are almost fully reliant, in military terms, on NATO's maritime capabilities in the event of a military crisis.

[138] Seminar (under the Chatham House Rule) on Estonia's National Defence Action Plan 2018-2022, February 20, 2018, ICDS, Tallinn.

[139] The Latvian navy has one mine layer refitted as a command ship, five minehunters, five patrol boats, and a support ship; Lithuania has one mine layer refitted as a command ship and three minehunters as well as five patrol and one support ship; the Swedish navy consists of seven corvettes, two corvettes refitted as patrol boats, six submarines, and ten minehunters. Source: International Institute for Strategic Studies, *The Military Balance 2016* (Abigdon: Taylor & Francis, 2016), 115, 116, 144.

[140] Jarmo Huhtanen, "Suomi tilaamassa neljä uutta sotalaivaa 1,2 miljardilla eurolla – Tutkimusapua taistelualuksiin saatu USA:sta" [Finland to spend over €1.2 billion on four new ships to its fleet – the US has provided research help for combat ships], *Helsingin Sanomat*, October 4, 2016, http://www.hs.fi/kotimaa/art-2000002923944.html (accessed August 15, 2017).

[141] Government of Sweden, *Final reports on deepened defence cooperation between Finland and Sweden*, 3-4, http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/final-reports-on-deepened-defence-cooperation-between-finland-och-sweden.pdf (accessed August 20, 2017).

[142] See Riigikantselei [State Chancellery], *Riigikaitse arengukava 2017-2026* [National Defense Development Plan 2017-2026] (Tallinn, 2017), https://riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf (accessed November 12, 2017).

[143] Experts of the Estonian Defense Forces, interview, August 28, 2017.

[144] See Bryan McGrath, "NATO at Sea: Trends in Allied Naval Power", *National Security Outlook* No 3 (Washington DC: American Enterprise Institute for Public Policy Research, 2013), http://www.aei.org/wp-content/uploads/2013/09/-national-security-outlook-no3-september-2013_1420494099.pdf (accessed 20 October 2017); Kalev Stoicescu and Henrik Praks, *Strengthening the Strategic Balance in the Baltic Sea Area* (Tallinn: International Centre for Defense and Security, 2015), https://www.icds.ee/fileadmin/media/icds.ee/failid/Kalev_Stoicescu__Henrik_Praks_-_Strengthening_the_Strategic_Balance_in_the_Baltic_Sea_Area.pdf (accessed 20 October 2017).

of engagement might not permit action against civilian ships suspected of sabotaging submarine infrastructure in international waters.

It is important to note that until a declared state of emergency, protection of critical infrastructure at sea is the responsibility of civilian agencies – border/coast guard and police forces.

It is important to note that until a declared state of emergency, protection of critical infrastructure at sea is the responsibility of civilian agencies – border/coast guard and police forces. Armed forces are deployed only in the case of a crisis, in support of and upon the request of the civilian authorities, or in wartime. Regarding the planned synchronizing submarine cables between Estonia and Finland, any required new infrastructure and the capability to survey actions around them would be the responsibility of border guard and their maritime and airborne components. In 2016, the Finnish border guard had four patrol ships and 13 helicopters to cover a 1,250-km coastline (excluding islands), with tasks including responding to violations of territorial waters, countering smuggling, etc.[145] Estonia does not publicly provide information on its border control maritime capabilities. These are presumed to be very small and focused on tasks directed against illegal trafficking and violation of territorial waters, not on protection of critical infrastructure in its EEZ.[146] The civilian authorities of both countries would be over-stretched and would struggle to maintain a persistent presence/ generate a quick response to suspicious activities and security incidents related to submarine interconnectors in their EEZs.

In the land domain, both Finland and Estonia take the issue of hybrid threats seriously and have been adjusting their legal frameworks, integrated civil-military response capabilities, and practices to be able to mount effective counter-measures to security violations and hostile activities on their territories. For instance, stricter security policy measures have been implemented in Finland, whereby the presence of unidentified paramilitaries has been outlawed; the appearance of such forces is now deemed to warrant immediate security action by the state.[147] Estonia has been holding regular interagency exercises to test its plans and preparedness to respond to "little green men" incidents and threats to critical infrastructure and vital services. Both countries continue to strengthen the security of their (and the EU's) land borders with Russia: for instance, Estonia is constructing a high-tech security fence on its side of the border with Russia in the south-east of the country.[148]

At the other end, in the direction of the Continental area, there is rather extensive border infrastructure on the Russian and Belarusian borders with Lithuania and Poland in the vicinity of the Suwałki Gap. Neither of the two countries provides publicly available information on their border control capabilities. However, Lithuania's capabilities mainly focus on guarding the border and enforcing regulations against illegal migration or smuggling as well as conducting search and rescue activities. Protection of critical infrastructure is not mentioned at least in the open-source description of the border guard service's tasks and functions.[149]

Even though border controls are not able to stop all illegal border activity – including even UAV overflights used by smuggling networks – Lithuanian authorities are still relatively well-equipped and have good situational awareness.[150] Lithuania has also announced plans to build a 130-km long fence on its border with Russia's Kaliningrad exclave, stretching from Vištytis to the Nemunas (Neman) River. The main stated reasons for this is the increased deterrence factor of the physical boundary

[145] "The Border Guard in figures", The Finnish Border Guard, accessed September 4, 2017, https://www.raja.fi/facts/the_border_guard_in_figures.

[146] Police and Border guard operate three SAR helicopters and a few small fixed-wing patrol aircraft. Experts of the Estonian Defense Forces, interview, August 28, 2017.

[147] "New Finnish law prohibiting unidentified militia comes into force", *YLE*, July 15, 2017, https://yle.fi/uutiset/osasto/news/new_finnish_law_prohibiting_unidentified_militia_comes_into_force/9725169 (accessed August 20, 2017)

[148] Andrew Retmann, "Security fears prompt fences on EU-Russia Border", *EUobserver,* August 28, 2015, https://euobserver.com/justice/130037 (accessed October 20, 2017).

[149] State Border Guard Service at the Ministry of the Interior of the Republic of Lithuania, accessed August 22, 2017, http://www.pasienis.lt/index.php?1713774498

[150] Miguel Simões and Andrew Camp, interview.

as well as the additional ability to protect the region from the infiltration of "little green men." Lithuania's State Border Guard Service has set up six stations in its Lazdijai District (in the vicinity of the Suwałki Gap) of which one is reserved for "special tasks."[151] Poland has also recognized the need to increase its presence on the border with Russia by announcing a plan to build watchtowers along its border with the Kaliningrad exclave.[152]

For further preparedness, a Lithuanian national rapid reaction force, comprising units of the Lithuanian Armed Forces and internal security agencies, was set up to respond to "little green men" incidents within hours anywhere in the country's territory.[153] According to new legislation, the affected areas can be declared a military operations zone and sealed off to unauthorized persons. Poland is also investing some €800 million in a territorial defense force projected to comprise 53,000 volunteers by 2019. The mission of this force is to counter possible hybrid threats to the country; however, units' priority deployment is in the eastern regions of Poland bordering Belarus, not to the north or north-east.[154]

Unlike the maritime domain—which is partially comprised of EEZs outside territorial waters—land is sovereign national territory on which national authorities can use their full legal powers.

In general, it can be as difficult to protect against threats on land as at sea. However, unlike the maritime domain – which is partially comprised of EEZs outside territorial waters – land is sovereign national territory on which national authorities can use their full legal powers to enhance surveillance, to stop, inspect, and detain suspect individuals or vehicles, seal off entire areas, etc. Capabilities as well as the organizational and legal frameworks to conduct such actions are largely already in place, and can be quickly augmented by mobilizing reserves; moreover, these capabilities are cheaper to generate and maintain than their maritime equivalents, whether civilian or military. Investments in strengthening land borders and territorial security (including national airspace), in light of ambitions to enhance management of EU external borders as well as hybrid threats emanating from Russia, are bound to continue – with sensitive areas such as the Suwałki Gap receiving additional attention given increased awareness of their strategic importance.

Freedom of movement in the Schengen area requires especially intensive and close intelligence cooperation among security and police agencies in member countries in order to detect and intercept plots against CEI.

However, freedom of movement in the Schengen area requires especially intensive and close intelligence cooperation among security and police agencies in member countries in order to detect and intercept plots against CEI before actual acts of sabotage take place. The record of such cooperation – in counter-terrorism and intelligence sharing, for instance – so far leaves much to be desired, as with the current state of maritime surveillance and information exchange in the Baltic Sea.[155]

How much can we then presume that political and military alliances are able to provide deterrence or response measures against possible physical attacks towards the synchronizing interconnector(s)? Looking at the the four possible synchronizing partner states, Estonia, Lithuania and Poland are members of NATO, while Finland – despite

[151] State Border Guard Service.

[152] "Lithuania Plans Fence on Russian Kaliningrad Border", *BBC News*, January 17, 2017, http://www.bbc.com/news/world-europe-38635737 (accessed August 20, 2017)

[153] Rick Lyman, "Ukraine Crisis in Mind, Lithuania establishes a Rapid Reaction Force", *The New York Times*, December 19, 2014, https://www.nytimes.com/2014/12/20/world/europe/lithuania-assembles-a-force-as-it-readies-for-whatever-russia-may-bring.html (accessed August 10, 2017).

[154] "Poland to Build Territorial Defense Force by 2019", *Deutsche Welle,* November 14, 2016, http://p.dw.com/p/2SffY (accessed August 10, 2017).

[155] Maïa De La Baume and Giulia Paravicini, "Europe's intelligence 'black hole'", *Politico*, March 12, 2015, https://www.politico.eu/article/europes-intelligence-black-hole-europol-fbi-cia-paris-counter-terrorism/ (accessed August 20, 2017); Gordon Corera, "Why intelligence sharing still has a long way to go", *BBC News,* January 1, 2016, http://www.bbc.com/news/world-europe-35154640 (accessed August 20, 2017).

increasingly close cooperation – has decided to remain outside the Alliance. According to some experts, a direct one-time physical attack on a single interconnector (or even two) would hardly justify triggering Article 5 of the North Atlantic Treaty (the collective defense clause).[156] However, the affected countries may request security consultations under Article 4 of the Treaty. These consultations may lead to various security assistance measures such as the deployment of the Very High Readiness Joint Task Force (VJTF) to the Suwałki Gap area, or of Standing NATO Maritime Group One (SNMG-1) to the Gulf of Finland. Those forces could provide a more robust deterrent against further escalation of attacks on CEI or against direct use of overt military measures on the territory (or in the territorial waters) of the relevant countries – excluding, of course, Finland.

However, before Article 4 consultations – which are reserved for extraordinary crisis circumstances and which moreover require unanimous consensus among all 29 Allies to begin – the assessing and countering of threats to critical energy infrastructure, as with hybrid threats in general, remains an internal issue and national responsibility of the affected country.

Such solidarity measures as providing additional capabilities or common responses could take place within a European Union framework.

This puts an even larger emphasis on each nation's individual capabilities, readiness, legal framework, and order of priorities to protect such infrastructure – as well as the strength of its ties with countries that could provide assistance on a bilateral basis to fill critical capability gaps.

Such solidarity measures as providing additional capabilities or common responses could take place within a European Union framework as well; as recent political developments within the EU show, it soon may be headed in the direction of establishing a more robust common defense and security framework.[157] In their Joint Communication on countering hybrid threats, the European Parliament and the European Council cited the protection of energy networks as one of the main means of building resilience against hybrid threats.[158] Given that the Treaty of the EU (TEU) contains a mutual security assistance clause (Article 42(7)) and that the Treaty on the Functioning of the EU (TFEU) has a solidarity clause (Article 222), there is indeed some potential for closer cooperation in building and operating common capabilities and providing crisis response within EU structures – whether among EU Member States themselves or in cooperation with/under the auspices of the European Commission. However, the relevant TEU/TFEU mechanisms remain largely untested in practice; national capitals do not conduct any planning for their application under various scenarios; common approaches to civilian and military capability building are still in their infancy, and traditionally "non-aligned" countries such as Finland insist on respecting their special status in implementing mutual solidarity and security clauses. With much uncertainty and complexity in this regard, national responsibility for critical cross-border infrastructure protection will remain unchanged for the foreseeable future.

Conclusions

This chapter has examined the physical threats to the synchronization interconnectors – submarine and overland – and the means as well as ways of ensuring their protection from deliberate acts of sabotage or against the efforts to recover their functioning after accidental disruptions.

Both the submarine and overland infrastructure required to synchronize the Baltic states with either the Nordic or Continental grids is vulnerable to deliberate physical attacks as well as unintended physical disruptions; and these vulnerabilities could be exploited to advance Russia's strategic goals, as discussed in Chapter I of this report. As submarine cables are unique in their design, there is a limited amount of spare parts compared to

[156] Veli-Pekka Tynkkynen, Professor in Russian energy policy, University of Helsinki, interview, Helsinki, June 22, 2017.

[157] Veli-Peka Tynkkynen, interview.

[158] European Commission, *Joint Framework on Countering Hybrid Threats: a European Union response*, JOIN (2016)18 final (Brussels, 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018 (accessed November 1, 2017).

overhead lines. The precise identification of a breakdown in a submarine cable is also harder to locate than with an overhead power line; as mentioned above, it usually takes longer to repair a submarine cable than an overhead line, given the shortage of repair ships and the complexity of the tasks.

Both the submarine and overland infrastructure required to synchronize the Baltic states with either the Nordic or Continental grids is vulnerable to deliberate physical attacks as well as unintended physical disruptions; and these vulnerabilities could be exploited to advance Russia's strategic goals.

Russia seems to have the knowledge and capabilities necessary to sabotage submarine infrastructure and would be able to exploit the unique physical and legal environment at sea to conceal its actions until it is too late to respond. Its naval action in international waters – with or without a legal pretext – could also considerably delay identification of damaged sections of the submarine cables and their repairs, which are complex and challenging tasks even without interference by a hostile actor. Difficulties of comprehensively observing and controlling maritime space – particularly beyond national territorial waters – and the lack of civilian and military naval capabilities (especially in Estonia) – as well as the considerable expense of building such capabilities mean that the options for credibly protecting submarine interconnectors are very limited.

In any case, management of hybrid threats – one of them being sabotage of energy infrastructure for coercive or destabilizing purposes – is primarily a national responsibility.

In the foreseeable future, the owners of such infrastructure would have to rely on the limited capabilities and willingness of Finland (and perhaps Sweden) as well as NATO or the EU to ensure such continuous protection and incident response. However, this option has serious political and strategic constraints as well. As of now, NATO has not shown any initiative to provide a stronger maritime presence in the Gulf of Finland, and may not consent to applying Article 4 security assistance measures in the event of a crisis, while the EU's mechanisms are largely untested and uncertain. As militarily nonaligned countries, both Finland and Sweden lack the same ability to provide deterrence as do NATO members. In any case, management of hybrid threats – one of them being the sabotage of energy infrastructure for coercive or destabilizing purposes – is primarily a national responsibility (for the submarine cables in the Gulf of Finland – of Estonia and Finland). The execution of this responsibility in the EEZ could also be a complicated matter from a legal perspective.

In addition to issues in the maritime domain, submarine cables also raise protection issues on land at the points where those interconnectors link to the grids. Physical capabilities in deterring, detecting, and responding to a threat to these overland segments differ from those in the maritime domain. In terms of protection capabilities, land-based surveillance and control measures are cheaper and easier to put in place than those needed for maritime surveillance, although they need to be more extensive. Furthermore, the land domain is a sovereign national territory where, unlike in an EEZ, nations have full authority to enact all the necessary civilian and military measures to protect their critical infrastructure, prevent attacks, capture suspects, and ensure the quick and undisturbed recovery of that infrastructure. The wider spread and use of aerial drones can be identified as one of the rising future threats, as they are likely to gain popularity among those with the intention to

Given that it is not easy to identify the perpetrator behind a drone attack or detect and observe all cross-border activities, we might see more "little blue drones" instead of "little green men" in the future.

damage or destroy relevant infrastructure. They are not only difficult to detect but might also be difficult to intercept or destroy. Given that it is not easy to identify the perpetrator behind a drone attack or detect and observe all cross-border activities, we might see more "little blue drones" instead of "little green men" in the future.

Synchronization through the current LitPol Link overhead line would place even more strategic pressure on the Suwałki Gap region. Because of the intense concentration of infrastructure in this narrow strip and its importance to the military reinforcement the Baltic states by the rest of NATO, the area is recognized as a strategic bottleneck. It is already being given special attention from both Poland and Lithuania as well as on an international level, ranging from enhancing control of external EU borders and improving operational and organizational frameworks and capabilities to respond to hybrid attacks to increasing the pace of military exercises in the area. Russia's asymmetric action – using special forces or proxies such as criminal groups – against overland synchronization interconnectors would have higher odds of failure and lesser impact on overall system resilience (in terms of recovery time) compared to asymmetric action at sea.

Neither direction provides a one hundred percent secure and attack-proof solution.

Which synchronous area would then be the better option in terms of combating non-linear means of disruption or managing their impact? Neither direction provides a one hundred percent secure and attack-proof solution. However, asymmetry in national maritime capabilities and in alliance memberships (as an ultimate deterrent) between Estonia and Finland as well as the maritime "gray zone" of action in the Nordic direction stands in stark contrast to the situation in the Continental direction, where there is a relative symmetry of security capabilities, shared NATO membership, and total sovereign control of the entire length of the relevant interconnectors.

Thus, based on the findings of this chapter, in terms of the nature of vulnerabilities and resilience, availability and development of the required capabilities as well as legal, political and international frameworks for their use, it can be concluded that synchronizing with the Continental grid would be more advantageous for the Baltic states compared to the Nordic option in terms of CEIP. However, the two-line scenario is certainly more optimal, compared to the one-line scenario, as it provides for greater physical resilience through redundancy in case of disturbances and crises.

Synchronizing with the Continental grid would be more advantageous for the Baltic states compared to the Nordic option in terms of CEIP. However, the two-line scenario is certainly more optimal, compared to the one-line scenario, as it provides for greater physical resilience through redundancy in case of disturbances and crises.

Chapter V

The Invisible Front: A Cyber Resilience Perspective

Hayretdin Bahşi

The protection of critical infrastructure (CI) against cyber threats is one of the foremost action items on national security agendas, as it aims to prevent malicious cyber activities that may cause major physical consequences such as human losses, property damage, and widespread disruption. Cyber security concerns are becoming more serious due to the increasing dependence of CI on information and communications technology (ICT) and operational technology (OT) systems, as well as the potential cascading effects of cyber incidents on many highly interdependent parts of national and cross-border CI. Cyber-attacks on an Iranian nuclear facility and on Ukrainian electricity infrastructure proved that cyber resilience has an important role in the overall resilience of critical infrastructure in general and the energy sector in particular, where electricity transmission systems play a vital role.[159] Hence, these systems need to resist cyber threats that are becoming more sophisticated and targeted.

The protection of critical infrastructure (CI) against cyber threats is one of the foremost action items on national security agendas.

The Baltic states are investigating options for desynchronization from the Russia-controlled IPS/UPS transmission grid and synchronization with the Continental or Nordic grids instead. In this chapter, the cyber resilience of the latter two grids is compared in order to provide domain-specific insights which could inform this strategic decision. Moreover, additional technical or organizational measures that can be taken during this transition period are provided as guidance for transmission system operators and relevant national/international authorities.

The important aspect of this chapter is that the planned transition coincides with the ongoing business and technological changes that have occurred due to the efficiency and decarbonization aims of European energy policy. In this new era, smart grid technology will act as a significant enabler, meaning that energy operations will be more dependent on information systems.[160] Moreover, ICT and OT systems will be more integrated in order to fulfill the new requirements.[161] Although current energy systems are also prone to cyber threats under conditions of relatively low-level integration of IT and OT components, future systems can be compromised by malicious actors with less capability in resources and sophistication, which means the threat landscape consisting mainly of nation-state actors would be extended to terrorist and criminal groups. Small and medium-sized electricity producers would be additional targets for criminal groups pursuing economic benefit. In addition, in order to induce a destabilizing effect, nation-state actors could use cybercrime groups as proxies to attack energy systems in target states. The cyber resilience of energy systems will thus become a much greater concern in the near future due to the possible diversification of the threat landscape.

Cyber resilience is described as the "ability to continuously deliver the intended outcome despite adverse cyber events".[162] In our specific

[159] "Stuxnet: Computer worm opens new era of warfare", *CBS News*, June 4, 2012, http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/ (accessed August 1, 2017); Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), *Cyber-attack Against Ukrainian Critical Infrastructure*, Alert (IR-ALERT-H-16-056-01) (Washington DC, 2016), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (accessed August 1, 2017).

[160] Pieter Vingerhoets, Maher Chebbo and Nikos Hatziargyriou, *The Digital Energy System 4.0* (Smart Grids European Technology Platform, 2016), https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf (accessed August 1, 2017).

[161] David Healey, Sacha Meckler, Usen Antia and Edward Cottle, *Cyber Security Strategy for the Energy Sector* (Brussels: European Parliament, 2016), http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf (accessed August 1, 2017).

[162] Fredrik Björck, Martin Henkel, Janis Stirna and Jelena Zdravkovic, "Cyber Resilience – Fundamentals for a Definition" in *Advances in Intelligent Systems and Computing*, Vol. 353, ed. Janusz Kacprzyk (Springer, 2105), 311–6, doi: 10.1007/978-3-319-16486-1_31, https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition (accessed August 1, 2017).

context, cyber resilience is perceived as the provision of electricity transmission in cases of encountering intentional/unintentional behaviors of people or natural events that have an impact on ICT or OT systems. Intentional behaviors encompass all types of malicious threats ranging from hacktivism to cyberterrorism and state-sponsored sabotage. Resilience against cyber threats is handled at different levels – supranational, national, regional, organizational, functional and technical.[163] In this chapter, the scope of the analysis is divided into five levels, as shown in Figure 1. The Transmission System Operator (TSO) Level analyzes the information security management and business continuity frameworks that are applied in organizations with electricity transmission responsibilities. Next, the Energy Sector Level deals with incident handling and crisis management capabilities across the whole energy sector and reviews existing regulatory frameworks on security standards, mandatory security requirements, security audits, incident reporting and, risk assesments. Third, the Critical Infrastructure (CI) Level examines the same items as the previous level from the perspective of all critical sectors. In addition, cooperation between CI actors and R&D organizations is reviewed at this level. The National Level covers findings that provide insights about national posture regarding cyber security. Finally, the Grid (i.e. Synchronous Area) Level gives an overview of the cyber security posture of all members of the Nordic and Continental grids. This level also outlines grid-wide information-sharing and incident-handling capabilities.

As a cyber incident may have cascading impact, the reliability of one grid member's electricity transmission systems depends on the systems of other members.

As a cyber incident may have cascading impact, the reliability of one grid member's electricity transmission system depends on the systems of other members. However, the states that act as connectors between the Baltic region and other grids are of foremost important in this analysis. The comparison of Poland and Finland is the most significant analysis point as these would be the immediate connectors for the Baltic states to the Continental or Nordic grids respectively. Germany and Sweden are also part of this comparative analysis, since they are the hubs and key players in their respective synchronous functioning areas. All levels except the Grid Level therefore compare these four countries.

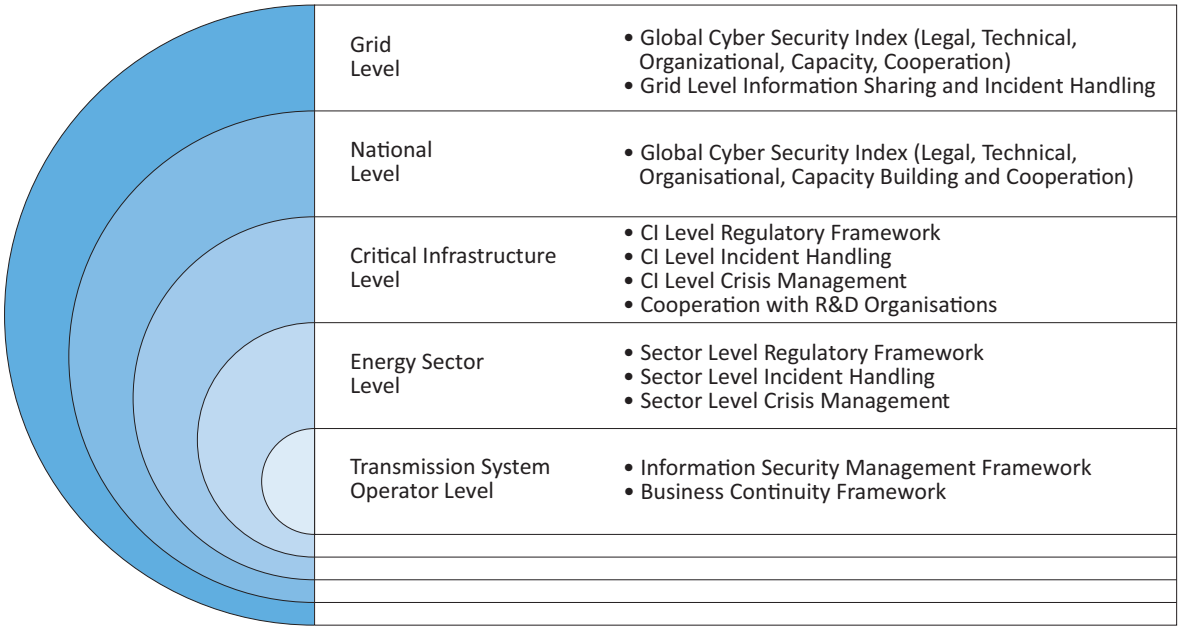

Figure 1. Scope of the Analysis

[163] Ibid.

The types of dependence between CI, which can be also applied to cross-border dependences, are classified into four categories: physical, cyber, geographic and logical.[164] As described in detail in section 5, the synchronization function does not itself create strong cyber dependence between the electricity transmission systems of the Baltic states and connector states. However, it does create dependence that can be classified as physical, meaning that the functional output of one system may impact the functions of others. In this analysis, the cyber resilience of connector states is important, since the impact of a major cyber incident on their systems can be propagated to the systems of Baltic states through the synchronization function.

The methodology of this study is mainly based on a desk review of policy documents and on analysis of reports and other open sources that provide information about each level within the scope of the study. In addition, surveys were conducted with the cyber security and IT experts of some TSOs.[165]

The limitation of this study is that the analysis is not based on the cyber risks to specific electricity transmission systems, information about which is restricted according to the confidentiality requirements of individual TSOs. However, a review of organizational and national cyber security frameworks and the relevant practices, as in this study, provides valuable insights into the short-, medium-, and long-term cyber resilience picture.

The reminder of this chapter is organized as follows. Section 1 gives an overview of the cyber resilience status of EU members in order to help the reader understand the spectrum of maturity levels currently achieved. Section 2 presents a comparison between Finland and Poland. Section 3 is dedicated to an analysis of Germany and Sweden. A grid-level analysis of the Continental and Nordic synchronous areas is given in Section 4. Recommended cyber security measures that can be applied during (de)synchronization periods appear in Section 5. The chapter concludes with a summary of the main findings in our analysis.

1. Overview of Cyber Resilience in Critical Infrastructure

The European Parliament adopted the Directive on Security of Network and Information Systems (NIS Directive) in July 2016.[166] This directive identifies the responsibilities of member states and CI operators on their territories. EU Member States are required to identify the operators of essential services, adopt a national strategy, designate competent authorities for monitoring the application of the directive, and establish cooperation mechanisms at national level. The directive urges operators of CI to take appropriate technical and organizational security measures and report security incidents to the relevant national authorities. This relatively new EU directive acts as an important milestone to accelerate efforts in CI protection by clearly assigning responsibilities to different actors at both the national and organizational levels.

EU Member States are required to identify the operators of essential services, adopt a national strategy, designate competent authorities for monitoring the application of the directive, and establish cooperation mechanisms at national level.

The NIS Directive sets out common ground for all CI sectors. In addition, the Energy Expert Cyber Security Platform (EECSP), established by the European Commission's Directorate-General for Energy, released a report emphasizing the importance of establishing

[164] Steven M. Rinaldi, James P. Peerenboom and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, December 2001: 11–25, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf (accessed August 1, 2017).

[165] Elering AS and Fingrid Oyj responded to our requests. An interview was conducted on May 31, 2017 with Elering AS, which also provided written responses to our additional questions. Fingrid completed our survey on July 21, 2017.

[166] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union", *Official Journal of the European Union*, 2016, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG (accessed August 1, 2017).

frameworks for threat and risk management, cyber response, maturity assessment, and capacity and competence development in the energy sector.[167] Without these frameworks, a reasonable level of assurance about cyber resilience of the sector may not be provided.

The EU Agency for Network and Information Security (ENISA) assessed the maturity level of eight EU members that have already initiated studies of ICS-SCADA cyber security within their critical infrastructure protection programs.[168] As of the date of this study, it is predicted that around 25% to 30% of member states had not initiated any activity in this field. Although the ENISA analysis does not give the maturity level of each participating state, it identifies various levels from "early developers" to "leaders". Even the "leaders" had not achieved the "established" level in every aspect, which means that "some required activities are not regularly conducted on the basic level." EU member states are fragmented in terms of cyber resilience levels in CIP, and much more progress is needed before the effects of the established EU regulatory frameworks appear in practice.

EU member states are fragmented in terms of cyber resilience levels in CIP, and much more progress is needed before the effects of the established EU regulatory frameworks appear in practice.

2. Comparison of Poland and Finland

2.1 TSO-level analysis

We did not receive any response to our survey request from the Polish TSO; we therefore conducted the comparison based on information about Polish TSO-level policies and practices available from open sources. Analysis of the Finnish TSO policies and practices is based on the survey response provided by Fingrid.

The Polish TSO, Polskie Sieci Elektroenergetyczne S.A. (PSE), has its own computer emergency response team (CERT). It formally conforms to standards in information security management (ISO 27001) and in business continuity management (ISO 22301).[169] PSE has established information-sharing channels with some national and international authorities. The company has signed an agreement with the National Cybersecurity Centre, which is responsible for information-sharing between the public and private sectors in Poland, and signed a letter of intent regarding the exchange of electricity infrastructure security-related information with the NATO Energy Security Centre of Excellence.[170] Two projects, for the implementation of Security Information and Event Management (SIEM) data communications security monitoring system and the deployment of data communication security systems at electrical substations, are listed in its development plans.[171] PSE agreed with Energa Grup, another big energy player in Poland, the creation of a CERT team for the entire Polish energy sector.[172]

[167] Energy Expert Cyber Security Platform, *Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,* Report, February 2017, https://ec.europa.eu/energy/sites/ener/files/documents/ee-csp_report_final.pdf (accessed August 1, 2017).

[168] Rosella Mattioli and Konstantinos Maulinos, *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors* (European Union Agency for Network and Information Security (ENISA), 2015), https://www.enisa.europa.eu/publications/maturity-levels/at_download/fullReport (accessed August 1, 2017).

[169] ISO 27001 is a comprehensive standard that includes business continuity. ISO 22301 gives more detailed guidance about providing availability. For PSE certificates, see: "Certificates", Polskie Sieci Elektroenergetyczne, accessed August 1, 2017, http://www.pse.pl/index.php?dzid=178&did=1305.

[170] "Hackers may attack the energy sector. Poland is arming itself", *Business Alert*, June 14, 2017, http://biznesalert.com/hackers-may-attack-energy-sector-poland-arming/ (accessed 1 August 2017).

[171] Polskie Sieci Elektroenergetyczne, *Development Plan for Meeting the Current and Future Electricity Demand for 2016-2025* (Konstancin-Jeziorna, 2015), http://www.pse.pl/uploads/kontener/Development_Plan_for_meeting_the_current_and_future_electricity_demand_for_2016-2025.pdf (accessed August 1, 2017).

[172] "Hackers may attack the energy sector".

The Finnish TSO, Fingrid, completed a continuity management project in 2014.[173] Fingrid has no specific TSO-level CERT.[174] It uses ISO 27001 as a framework, but does not claim formal conformity with this standard. Cyber exercises that address the security issues of industrial control systems have been organized in this environment. Fingrid conducted a cyber exercise for sector operators in February 2017 with power grid company Elenia Oy.[175] The cyber range operated by JYVSECTEC at the JAMK University of Applied Sciences was used in this exercise.[176]

In summary, PSE formally conforms to ISO 27001 and ISO 22301, has two security projects in its development plans, and has a dedicated CERT which even shows willingness to create a sector-level CERT in Poland. On the other hand, Fingrid completed a continuity management project, uses ISO27001 as a framework, incorporated cyber resilience into its operational exercises, and has the advantage of having closer cooperation with R&D institutions in conducting cyber security exercises. It can be concluded that there is no significant difference between the two TSOs with regard to policies and practices aimed at enhancing their cyber resilience.

2.2 Energy and Critical Infrastructure Level Analysis

Poland launched a National Cybersecurity Center in 2016 in order to improve collaboration and data exchange among various sectors and institutions in the country.[177] Poland has established CERT organizations such as CERT. GOV.PL and CERT Polska, and the former is involved in CI protection.[178] The Government Centre for Security runs a comprehensive critical infrastructure protection program that includes physical and cybernetic systems.[179] However, based on open sources alone, it was impossible to ascertain the existence of action plans and activities at this level of cyber resilience. Although Poland has published a national cyber security strategy and established relevant national-level bodies, sector-specific cyber security plans have not yet been developed.[180] The Cybersecurity Foundation, a non-governmental organization established to raise cyber security awareness, has organized cyber security exercises for critical sectors such as energy, finance and telecommunications.[181] In 2012 an exercise was held with the involvement of energy companies.

Poland launched a National Cybersecurity Center in 2016 in order to improve collaboration and data exchange among various sectors and institutions in the country.

CI security is the main theme of Finland's national cyber security strategy.

CI security is the main theme of Finland's national cyber security strategy. Action point 16 of the "Implementation Program for Finland's Cyber Security Strategy for 2017–2020" specifically addresses protection of the electricity sector. In action point 17, considerable budgetary and human resources are allocated to the cyber security development projects of the National Emergency Supply Agency (NESA). Sector-specific security

[173] Mira Muurinen, "Continuity management is day-to-day work", *Fingrid – Corporate Magazine* 3/2014: 10–11, http://www.fingrid.fi/en/news/News%20liitteet/Magazines/2014/Fingrid_3_2014_EN.pdf (accessed August 1, 2017).

[174] Based on the survey response received from Fingrid on July 21, 2017.

[175] Heli Sutinen, "Cyber Exercises for Operators in the Industry Sector was Piloted", *JYVSECTEC – Jyveskyla Security Technology,* 21 February 2017, http://jyvsectec.fi/en/media/ (accessed August 1, 2017).

[176] "JYVSECTEC Cyber Range: RGCE and solutions", JYVSECTEC, accessed August 1, 2017, http://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range1.pdf.

[177] "National Cybersecurity Center launched in Warsaw", *Radio Poland,* July 5, 2016, http://www.thenews.pl/1/9/Artykul/260202,National-Cybersecurity-Center-launched-in-Warsaw (accessed August 1, 2017).

[178] BSA, *EU Cybersecurity Dashboard*: *A Path to a Secure European Cyberspace* (London, 2015), http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf (accessed August 1, 2017).

[179] Government Centre for Security, *The National Critical Infrastructure Protection Programme* (Warsaw, 2015), http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf (accessed August 1, 2017).

[180] BSA, *EU Cybersecurity Dashboard*.

[181] "About Cybersecurity Foundation", Cybersecurity Foundation, accessed August 1, 2017, https://www.cybsecurity.org/en/home-page/.

priorities have not been identified.[182] National Cyber Security Centre Finland, which was established in 2014, runs an early warning and monitoring system named HAVARO and a bulk incident reporting system called Autoreporter for critical infrastructure and government institutions.[183] Finland's national CSIRT (CERT) is run by this center. Its service lists include the protection of CI, but it has not developed SCADA security capabilities.[184] In Finland, no cyber security regulation is applied to the electricity transmission sector.[185] However, the NIS Directive will be in force from 2018. VTT Technical Research Centre of Finland Ltd., in cooperation with NESA, conducts several cyber security projects, including in industrial control system security.[186] A fifth national cyber security exercise was held in May 2017.[187] A cyber exercise for the energy sector was conducted in February 2017.[188]

In summary, Poland has a strong critical infrastructure protection program with a broad scope, but the link between this program and any specific cyber resilience action items is not clear. Finland is at the stage of developing the 2017–2020 Implementation Program, which establishes such linkages. Neither country has developed mature national cyber security capabilities for CI protection. However, the Finnish Implementation Program includes clear responsibilities and action points. The cooperation between the Finnish national emergencies management authorities and R&D organizations in the area of industrial control system security is also noteworthy.

Poland has a strong critical infrastructure protection program with a broad scope.

2.3 National level analysis

In 2014 and 2017, the International Telecommunication Union conducted and published studies under the title "Global Cybersecurity Index" in which the national cyber security commitments of states were evaluated and ranked in five pillars: legal, technical, organizational, capacity-building, and cooperation.[189] Although the index addresses general national cyber security issues and is not dedicated to CI protection, it constitutes a useful resource for performing a comparative analysis of the national-level cyber security activities of different countries. According to their scores, states are categorized into three main groups: leading, maturing, and initiating. Being in the "Leading" category means that a country shows high commitment in all five pillars. States that have developed complex commitments and engage in cyber security programs and initiatives are classified as "maturing".

Finland has a score of 0.741 and is ranked 16th in the Global Cyber Security Index 2017, while Poland scores 0.622 and is ranked 33rd. In the 2014 studies, Finland and Poland had scores of 0.618 and 0.519 respectively. Twenty-two countries have a higher score than Finland and 35 are better than Poland in the 2014 index.[190] These results show that Finland is ranked higher than Poland in both studies – and had been making greater progress from 2014 to 2016 to ensure national cyber resilience.

Both Poland and Finland pursue ambitious goals in cyber security. Finland's national cyber security strategy sets the aim of being a "global forerunner" in preparedness against cyber threats. Poland is interested in being a global

[182] BSA, *EU Cybersecurity Dashboard*.

[183] "CERT-FI service description (RFC 2350)", Finnish Communications Regulatory Authority, last modified April 4, 2017, accessed August 1, 2017, https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html.

[184] "Searchable Team Database", TF-CSIRT Trusted Introducer, last modified November 3, 2017, accessed November 3, 2017, https://www.trusted-introducer.org/directory/teams.html; Fingrid survey response.

[185] Fingrid survey response.

[186] "Cyber Security", VTT Technical Research Centre of Finland Ltd., accessed August 1, 2017, http://www.vttresearch.com/services/digital-society/cyber-security.

[187] "Viides kansallinen kyberharjoitus järjestetään toukokuussa" [A fifth national cyber exercise will be held in May], Puolustusministeriö [Ministry of Defense], last modified March 16, 2017, accessed August 1, 2017, http://www.defmin.fi/ajankohtaista/tiedotteet?9_m=8296.

[188] "Viides kansallinen kyberharjoitus järjestetään toukokuussa".

[189] "Global Cybersecurity Index", International Telecommunications Union, accessed August 1, 2017, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

[190] The Global Cyber Index 2014 study does not give exact rankings as many countries share the same ranking value. We therefore conducted comparisons based on the number of countries having higher scores than the state being considered.

leader in the cyber security sector.[191] The Finnish Information Security Cluster was established in 2012 by major cyber security companies to promote business and operations.[192] Poland's "Cyberpark Enigma" program intends to increase the number of R&D institutions.[193] Although both countries are determined to improve national cyber security efforts, Finland reflects its aim in official documents and has taken solid steps towards enhancing the cyber security industry by establishing a security cluster.

Both Poland and Finland pursue ambitious goals in cyber security.

A non-profit organization, CyberGreen Institute, provides measurement results about the IP addresses belonging to a specific country or autonomous system in order to offer insight to CERTs, network operators, and policymakers on the overall cyber security status of individual entities.[194] Such measurements can serve as one indicator of overall national cyber resilience.

The numbers of misconfigured Domain Name System (DNS), Network Time Protocol (NTP), Simple Network Management Protocol (SNMP) and Simple Service Discovery Protocol (SSDP) services, Mirai infections, and the estimated size of distributed denial of service (DDoS) traffic within the IP address blocks of Finland and Poland are compared in Figure 2, based on results derived from the CyberGreen Institute. Attackers can use misconfigured network services to amplify DDoS attacks that they launched against other targets.[195] These statistics can be used to highlight differences between the prevalence of cyber security practices in these countries. The graphs in Figure 2 only compare the number of misconfigured IP addresses and do not normalize them according the countries' total network size. There are approximately 13 million IP addresses in Finland and 21 million in Poland.[196] These numbers can give an insight into the network size of the respective countries. Considering this fact, it can be deduced that Finland has a much lower number of recursive DNS and SSDP misconfigurations than Poland. The SNMP graph demonstrates that Poland has a decreasing pattern in the range of 40k and 80k, while Finland has a decreasing line with around 10k and below, which means Finland has better results in this category as well. Although the difference is smaller than in the previous graphs, Finland has a less vulnerable ratio in NTP services, as Poland stays roughly in the range of 30k – 40k, while Finland fluctuates between 10k and 20k. The CyberGreen Institute also estimates the size of DDoS traffic that can be generated by using misconfigured devices. Estimated DDoS traffic originating from Polish networks fluctuates between 10 and 40 TBit/sec, while Finnish networks produce values of 10 TBit/sec and below. This result shows that Finnish network services may cause DDoS amplification attacks with less traffic.

[191] Danielle Kriz, "Poland expands leadership role in cybersecurity", *Paloalto Networks Blog*, October 11, 2016, https://researchcenter.paloaltonetworks.com/2016/10/gov-poland-expands-leadership-role-on-cybersecurity/ (accessed August 1, 2017); Wiesław Goździewicz, Cyprian Gutkowski, Lior Tabansky and Robert Siudak, *Security Through Innovation: Cybersecurity sector as a driving force in the national economic development* (Krakow: The Kosciuszko Institute, 2017), http://www.ik.org.pl/wp-content/themes/ik/report-img/security-through-innovation.pdf (accessed August 1, 2017).

[192] Finnish Information Security Cluster, accessed August 1, 2017, http://www.fisc.fi/en/.

[193] Ministerstwo Rozwoju [Ministry of Development], Responsible Development Plan (Warsaw, 2016), https://www.mr.gov.pl/media/14873/Responsible_Development_Plan.pdf (accessed August 1, 2017).

[194] CyberGreen Institute, accessed August 1, 2017, https://www.cybergreen.net/.

[195] Christian Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse", Network and Distributed System Security Symposium, 2014, http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/01_5.pdf (accessed August 1, 2017)

[196] "IP Address Range Usage in Finland", ipaddress.live, accessed October 1, 2017, https://www.ipaddress.live/ip-address-finland.php; "IP Address Range Usage in Poland", ipaddress.live, accessed October 1, 2017, https://www.ipaddress.live/ip-address-poland.php.

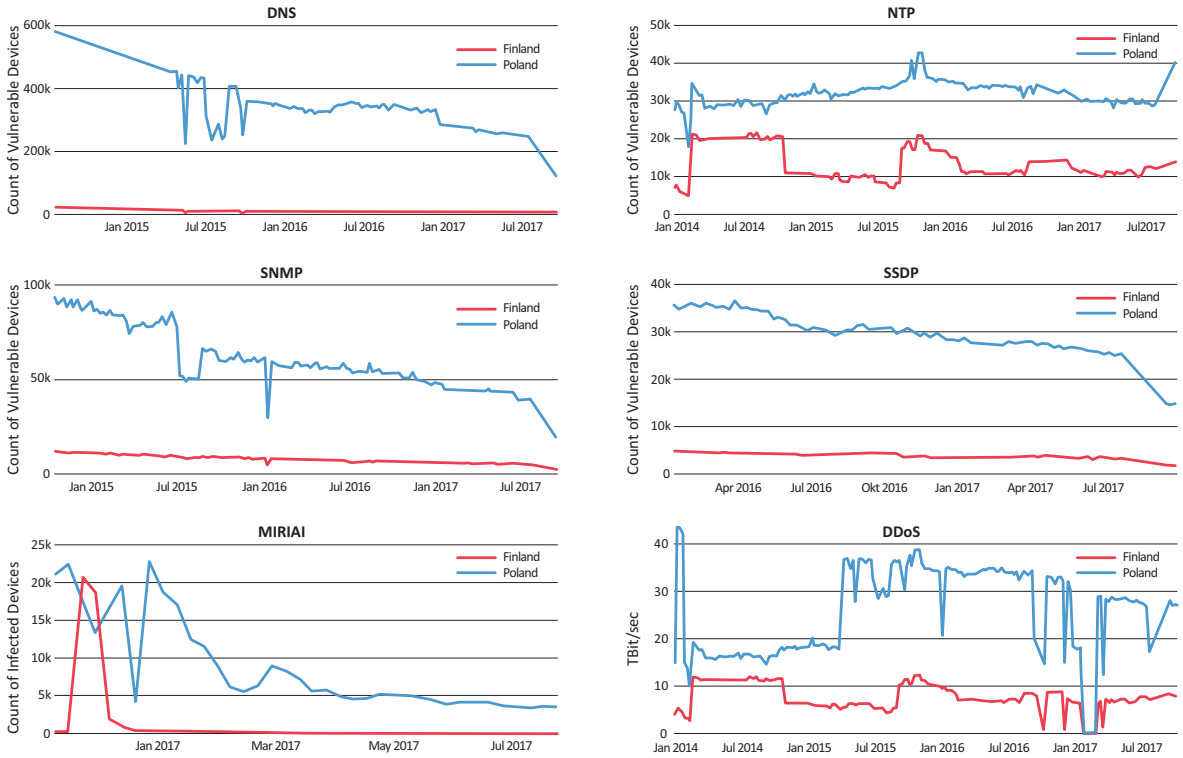

Figure 2. Misconfigured network services, Mirai infections and estimated DDoS size: Finland and Poland.

Numerous targets – including the website of computer security journalist Brian Krebs (Krebs on Security), the French web-hosting firm OVH, and, the DNS provider DYN – were exposed to massive DDoS attacks in 2016.[197] The attacks were launched from a botnet consisting of IoT devices compromised by Mirai malware. This was the first massive attack to exceed 600 Gbps in volume. CyberGreen Institute also provides data showing the number of infected devices that have been part of a Mirai botnet in Poland and Finland. The Mirai graph in Figure 2 encompasses the period from the end of 2016 to July 2017. When this graph is analyzed together with the results given in the study by Antonakakis et al., it can be seen that the spike of infections at the end of 2016 and early 2017 is very probably related to a variant of Mirai that compromises a remote code execution exploit in router devices. This vulnerability requires immediate patching actions by internet server providers (ISPs) and other network operators. Despite the spike in infected devices in December 2016, it can be deduced that Finnish network operators managed to address the problem in a relatively short time. However, in Polish networks, mitgating the problem and restoring stability took longer.

Microsoft gathers and analyzes a huge amount of data from the computers that run Microsoft security programs and services, publishing quarterly security intelligence reports that include country-based results. The comparison of Poland and Finland in terms of five security metrics is given in Table 1. The metrics analyzed in this part are defined as follows. "Encounter rate" refers to the percentage of computers running Microsoft security products that report a malware encounter. "Phishing sites" counts the number of known phishing sites that have been accessed by users. "Malware hosting sites" gives the number of sites running malware, and "drive-by download pages" shows the number of websites that host exploits aimed at compromising of users' web browsers. The ratios for site access variables are calculated per 1,000 URLs. High values in these metrics may occur for two reasons: 1) Information systems in the corresponding country are not secure enough to

Websites in Finland have stronger protection against malware.

[197] Manos Antonakakis et al., "Understanding the Mirai Botnet," 26th USENIX Security Symposium, 2017, https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf (accessed August 1, 2017).

contain and eliminate cyber threats, so security tools detect a higher number of malicious activities 2) Information systems face much more cyber threats due to factors such as the high prevalence of cybercrime. While analyzing the results of these metrics, it is not easy to discern which have an impact on overall results and to what extent. However, the last three metrics may give a clear insight into the security of websites in individual countries. As Finland is better in each item according to results given in Table 1, it can be concluded that websites in Finland have stronger protection against malware.

Security metric	Poland	Finland	World average
	1Q17	1Q17	1Q17
Encounter rate	7.7	2.9	9.06
Drive-by download pages	0.10	0.09	0.17
Phishing sites	7.3	2.4	6.3
Malware hosting sites	6.1	4.1	14.8

Table 1. Country-based Microsoft security intelligence outputs: Poland and Finland[198]

3. Comparison of Germany and Sweden

3.1 TSO level analysis

Svenska Kraftnät is the electricity supply regulator and also manages the Swedish electricity grid. The budget for security protection and information security measures was 23 million Swedish kronor (€2.3 million) in 2015 and 14 million kronor (€1.4 million) in 2016.[199] The company uses the ISO 27000 series as a framework approach for information security.[200] Germany's power grid is composed of four control areas, each controlled by one operator. As transmission system operator 50Hertz manages the area that includes the Polish border, the cyber security framework and practices of this operator are included in the study. The company developed a two-year implementation plan for the establishment of information security management system (ISMS). Its annual report for 2016 states that operational IT security tasks include virus/spam detection and monitoring of the company's internet presence.[201]

Svenska Kraftnät assigns a specific budget for information security and has a policy for information security management. However, no detailed information was available about this company's level of ISMS implementation. 50Hertz has a specific implementation plan for the establishment of ISMS. On the other hand, the operational tasks listed in the annual report gives no clue as to the extent to which OT systems are included in operational security tasks.

3.2 Energy and critical infrastructure level analysis

The Swedish Civil Contingencies Agency (MSB) is responsible for the administration of Sweden's national information security strategy and handling cyber incidents. The National Computer Emergency Response Team has been part of MSB since 1 January 2011. MSB has published an action plan for the protection of critical infrastructure.[202] Each sector authority is required to develop a sectoral plan by 31 December 2017. MSB developed a national response plan for handling serious IT incidents

[198] Microsoft Corporation, *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Finland* (Redmond, WA, 2017), http://download.microsoft.com/download/0/5/A/05AF93AF-BBF9-4754-B86A-2ACCA03610AC/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Finland.pdf (accessed August 1, 2017); Microsoft Corporation, *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Poland* (Redmond, WA, 2017), http://download.microsoft.com/download/C/B/0/CB0DB5F5-7D10-4538-9B7B-180F89A7F9C6/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Poland.pdf (accessed August 1, 2017).

[199] Svenska Kraftnät, *Annual Report for 2015* (Stockholm, 2016), http://www.svk.se/siteassets/om-oss/organisation/finansiell-information/annual-report_2015.pdf (accessed August 1, 2017); Svenska Kraftnät, *Annual Report for 2016* (Stockholm, 2017), http://www.svk.se/siteassets/om-oss/organisation/finansiell-information/annual-report-svenska-kraftnat-2016.pdf (accessed August 1, 2017).

[200] Svenska Kraftnät, *Svar på frågor i Consultation Paper on risk preparedness in the area of security of electricity supply*, D-nr: Svk 2015/1612, Ert d-nr: dnr M2015/2810/Ee (September 14, 2015), http://www.svk.se/siteassets/om-oss/remissvar/svenska-kraftnats-svar-pa-eu-consultation-paper-on-risk-preparedness-plans.pdf (accessed August 1, 2017).

[201] 50Hertz Transmission GmbH, *Annual Report 2016: A Successful Energy Transition – for a Sustainable World* (Berlin, 2016): 54, http://www.50hertz.com/Portals/3/Content/Dokumente/Medien/Publikationen/2016/50Hertz_GB_Gesamt_E_Web.pdf (accessed August 1, 2017).

[202] Swedish Civil Contingencies Agency (MSB), *Action Plan for Protection of Vital Societal Functions and Critical Infrastructures* (Karlstad, 2014), https://www.msb.se/RibData/Filer/pdf/27412.pdf (accessed August 1, 2017).

in 2011.[203] It runs a program dedicated to the cyber security of industrial control systems, has established the FIDI-SC forum – an information-sharing platform between the representatives using ICSs; has released guidance about ICS security, and has organized relevant courses with Svenska Kraftnät.[204] A national cyber security exercise, *NİSÖ 2012*, was conducted with the involvement of the energy, telecommunications and transport sectors.[205] In 2015, Svenska Kraftnät collected information about the information security risks of 20 actors in electricity supply.[206] It has also launched a portal on energy security issues.[207] The Swedish cyber security community organizes ICS security dedicated events such as CS3STHLM.[208] In Sweden, no cyber security regulation is applied to critical infrastructure in areas such as incident reporting or conformity to information security standards.[209] However, MSB provides guidelines and tools that help organizations to establish information security management systems.[210] This agency has funded research centers such as the Centre for Resilient Critical Infrastructures (CERCES) and the National Research Centre on Resilient Information and Control Systems. Meanwhile, the Swedish Defense Research Agency (FOI) has established a National Center for Security in Industrial Control Systems.[211] FOI maintains the training and exercise infrastructure named "Cyber Range and Training Environment (CRATE)."[212]

In Germany, the Bundesamt für Sicherheit in der Informationstechnik [Federal Office for Information Security] (BSI) is responsible for ensuring the security of critical infrastructure and has a dedicated branch for the purpose.[213] Another branch tasked with operational aspects has a section dealing with ICS security. This branch also includes a National Cyber Response Centre, which was established in 2011 and is responsible for information-sharing between relevant authorities. The Federal Ministry of the Interior published a National Plan for Information Infrastructure Protection in 2005, the CIP Implementation Plan in 2007 and National Strategy for Critical Infrastructure Protection in 2009.[214] The IT Security Act that came into effect in 2015 requires the CI operators to implement state-of-the-art technical and organizational security measures and to report incidents to the BSI.[215] Operators of electricity grids must establish information security management systems

[203] Swedish Civil Contingencies Agency (MSB), *Handling Serious IT Incidents: National Response Plan, interim version, March 2011* (Karlstad, 2011), https://www.msb.se/RibData/Filer/pdf/26085.pdf (accessed August 1, 2017).

[204] Swedish Civil Contingencies Agency (MSB), *Guide to Increased Security in Industrial Information and Control Systems* (Karlstad, 2014), https://www.msb.se/RibData/Filer/pdf/27473.pdf (accessed August 1, 2017); "News from the Industrial Information and Control Systems Programme", Swedish Civil Contingencies Agency (MSB), last modified June 19, 2017, accessed August 1, 2017, https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-programmet-for-industriella-informations--och-styrsystem/Utbildningstillfallen-i-november/.

[205] Roger Holfeldt, "National Cyber Security Exercise (NİSÖ 2012): Conducting the exercise and main lessons learned," Swedish Civil Contingencies Agency (MSB), presentation, 2012, https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/roger-holfeldt-msb-sweden-the-national-cyber.pdf (accessed August 1, 2017).

[206] Svenska Kraftnät, *Annual Report for 2015*.

[207] Energy Security Portal, accessed August 1, 2017, https://www.energisakerhetsportalen.se/.

[208] The Stockholm International Summit on Cyber Security in SCADA and Industrial Control Systems, October 23–26, 2017, accessed 1 August 2017, https://cs3sthlm.se/.

[209] Jim Runsten, Ida Häggström and Vencel Hodák, "Cybersecurity", Synch Advokat AB, 2017, https://gettingthedealthrough.com/area/72/jurisdiction/38/cybersecurity-sweden/ (accessed August 1, 2017).

[210] "Stöd för systematiskt arbete med informationssäkerhet i organisationer" [Support for systematic work with information security organizations], Informationssakerhet.se, accessed August 1, 2017, https://www.informationssakerhet.se/.

[211] Richard Oehme, "Cyber security in Sweden – With focus on National Collaboration forum and Private Public Partnership", Swedish Civil Contingencies Agency (MSB), Presentation, 2015, https://www.viestintavirasto.fi/attachments/esitykset/Richard_Oehme_Presentation_Fi_2015-11-04.pdf (accessed August 1, 2017).

[212] "CRATE – Cyber Range and Training Environment", Swedish Defense Research Agency (FOI), accessed 1 August 2017, https://www.foi.se/en/our-knowledge/information-security-and-communication/information-security/labs-and-resources/crate---cyber-range-and-training-environment.html.

[213] "Organisational Chart", Federal Office for Information Security, last updated September 14, 2017, accessed September 19,2017, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf.

[214] Federal Ministry of the Interior, *National Plan for Information Infrastructure Protection* (Berlin, 2005), http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf (accessed August 1, 2017); Federal Ministry of the Interior, *CIP Implementation Plan of the National Plan for Information Infrastructure Protection* (Berlin, 2005), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile (accessed August 1, 2017); Federal Ministry of the Interior, *National Strategy for Critical Infrastructure Protection* (Berlin, 2009), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile (accessed August 1, 2017).

[215] "Gesetz zur Erhöhung der Sicherheit informations technischer Systeme (IT-Sicherheitsgesetz)" [Law to increase the security of information technology systems (IT Security Act)], *Bundesgesetzblatt Federal Law Gazette*, No. 31, 2015, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start= //*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1506502999550 (accessed 1 August 2017).

compatible also with ISO 27001.[216] UP KRITIS, a cross-sectoral cooperation platform between critical infrastructure sectors and government, was also established.[217] The BSI is creating Mobile Incident Response Teams (MIRTs) to examine serious incidents that could occur in any IT system, including those of critical infrastructure. The law on digitalizing energy transformation sets out security requirements for smart energy meters.[218] The BSI publishes annual reports that give an overview of the security of IT systems in Germany, including those of critical infrastructure.[219] In 2011, Germany conducted a national crisis management exercise, *LÜKEX 11*, which focused on the protection of critical infrastructure against cyber-attacks. The Fraunhofer Institute conducts various research projects, such as "Smart Grid Protection against Cyber Attacks" and "Hardware-based Security for Industrial IT Networks".[220] Fraunhofer established a lab for the cyber security of industrial control systems in 2014.[221]

The assignment of comprehensive cyber security duties to the national contingencies authority may enable Sweden to deal with a serious cyber crisis situation more coherently. Germany has a strong information security authority with advanced technical and organizational capabilities in addition to having legal enforcement powers.

The Swedish authorities responsible for the energy sector in particular and critical infrastructure sectors in general provide detailed guidance about the implementation of ISMSs, while Germany has adopted an enforcement approach through strong regulation. The assignment of comprehensive cyber security duties to the national contingencies authority may enable Sweden to deal with a serious cyber crisis situation more coherently. On the other hand, Germany has a strong information security authority that has advanced technical and organizational capabilities in addition to legal enforcement powers. The IT Security Act is an important legal instrument for strengthening the cyber protection of critical infrastructure. Electricity grids are required to implement ISO 27001. Germany's national CERT has developed specific technical capabilities for incident handling in ICSs. However, in Germany, preparedness for serious cyber crises requires much more involvement of the national contingencies authority. Both countries conduct national-level cyber security exercises, but the frequency of these could be increased. Apart from some efforts that address the energy sector, sector-specific action plans do not exist in either country.[222] They do, however, conduct research regarding the security of ICSs.

3.3 National level analysis

In the Cyber Security Index 2017, Germany has a score of 0.679 and is ranked 24th, while Sweden scores 0.733 and is 17th. In the 2014 study, Germany's score was 0.706 and seven countries scored higher, while Sweden scored 0.647, with 19 countries scoring higher.

Based on data from the CyberGreen Institute, a comparison between Sweden and Germany is

[216] Taylor Wessing, "The German IT Security Law – Fact Sheet", *Lexology*, July 22, 2016, https://www.lexology.com/library/detail.aspx?g=0ca121a8-319f-4125-94cb-682d3a9343a4 (accessed August 1, 2017).

[217] UP KRITIS, *Public-Private Partnership for Critical Infrastructure Protection* (Bonn, 2014), http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile (accessed August 1, 2017).

[218] Dennis Laupichler, "Smart Meter Gateway", *BSI Magazine* 1 (2017): 60–1, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-01.pdf?__blob=publicationFile&v=4 (accessed August 1, 2017).

[219] For the latest, see Federal Office for Information Security, *The State of IT Security in Germany 2016* (Berlin, 2016), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3 (accessed August 1, 2017).

[220] "Overview", SPARKS – Smart Grid Protection Against Cyber Attacks, accessed August 1, 2017, https://project-sparks.eu/; "Trusted Core Network: Hardware-based Security for Industrial IT Networks", Fraunhofer Institute for Secure Information Technology, accessed 1 August 2017, https://www.sit.fraunhofer.de/en/tcn/.

[221] Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (Fraunhofer IOSB), *Annual Report 2015/2016* (Karlsruhe, 2016), https://www.iosb.fraunhofer.de/servlet/is/62654/ANNUAL-REPORT-Fraunhofer-IOSB-2015_2016.pdf (accessed August 1, 2017).

[222] BSA, "Country: Sweden", *EU Cyber Security Dashboard*: *A Path to a Secure European Cyberspace* (London, 2015), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_sweden.pdf (accessed August 1, 2017); BSA, "Country: Germany", *EU Cyber Security Dashboard*: *A Path to a Secure European Cyberspace* (London, 2015), http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf.

presented in Figure 3. There are approximately 120 million IP addresses in Germany and 27 million in Sweden.[223] Taking into account the differences between these numbers, it can be derived that the ratio of network nodes with DNS and NTP vulnerabilities are similar. Germany has lower ratios in the SNMP and SSDP categories. An important observation is that Germany has a decreasing pattern in all vulnerability groups, while Sweden is stable in NTP and SNMP, shows a slow decline in DNS recursive vulnerabilities, and fluctuates between 20k and 25k in SSDP vulnerabilities. Sweden's estimated DDoS traffic is roughly in the 20–25Tbit/sec range, while traffic originated in Germany shows a general continuous decrease below 100Tbit/sec, except a spike in 2017. Although these traffic volumes do not take the difference in network size into account, the gradually decreasing pattern in Germany is noteworthy. Figure 3 also gives the number of Mirai-infected devices. Fluctuations in the graphs do not reflect the effectiveness of incident response activities. However, Germany has a lower ratio of infected devices if the difference in network size is taken into account. Germany and Sweden are compared in Table 2 according to the statistics given in Microsoft Security Intelligence Reports. Results for the first quarter of 2017 show that Sweden has lower encounter, phishing, and malware hosting site figures.

Security metric	Germany 1Q17	Sweden 1Q17	World average 1Q17
Encounter rate	4.26	3.5	9.06
Drive-by download pages	0.03	0.03	0.17
Phishing sites	5.1	3.3	6.3
Malware hosting sites	7.0	5.7	14.8

Table 2. Country-based Microsoft security intelligence outputs: Germany and Sweden[224]

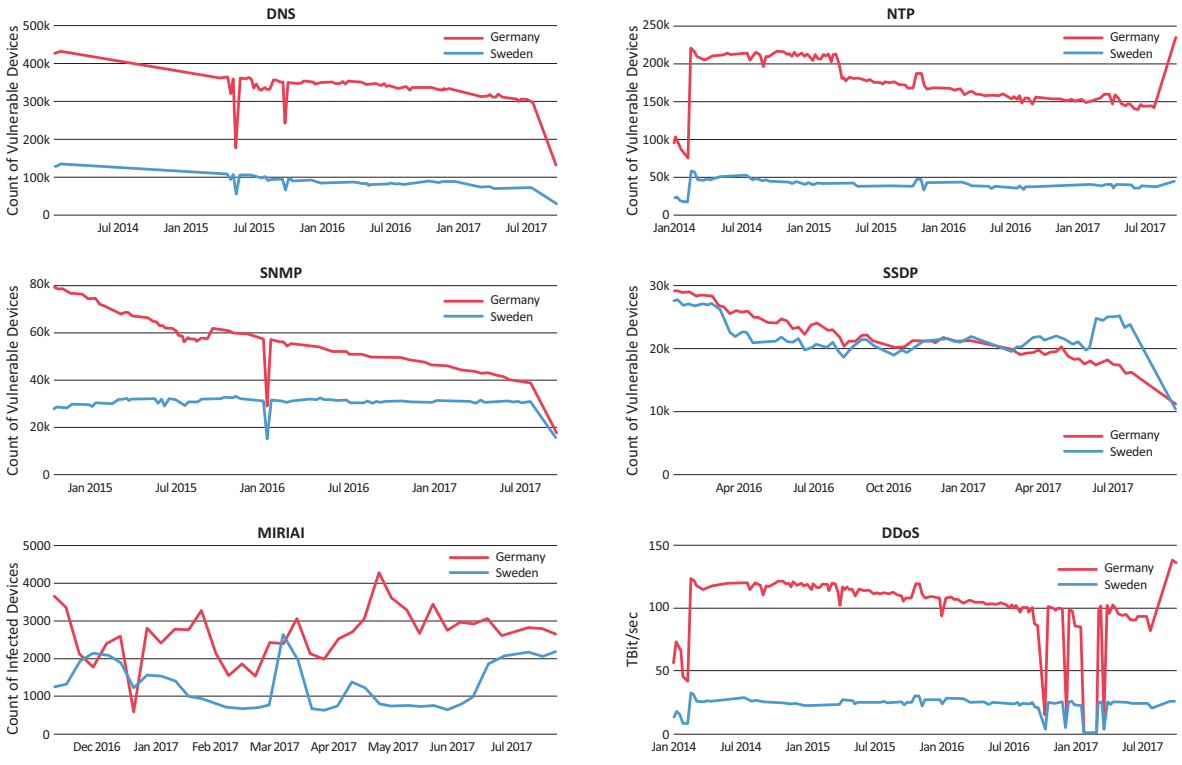

Figure 3. Misconfigured network services, Mirai infections and estimated DDoS size: Germany and Sweden.

[223] "IP Address Range Usage in Germany", ipaddress.live, accessed October 1, 2017, https://www.ipaddress.live/ip-address-germany.php; "IP Address Range Usage in Sweden", ipaddress.live, accessed October 1, 2017, https://www.ipaddress.live/ip-address-sweden.php.

[224] Microsoft Corporation, *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Germany* (Redmond, WA, 2017), http://download.microsoft.com/download/8/3/7/837488C4-D42D-47E5-820B-92DE154FD-FD3/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Germany.pdf (accessed August 1, 2017); Microsoft Corporation, *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Sweden* (Redmond, WA, 2017), http://download.microsoft.com/download/D/C/F/DCFD5A9E-98C2-4E91-8DB2-93E7385B93A9/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Sweden.pdf (accessed August 1, 2017).

4. Grid Level Comparison

According to the Global Cyber Security Index 2017, Estonia belongs to the leading group, while Latvia and Lithuania are classified as maturing states. Most of the 24 members of the Continental area belong to the maturing group (20 maturing, three leading and one initiating). Three members of the Nordic Grid – Finland, Sweden and Norway – are identified as leading states in cyber security. Denmark, a member of both grids, is in the "maturing" category. These results demonstrate that the cyber security commitments of members of the Nordic grid are stronger than for members of the Continental grid.

According to the Global Cyber Security Index 2017, Estonia belongs to the leading group, while Latvia and Lithuania are classified as maturing states. Most of the 24 members of the Continental area belong to the maturing group. Three members of the Nordic Grid – Finland, Sweden and Norway – are identified as leading states in cyber security.

In many countries, dedicated CERTs have been established to provide incident handling and information-sharing services to critical infrastructure sectors. According to ENISA, there are 38 CERTs that address critical infrastructure protection.[225] However, 32 of these provide support to the finance sector. In Norway, KraftCERT focuses on the energy sector. CERTSI in Spain responds to information security incidents in industrial control systems and provides services to relevant critical infrastructure. The national CERTs of Estonia, France, Belgium, Germany, Switzerland, Luxembourg and Finland include the protection of critical infrastructure in their service lists, according to information given by the accreditation and certification service of TF-CSIRT.[226]

The European Energy–Information Sharing & Analysis Centre (EE-ISAC), which was established by some European utility companies, academic institutions and governmental and non-profit organizations, constitutes a forum-type information-sharing platform for the energy sector in Europe.[227]

Norway, Sweden, Iceland, Finland, and Denmark established Nordic National CERT Collaboration in order to enhance a collective cyber incident response capability. Nordic Financial CERT is another cross-country cooperation platform, created by Nordic banks to fight cybercrime in the financial sector.[228] Nordic-Baltic Eight (NB8) is a high-level regional cooperation framework between Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden. Energy and cyber security are among the agenda items at its periodic meetings. In October 2014 Nordic countries held a tabletop exercise using the scenario of an energy shortage in the region.[229] Cyber-attacks against IT systems used for control and supervision of the link between Finland and Estonia were included as a component in this exercise.

Although KraftCERT may help improve incident handling capabilities in the Nordic grid, the national CERTs belonging to both grids are indistinguishable in terms of their contribution to critical infrastructure protection. EE-ISAC encompasses all European countries, and this does not create additional differences between the two grids. Members of the Continental grid have no information-sharing platform that specifically covers only that synchronous area. All information-sharing platforms in the Nordic region show that there is a strong culture of

[225] "CSIRTs by Country – Interactive Map", European Union Agency for Network and Information Security, accessed August 1, 2017, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

[226] TF-CSIRT Trusted Introducer, "Searchable Team Database".

[227] European Energy – Information Sharing & Analysis Centre, accessed August 1, 2017, http://www.ee-isac.eu/.

[228] "Press release: Nordic banks collaborate on fighting cybercrime", Nordea, last updated April 10, 2017, accessed August 1, 2017, https://www.nordea.com/en/press-and-news/news-and-press-releases/press-releases/2017/04-10-08h00-nordic-banks-collaborate-on-fighting-cybercrime.html.

[229] NordBER (Nordic Contingency Planning and Crisis Management Forum), *Energy shortage - Coordinated handling of a potential disturbance in the Nordic power system,* Reykjavik, September 9–10, 2015, http://www.energimyndigheten.se/globalassets/trygg-energiforsorjning/el/energy-shortage---co-ordinated-handling-of-a-potential-disturbance-in-the-nordic-power-system.pdf (accessed August 1, 2017).

collaboration between Nordic countries that includes cyber security activities. However, the contribution of these efforts to the cyber security of energy systems can appear limited due to the absence of a permanent formal cooperation framework. The small size of the Nordic grid is another factor limiting the benefit to be obtained from information-sharing between grid members.

All information-sharing platforms in the Nordic region show that there is a strong culture of collaboration between Nordic countries that includes cyber security activities.

5. Measures for the Transition Period

This section analyzes the dependence of the synchronization function on IT or OT systems and lists additional countermeasures that can be taken during the synchronization period. The interview with Elering and survey results obtained from Fingrid provided a significant input to this analysis.

According to the interviewed experts, the synchronization function requires the exchange of real-time system data for the purpose of frequency balancing between different members of the synchronization area. Estonia has AC power lines that connect the Baltic region with Russia. As Estonia is part of the IPS/UPS system, these lines actively form part of the synchronization of the Baltic region, as local system data is exchanged with the other parties. SCADAs in the control centers of Estonian and Russian TSOs share these data over a dedicated network connection by using an Inter-control Center Communications Protocol (ICCP) that runs on top of TCP/IP. Both sides run ICCP client and server modules that enable two-way data-sharing. There is no hierarchical relationship between the parties. Neither party has access rights to any kind of information system or industrial control assets of the other. Elering applies network-based countermeasures such as network segregation, network-based access control, intrusion detection, and antivirus control via two different unified threat-management devices. The availability requirements of these data are not well defined, and the interconnection is not included in business continuity plans. There is no formal agreement between Russia and the Baltic states about the security requirements of the exchanged data.

For synchronization, Finland exchanges system data with Norway and Sweden over dedicated network lines, which also have backup lines. Firewalls, intrusion detection, virus protection, and network segmentation are the security mechanisms used for network traffic carrying synchronization data. Fingrid conducts risk assessments that do not formally include the exchange of synchronization data.[230] Fingrid applies the availability requirement which, for the exchanged synchronization data, is 99.998%. Values for confidentiality, integrity and availability are determined nationally, but there is no region-level Nordic agreement on these values.[231]

Dependence of the synchronization process on IT or OT systems is solely limited to the exchange of local system data. The attack surfaces created by the synchronization function itself are minimal, as the data communication occurs over dedicated network lines and communicating parties do not require access privileges to the others' systems.

Increased scrutiny in the security monitoring of data exchange traffic, greater staff security awareness, and improved integrity controls in industrial control software are vital measures that should be applied during the desynchronization phase.

The synchronization function should be included in risk assessments and business continuity plans by all Baltic states. Increased scrutiny in the security monitoring of data exchange traffic, greater staff security awareness, and improved

[230] Survey response from Fingrid.

[231] Ibid.

integrity controls in industrial control software are vital measures that should be applied during the desynchronization phase. While synchronizing with the Nordic or Continental grids, it is important to review the establishment and maintenance of the interconnections between the new grid and the Baltic states from the perspective of cyber security. In order to foster common understanding about the asset values, risk assessment approaches, security responsibilities and relevant countermeasures, a security agreement should be signed before synchronization. NIST Special Publication 800-47 could serve as guidance for outlining such an agreement.[232]

Conclusions

In this chapter, the Continental and Nordic grids have been compared from the perspective of cyber resilience. Based on desk reviews of open sources and survey responses from some TSOs, the analysis was conducted on five levels: TSO, energy sector, critical infrastructure, national and grid-wide. As immediate connector states for the corresponding grids, Finland and Poland are the most important countries in this analysis. The comparison of Germany and Sweden also constitutes a significant input to the overall picture.

The evidence shows that there are no significant differences between the cyber resilience levels of Finnish and Polish TSOs. Although both countries have seen national-level improvements in the protection of critical infrastructure to some extent, more players – such as emergency management authorities, national CERT and R&D organizations – take responsibility in Finland. Finland conducts national and sector-based cyber security exercises more frequently. National programs are only weakly reflected in the energy sector in general and the electricity transmission sector in particular, which means both countries should establish sector-specific cyber security programs. Finland ranks higher in the Global Cyber Security Indexes for 2014 and 2017. Analysis of CyberGreen Institute data and Microsoft Security Intelligence Reports indicates that the Finnish network services have fewer vulnerabilities, and their websites host less malware. In addition, it is shown that Finnish network operators reacted more quickly in the event of Mirai attack.

Based on the limited information available in open sources, we could not identify any evidence of the superiority of either German or Swedish TSOs. Both countries have made significant improvements in their critical infrastructure protection. Germany has strong information security regulation and has established an information security authority with advanced capabilities. Sweden provides detailed guidance to the critical infrastructure companies rather than using legal instruments for enforcement. However, Germany's regulatory framework may help establish stronger organizational capabilities in critical infrastructure companies. Despite not having the same level of capabilities as its German counterpart, the Swedish authority, as the national contingencies agency, has the advantage of combining contingency management and cyber resilience responsibilities in one place, which may enable Sweden to deal with a serious national-level cyber crisis in a more coherent way. Both countries lack detailed sector-specific cyber security programs. Germany has a better position in the 2014 Global Cyber Security Index, while Sweden has a better score in the 2017 study. Analysis of CyberGreen Institute data shows that Germany has had fewer vulnerable devices in the SNMP and SSDP categories and fewer Mirai infections. The other important observation is that Germany has gradually decreasing results in all vulnerability groups except Mirai infections. Microsoft Security Intelligence Reports show that Sweden has lower ratios in the phishing and malware site categories.

Grid-level assessment shows that the average ranking of Nordic grid members is higher than members of the Continental grid in the 2017 Global Cyber Security Index. In spite of the fact that the Nordic region has a greater culture of collaboration, which has been also observed in the field of cyber security, existing crisis management and information-sharing practices lack a permanent formal cooperation framework.

[232] Tim Grance et al., *Security Guide for Interconnecting Information Technology Systems* (Gaithersburg, MD: National Institute of Standards and Technology, US Department of Commerce, 2002), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf (accessed August 1, 2017).

The national-level comparison between Finland and Poland demonstrates the relatively better situation in the former. However, the immaturity of both countries identified in our critical infrastructure and energy sector level analysis reduces the importance of this superiority. The analysis of Sweden and Germany does not indicate a clear difference between these countries. Nordic grid members have greater national-level commitments according to the grid-level comparison, but the members of both grids need to improve their cyber resilience at the levels of critical infrastructure, energy sector and TSOs. This study concludes, with some caveats, that the Nordic grid is a better option for the Baltic states from the perspective of cyber resilience.

The national-level comparison between Finland and Poland demonstrates the relatively better situation in the former. However, the immaturity of both countries identified in our critical infrastructure and energy sector level analysis reduces the importance of this superiority.

Conclusions and Recommendations

Emmet Tuohy
Tomas Jermalavičius
Anna Bulakh

As this report has sought to demonstrate, the choice between synchronous areas for the Baltic states goes beyond dimensions such as technical system characteristics or financial cost analyses. As a decision taken in a worsening geopolitical environment, it has *consequences* in those domains. The decision accordingly needs to be made with these potential consequences in mind – and ought ultimately to be aimed at joining a resilient synchronous area that represents an improvement on the status quo. In other words, it should bring the Baltic states into a synchronous area in which members are best able – and willing – to work to deter and respond to disruptions or attacks, even while themselves being subject to broader campaigns of influence designed to undermine their internal stability, societal coherence, and economic prosperity.

The choice between synchronous areas for the Baltic states goes beyond dimensions such as technical system characteristics or financial cost analyses.

After all, Ukraine has in a sense seen it all already, from physical disruption of critical infrastructure via attacks on electricity stations, to sophisticated cyber-attacks on its electricity grid, to disinformation efforts aimed at weakening public trust in government institutions.

These campaigns of influence are not the only risk to synchronization. Given the history that the Baltic states have with what Estonians euphemistically refer to as the *idanaaber* (eastern neighbor), as outlined above in Chapter I, anything from simulated accidents to outright invasion are not outside the realm of plausibility – depending on developments in the broader context of relations between Russia and the West as well as on Russia's internal dynamics. After all, Ukraine has in a sense seen it all already, from physical disruption of critical infrastructure via attacks on electricity stations, to sophisticated cyber-attacks on its electricity grid, to disinformation efforts aimed at weakening public trust in government institutions. Accordingly, the planners must factor the full spectrum of these potential developments into the synchronization decision – especially given the essential nature of an electricity grid to almost every area of modern human activity, from industrial production to healthcare services to communications and many more.

But how can we *measure* the risks to this resilient functioning – especially since "resilience" is a term now rather frequently used in different, often contradictory ways? In order to offer a recommendation on the choice of synchronous area on the most comprehensive basis possible, we measure and assess each region's degree of resilience across **five dimensions of resilience: external political, internal political, economic, physical,** and **cyber resilience.** Before sharing our assessments, let us first review which elements are included in each of these dimensions.

- **External political resilience** includes political commitments and national interests, policy towards Russia, bilateral relations with key players within a given synchronous area, and the ability of the EU/NATO to shape developments in a country or area.

- **Internal political resilience** refers to the degree to which a country or area exhibits good governance via institutions that follow the rule of law and that are protected from political interference. Additionally, this dimension assesses the degree to which radical anti-EU political actors are present in society – and the likelihood they can affect a state's decision to work with its EU partners. In this measure, we also include the extent to which Russia either already exercises or might subsequently choose to exercise influence over a state's decision-making.

- **Economic resilience,** in this report, includes both the overall state of energy markets and the energy sector in the relevant synchronous areas – including general aspects (e.g., the degree to which members of the area have supported the goal of a single EU energy market), technical aspects (e.g. the reliability of the proposed interconnectors as well as of the target grid itself), and finally issues such as the cost-effectiveness of the interconnection options and their impact on security of supply – aspects not explored in as much detail here as in the JRC and other cited studies, but that nonetheless need to be taken into consideration in the final analysis.

- **Physical resilience** refers to the ability to prevent or respond to kinetic attempts to disrupt or destroy synchronous interconnectors, including aspects such as maritime security in the Gulf of Finland (and the extent to which it is a "gray zone" in which states lack the situational awareness, capability or authority to act) and the vulnerability of the connectors in the Suwałki Gap linking Poland and Lithuania in a narrow stretch of land between Belarus and Russia's Kaliningrad exclave.

- **Cyber resilience** refers to the overall level of cyber security efforts both at a national and regional level, including more specific aspects such as present and planned activities by TSOs and other authorities to prepare against cyber-attacks on the electricity grids; the extent of cooperation within the synchronous area; and adoption of best practices such as the development of public-private partnerships.

Fundamentally, our main finding is simple: from the broad and multidimensional perspective chosen for this report, there is no ideal solution (except the one in which the Nordic and Continental areas are merged at some point, which would be an unrealistic expectation). This stems, first, from the geographical fact that the Baltic states, whichever of the two directions they choose, will remain a small peninsula in a larger synchronous area, connected to that area via a single particular country – Finland or Poland – and via a particular geographical domain (sea or land) each of which has strengths and weaknesses. Second, this finding also flows from the fact that both Finland and Poland – as well as the countries further "upstream" in each synchronous area – have their own understanding of the situation and of their interests, which may not necessarily align either fully or even partially with the interests and perspectives of the Baltic states. Indeed, there is a fundamental asymmetry of interests at play, with the three Baltic countries being eager to synchronize while the prospective partners at each end simply not perceiving as much interest or impact in the project, even if they are supportive (albeit according to their own conditions). Choosing either option will entail equally difficult bargaining, compromises, and trust-building. Third, neither of the two areas is a paradise or a promised land; while they have their own distinct advantages, they also contain various deficiencies and risks across all of the dimensions considered in this report. In Annex C, we summarize our analysis of these specific advantages, disadvantages and risks and also consider how likely that particular scenario is to occur, given the confluence of various circumstances.

Neither of the two areas is a paradise or a promised land.

Based on the findings and conclusions in each of the chapters, we also assigned certain values using a scale from 0 (complete absence of resilience) to 5 (complete resilience) to each synchronous area (see Annex D). In our judgement, all in all, the Continental synchronization option scores somewhat better compared to the Nordic option. However, this comes with an important caveat: our evaluation is based on a scenario in which two overhead lines connect the Baltic states with the Continental grid – an option seen as most preferable by almost every source consulted during the preparation of this report. However, the probability of this scenario is presently rather low, given how reluctant the current Polish government is to consider it. This position is determined by a variety of reasons – both explicitly stated and otherwise implied, such as the desire to protect domestic coal and electricity production, avoid higher financial costs and environmental impact, and the simple unwillingness to spend political capital on making this solution acceptable to affected local communities in the northeastern part of Poland.

Once the scenario is modified to reflect a one-line solution, the overall score of the Continental option becomes somewhat lower, particularly on the physical resilience dimension, as the synchronization linkage essentially loses redundancy. This would be troublesome even in the best of times, when adverse natural and other events almost routinely cause disruptions (as highlighted in Chapter IV); in a more challenging geopolitical environment marked by heightened tensions and a Russian strategy of pursuing hybrid warfare tactics, the one-line solution becomes even riskier. It could potentially amplify the impact of sabotage efforts and "active measures," from the psychological effect of a one-off attack immediately after synchronization to underscore a new area of vulnerability for the Baltic states and to discredit their strategic choice of desynchronization at one end of the spectrum, to creating or exploiting political tensions among the synchronization partners on the other.

There is a symbolic and intuitive side to this choice, one related to how the future of Europe is perceived.

The different advantages, disadvantages, and risks identified in this report and in other analyses will be weighed differently by different stakeholders of the synchronization process. Some will find the Russian threat and its attendant risk of sabotage, disruption, and coercion compelling enough to act with a great sense of urgency; others may treat it just as a theoretical possibility – notwithstanding our argument that it is important to take prudent measures to hedge even against possibilities that are merely theoretical in nature. Some are prepared to put more trust into a single thread connecting to a stronger (larger, more stable) synchronous area via a partner that is a NATO member with a robust attitude towards Russia but that is experiencing internal political resilience issues; others may prefer to rely on more numerous but harder-to-protect links to a weaker area via an internally resilient country that however is not a NATO member and that is very cautious about not antagonizing Russia. Some will find economic costs and benefits to be the most important aspects, while others may argue that it is worth paying a higher price – including for security capabilities – for the most optimal result. Last, but not least, there is a symbolic and intuitive side to this choice, one related to how the future of Europe is perceived. As one Nordic official observed, "if you hold the notion that the Nordics are going to be some island of tranquility in the midst of geopolitical turbulence, then [synchronization with the Nordic area] might be a good solution; but if you believe that your security lies with the EU as a whole, then the Continental area is the best option."

A two-line synchronous connection to the Continental area is a more robust solution which the Baltic states must work towards eventually implementing.

In our analysis, all selected dimensions of resilience carry equal weight; it confirms that a two-line synchronous connection to the Continental area is a more robust solution which the Baltic states must work towards eventually implementing. Compromising by agreeing to a one-line solution as a permanent (rather than a temporary stop-gap measure), or opting for the Nordic solution instead, carry additional risks of different kinds that we map in this report. Those risks would need to be carefully considered before going forward – and not just by electricity or energy policy experts, but by a much wider circle of decision makers. On the other hand, turning down the opportunity of a one-line Continental solution would entail operating in an isolated Baltic area for a very protracted period of time – probably between 2020 (when Russia becomes ready to desynchronize) and 2030 (the earliest time when the Nordic alternative might be ready). This significantly prolongs exposure of the Baltic states to Russia's coercive measures.

The Baltic states might end up in an isolated Baltic operation (a "Baltic island") by default, due to Russia's BRELLxit and/or Baltic disunity over the synchronization option.

Indeed, the Baltic states might end up in an isolated Baltic operation (a "Baltic island") by default, due to Russia's BRELLxit and/or Baltic disunity over the synchronization option. This might even be seen by some as an outcome preferable to the other scenarios considered here. However, as outlined above, we have chosen not to focus on this scenario both because of the findings of the earlier studies that this is a more expensive and less reliable solution. More importantly, that isolated operation is not in line with the European integration mindset and a well-established foreign and security policy paradigm of the Baltic states – one formed by the geopolitical imperative of "never alone" forged by the ever-present memory of the predicament faced by the three countries in 1940.

However, implementing the more robust Continental option does not come without its risks. These are risks that require action – or, at the very least, close and continuous attention. Given their nature, this attention and action is needed not only from TSO officials and energy policy actors, but also from diplomatic and security services as well as high-level political leaders. These issues to be monitored and addressed include:

- **Unity of the Baltic states.** Synchronization is not the first common infrastructure project undertaken by the Baltic states; just like the others, such as Rail Baltic(a), it is extremely vulnerable to delays caused by the absence of a common position. To counter Russia's "active measures" against the project, the Baltic states will have to act with unity, demonstrating a greater degree of urgency as well as respect and solidarity regarding each other's interests (e.g. regarding Lithuania's concerns about the Astravyets nuclear power plant in Belarus).

- **Political support for the Baltic synchronization project**. The Baltic states need to devote more effort to explaining their rationale (especially geopolitical and security aspects) for synchronization to the countries of the Continental area as well as to communicating their political concerns. This diplomatic outreach should focus particularly on the V4 countries and Germany. The Baltic states could leverage their participation in the Three Seas Initiative to broaden the base of support within the Continental area for their synchronization as a political and security project.

- **Bilateral relations between some members of the Continental area**. To avoid solidarity breakdowns in critical future circumstances, and to make it more difficult for Russia to utilize a "divide and rule" approach, it is not only the Baltic states that need to improve cohesion among themselves. Particular attention should be paid to the relations between Lithuania and Poland. The two countries must return to close strategic partnership and relationship of full mutual trust as well as appreciation of each other's value and importance to common regional security. Lithuania's claims to leadership on the synchronization project would be more credible and dependable if the country had focused more closely and intensely on developing a sound political and strategic partnership with Poland. It is in Estonia's and Latvia's fundamental interest to encourage and, if necessary, facilitate this rapprochement.

Particular attention should be paid to the relations between Lithuania and Poland. The two countries must return to close strategic partnership and relationship of full mutual trust.

- **Political developments in the Continental area.** For the Baltic states, it is important to monitor the developments and underline to their V4 partners that upholding the common values and principles enshrined in the treaties binding the EU together is a matter of maintaining the fundamental national

Upholding the common values and principles enshrined in the treaties binding the EU together is a matter of maintaining fundamental national and collective security interests.

and collective security interests of all these states; indeed, it goes to the heart of entire self-identification and integration effort by the Baltic states with the European and Euro-Atlantic space. While pursuing pragmatic solutions in the synchronization project, the Baltic states must not forget that, eventually, in implementing the Continental option they are deepening their security dependence and increasing their reliance for solidarity in crisis circumstances on actors who might often be not fully in tune with these fundamentals of integration. Balancing between realist policies and high principles will have to become part of diplomatic and political interactions with Warsaw – in energy security matters and well beyond – in ways that would not be the case with, for instance, Helsinki.

The "spotlight" on the Kremlin's intent and action must constantly maintained for the sake of public awareness across NATO and the EU – including, if necessary, "naming and shaming" of Russia's political influence agents.

- **Alertness to Russia's actions.** The diplomatic and intelligence services and political leadership of the Baltic states must remain alert to potential Russian actions directed against the synchronization project – and must be prepared to counter them. The "spotlight" on the Kremlin's intent and action must constantly maintained for the sake of public awareness across NATO and the EU – including, if necessary, "naming and shaming" of Russia's political influence agents working to deepen and exploit political, societal or economic vulnerabilities. Situational awareness and analysis would certainly benefit from closer cooperation on this issue among the three NATO Centers of Excellence hosted by the Baltic states (Cooperative Cyber Defense in Tallinn, Energy Security in Vilnius, and Strategic Communication in Riga) and Poland (Counter-Intelligence, in Kraków) as well as the European Centre of Excellence for Countering Hybrid Threats in Helsinki.

- **Physical security and resilience of interconnectors.** Even though the interconnector(s) to the Continental area cannot be made 100% safe against asymmetric kinetic actions, Lithuania and Poland should be strongly encouraged to treat critical infrastructure protection in the Suwałki Gap as a priority in their national assessments and in the subsequent development and deployment of their security (border, territorial, rapid response) capabilities. Additional attention is needed to prevent the illegal uses of UAVs across national borders and in the proximity of critical energy infrastructure. Physical security would also benefit from greater cross-border police, intelligence, and security information exchange and cooperation among the Schengen countries in the Continental area to prevent the abuse of freedom of movement and deployment of non-state proxies or special forces inside this area against critical energy (and other) infrastructure.

Lithuania and Poland should be strongly encouraged to treat critical infrastructure protection in the Suwałki Gap as a priority in their national assessments.

  - Physical resilience would be one of the benefits of an increased redundancy in synchronization infrastructure, i.e., of constructing the **second overhead interconnector** (LPL2) between Lithuania and Poland. However, this could be delayed or entirely torpedoed by Moscow's "active measures," which energize environmentalist and local not-in-my-backyard (NIMBY) movements – thereby substantially raising the political costs of the project to the national decision-makers in Warsaw.

Physical resilience would be one of the benefits of an increased redundancy in synchronization infrastructure, i.e., of constructing the second overhead interconnector.

This second line should, in other words, be pursued actively but also with due caution, in order not to create an environment in which Poland and the Baltic states end up in a bitter political confrontation in which various domestic and bilateral political sensitivities are unduly sharpened and perhaps further deepened by Russia's "active measures".

- **Cyber resilience.** Increased scrutiny in the security monitoring of data exchange traffic, greater staff security awareness, and improved integrity controls in industrial control software are vital measures that should be applied by the Baltic TSOs during the desynchronization phase. While synchronizing with Continental grids, it is important to conduct regular reviews of progress in establishing and maintaining the new synchronous interconnections from a cyber security perspective. In order to create common understanding about risk assessment approaches, security responsibilities, and relevant countermeasures, a cyber security agreement should be established within the ENTSO-E framework before synchronization.

- **Involvement of the European Commission**. Given the growth of Euroskeptic attitudes and political trends in Central Europe, a greater role of the Commission might seem to be a liability. However, there are very strong reasons to promote a greater role for Brussels in Baltic synchronization specifically, and fully support the Commission in implementing a range of broader policies and strategies:

  - The Commission's weight is necessary to **negotiate with Russia**, including debunking and defusing the issue of the alleged isolation of Kaliningrad, which Moscow seems to be inclined to use as instrument of suasion towards some EU capitals.

  - Continued development of the **Energy Union –** especially its first two priorities of ensuring diversity and security of supply, and of completing the integration of the internal European energy market – would harness the potential of the Baltic states to contribute to a low-carbon, sustainable energy future for the entire continent while helping to reduce their vulnerability to outside interference. Synchronization must continue to be seen as an important element of advancing this agenda.

  - Development of the EU as a **Security Union** with an emphasis on the security of external EU borders, counter-terrorism, cyber security, critical infrastructure protection, and resilience of vital services as well as police and intelligence cooperation, all of which is very pertinent to the Baltic synchronization project – i.e. protection of infrastructure from sabotage. The Baltic states should maintain their strong support for progress in building the Security Union and encourage their Polish partners to do the same, despite their common instinct to rely more on NATO and the United States in their national and regional security policies.

The Baltic states should maintain their strong support for progress in building the Security Union and encourage their Polish partners to do the same.

The Commission should have an extensive role in setting and monitoring common standards for cyber security and cyber resilience of critical energy infrastructure.

  - The Commission should have an extensive role in setting and monitoring common **standards for cyber security and cyber resilience of critical energy infrastructure**. The EU also needs to advance greater information sharing and cooperation concerning cyber security in general. The creation of a new EU Cyber Security Agency would be a very welcome step in developing more coherent approach across the ENTSO-E in this domain.

  - Created as an impartial guardian of the EU Treaties and the **rule of law** enshrined in them, the Commission clearly has an important role in ensuring that tendencies in the politics of some EU member

states do not undermine the framework of common values in which the four fundamental freedoms of the EU's single market are anchored. Good governance and respect for the rule of law are very pertinent to the operations of TSOs and the electricity sector. The rules of ENTSO-E on the management of emergency situations must remain insulated from whatever political trends manifest themselves in different member states. If there are any attempts to interfere and compromise this principle, the Commission should be prepared to take measures to guarantee the transparent and secure functioning of the electricity sector in general and of the operation of the synchronous area in particular.

Good governance and respect for the rule of law are very pertinent to the operations of TSOs and the electricity sector.

Defining and continuously reviewing the Alliance's role and options in supporting individual Allies in critical energy infrastructure protection (CEIP) against kinetic attacks must be part of preparedness planning.

- **Role of NATO.** The overhead synchronization interconnectors to the Continental area would lie entirely in NATO territory. Defining and continuously reviewing the Alliance's role and options in supporting individual Allies in critical energy infrastructure protection (CEIP) against kinetic attacks must be part of preparedness planning. The Baltic states and Poland would have to work to ensure that NATO's plans for the region include scenarios related to this infrastructure, particularly in order to deter escalation and larger scale destabilization. Closer NATO-EU cooperation in CEIP during crisis – blending the EU's civilian security and NATO's military capabilities to support Polish and Lithuanian authorities – would also be necessary.

- **Role of the Nordic countries.** Choosing the Continental option does not mean that the Baltic states are turning their backs on their Nordic partners. The Baltic states will remain part of the highly successful Nord Pool Spot electricity trading market and will continue to operate submarine asynchronous interconnectors to those countries. Economic resilience in crisis circumstances (e.g. severing of their interconnector[s] to the Continental area and temporary operation of their grids in isolated mode) would benefit from deepening this cooperation across the Baltic Sea. The Baltic states should initiate political and technical dialogue with their Nordic partners regarding the principles, procedures, and measures necessary for the effective use of the existing links in emergency situations.

Choosing the Continental option does not mean that the Baltic states are turning their backs on their Nordic partners.

- **Maritime capabilities investments.** To secure the use of the infrastructure outlined above, as well as that of other critical submarine infrastructure such as communication cables, the Baltic states cannot forever sidestep the question of how to enhance their maritime security and defense capabilities, even if the Continental option of synchronization is implemented. In the long term, given that countering hybrid threats predominantly remain a national responsibility, the Baltic states will have to become much more serious about their own Maritime Situational Awareness (MSA) and control/response capabilities of their civilian security agencies as well as militaries.

The Baltic states cannot forever sidestep the question of how to enhance their maritime security and defense capabilities.

- Addressing many of the above points could be seen as **"win-win" political, diplomatic, economic, security, and military investments**. Whether the Continental or Nordic option is chosen in the end, the overall security of the Baltic states will be considerably enhanced by the outlined measures. Successful synchronization in any form is contingent on the partners' trust in the Baltic states themselves – their internal and external political as well as economic resilience and responsible management of CEI and cyber security. In the era of hybrid threats, this is where it all starts and ends: on the home front.

Successful synchronization in any form is contingent on the partners' trust in the Baltic states themselves.

List of References

Introduction and Chapter I

Alcaro, Riccardo. *West-Russia Relations in Light of Ukrainian Crisis*. Rome: Edizioni Nuova Cultura & Istituto Affari Internazionali, IAI, 2015. http://www.iai.it/sites/default/files/iairp_18.pdf. Accessed September 8, 2017.

Brands, Hal. "Paradoxes of the Gray Zone". *Foreign Policy Research Institute*, February 5, 2016. https://www.fpri.org/article/2016/02/paradoxes-gray-zone. Accessed September 9, 2017.

Chivvis, Christopher S. *Understanding Russian "Hybrid Warfare" And What Can Be Done About It* [Testimony presented before the House Armed Services Committee]. Santa Monica: RAND Corporation, 2017. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf. Accessed September 8, 2017.

Crowley, Michael. "Putin's revenge". *Politico*, December 16, 2016. https://www.politico.com/magazine/story/2016/12/russia-putin-hack-dnc-clinton-election-2016-cold-war-214532. Accessed September 5, 2017.

Dayton, Keith W. "Director's Letter." *per Concordiam*, 8:2 (2017): 4. Accessed October 12, 2017. http://perconcordiam.com/perCon_V8N2_ENG.pdf.

Freedman, Lawrence. "Introduction." In *Strategic Coercion: Concepts and Cases*. Edited by Lawrence Freedman. Oxford: Oxford University Press, 1998, 1-14.

Friedberg, Aaron L. *The Authoritarian Challenge: China, Russia and the Threat to the Liberal International Order*. Tokyo: The Sasakawa Peace Foundation, 2017. http://www.spf.org/jpus-j/img/investigation/The_Authoritarian_Challenge.pdf. Accessed October 2, 2017.

Galeotti, Mark. *Crimintern: How the Kremlin Uses Russia's Criminal Networks in Europe*. London: European Council on Foreign Relations, 2017. http://www.ecfr.eu/page/-/ECFR208_-_CRIMINTERM_-_HOW_RUSSIAN_ORGANISED_CRIME_OPERATES_IN_EUROPE02.pdf. Accessed September 8, 2017.

Giles, Keir. *Russia's 'New Tools' for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, 2016. https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf. Accessed September 8, 2017.

Greene, James. "Russian Responses to NATO and EU Enlargement and Outreach". *Chatham House Briefing Papers*, June, 2012. https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Russia%20and%20Eurasia/0612bp_greene.pdf. Accessed September 8, 2017.

Grigas, Agnia. "Legacies, Coercion and Soft Power: Russian Influence in the Baltic States". *Chatham House Briefing Paper*, August, 2012. http://irsociety.org/wp-content/uploads/2014/09/Legacies-Coercion-and-Soft-Power-Russian-Influence-in-the-Baltic-States.pdf. Accessed September 8, 2017.

Gurzu, Anca. "Baltics threaten to unplug Russian region." *Politico*, April 11, 2015. https://www.politico.eu/article/baltics-threaten-to-unplug-russian-region-power-kaliningrad-electricity-interconnectors-lithuania-poland-sweden/. Accessed August 20, 2017.

Hansen, Flemming Splidsboel. *Russian Hybrid Warfare: A study of disinformation*. Copenhagen: Danish Institute for International Studies, 2017. http://pure.diis.dk/ws/files/950041/DIIS_RP_2017_6_web.pdf. Accessed August 16, 2017.

Healey, Jason, and Michelle Cantos. "What's next for Putin in Ukraine: Cyber escalation?" In *Cyber War in Perspective: Russian Aggression against Ukraine*. Edited by Kenneth Geers. Tallinn: NATO Cooperative Cyber Defense Centre of Excellence, 2015: 153-158. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Healey_Cantos_17.pdf. Accessed October 31, 2017.

Hoellerbauer, Simon. "Baltic Energy Sources: Diversifying Away from Russia". *Baltic Bulletin*, Foreign Policy Research Institute, June 14, 2017. https://www.fpri.org/article/2017/06/baltic-energy-sources-diversifying-away-russia/. Accessed September 12, 2017.

Holoboff, Elaine M. "Bad Boy or Good Business? Russia's Use of Oil as a Mechanism of Coercive Diplomacy". In *Strategic Coercion: Concepts and Cases.* Edited by Lawrence Freedman. Oxford: Oxford University Press, 1998, 179-211.

IDGC North-West МРСК Северо-Запада. "Приказ Министерства энергетики Российской Федерации «Об утверждении изменений, вносимых в инвестиционную программу ПАО «МРСК Северо-Запада», утвержденную приказом Минэнерго России от 30.11.2015 № 906»" [Decree of the Ministry of Energy of the Russian Federation "On the approval of changes made to the investment program of the public JSC 'IDGC North-West', passed by the decree of the Ministry of Energy of Russia No 906 on November 30, 2015]. December 16, 2016, accessed August 1, 2017. http://www.mrsksevzap.ru/cs/Satellite?blobcol=urldata&blobheader=application%2Funknown&blobheadername1=Content-Disposition&blobheadername2=MDT-Type&blobheadervalue1=inline%3B+filename%3DInvestitcionnaia_programma_na_2016-2025_gody.rar&blobheadervalue2=abinary%3B+charset%3DUTF-8&blobkey=id&blobtable=MungoBlobs&blobwhere=1384344669352&ssbinary=true.

Larrabee, F. Stephen, Stephanie Pezard, Andrew Radin, Nathan Chandler, Keith Crane, Thomas S. Szayna. *Russia and the West After the Ukrainian Crisis: European Vulnerabilities to Russian Pressures.* Santa Monica: RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1305/RAND_RR1305.pdf. Accessed September 8, 2017.

Lucas, Edward. "The Kremlin's 20 Toxic Tactics". *Europe's Edge*, October 30, 2017. http://cepa.org/EuropesEdge/The-Kremlins-20-toxic-tactics. Accessed November 1, 2017.

Lucas, Edward. *The Coming Baltic Storm: Baltic Sea Security Report*. Washington DC: Center for European Policy Analysis, 2015. http://cepa.org/sites/default/files/styles/medium/Baltic%20Sea%20Security%20Report-%20(2).compressed.pdf. Accessed September 8, 2017.

Lutsevych, Orysia. *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood*. London: Chatham House, 2016. https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2016-04-14-agents-russian-world-lutsevych.pdf. Accessed September 8, 2017.

Meister, Stefan. *Isolation and Propaganda: The Roots and Instruments of Russia's Disinformation Campaign*. Washington DC: Transatlantic Academy, 2016. http://www.transatlanticacademy.org/sites/default/files/publications/Meister_IsolationPropoganda_Apr16_web_0.pdf . Accessed September 8, 2017.

Oldberg, Ingmar. "Is Russia a status quo power?". UIPaper, No 1, 2016. https://www.ui.se/globalassets/butiken/ui-paper/2016/is-russia-a-status-quo-power---io.pdf. Accessed September 8, 2017.

Park, Donghui, Julia Summers, Michael Walstrom. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks". *The Henry M. Jackson School of International Studies (University of Washington)*, October 11, 2017. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/. Accessed October 31, 2017.

Praks, Henrik. *Hybrid or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics – the Case of Estonia*. Rome: NATO Defense College, 2015. https://www.icds.ee/fileadmin/media/icds.ee/failid/Henrik_Praks_-_Deterring_and_Defeating_Russia_s_Ways_of_Warfare_in_the_Baltics.pdf . Accessed September 8, 2017.

Rosseti Россети. "Совет директоров ПАО «Россети» принял ряд стратегических решений" [The Board of Directors of Rosseti adopted a number of strategic decisions]. June 10, 2016, accessed August 1, 2017. http://www.rosseti.ru/press/news/?ELEMENT_ID=26881&sphrase_id=301177.

"Russia Won't Re-Open Oil Pipeline, Lithuania Says". *Reuters*, October 11, 2007. http://uk.reuters.com/article/lithuania-russia-oil/russia-wont-re-open-oil-pipeline-lithuania-says-idUKL1159854520071011. Accessed October 5, 2017.

Sukhodolia, Oleksandr, Dmytro Bobro, Vytautas Butrimas, Jaroslav Hajek, and Sergii Karasov. *Hybrid Warfare Against Critical Energy Infrastructure: The Case of Ukraine.* Vilnius: NATO Energy Security Centre of Excellence (ENSEC COE), 2017 [forthcoming].

Tuohy, Emmet, Anna Bulakh, and Yuri Tsarik. *Desynch or Sink – A Political Analysis of Baltic Electricity Desynchronization*. Tallinn: International Centre for Defense and Security, 2017. https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Analysis_Desynch_or_Sink_Tuohy-Bulakh-Tsarik_May_2017.PDF. Accessed August 1, 2017.

U.S. Army Asymmetric Warfare Group. *Ambigous Threats and External Influences in the Baltic States. Phase 2: Assessing the Threat.* November, 2015. https://info.publicintelligence.net/AOWG-ThreatsBalticStates.pdf. Accessed September 12, 2017.

Chapter II

"Anti-immigrant Sweden Democrats Move into Second Place in Polls." *Reuters*, March 23, 2017. https://www.reuters.com/article/us-sweden-politics/anti-immigrant-sweden-democrats-move-into-second-place-in-polls-idUSKBN16U1NS. Accessed November 5, 2017.

"Baltics Agree on Grid Synchronization Via Poland". *The Baltic Times*, May 10, 2017. https://www.baltictimes.com/baltics_agree_on_grid_synchronization_via_poland/. Accessed November 4, 2017.

Booth, Michael. "Stop the Scandimania: Nordic Nations Aren't the Utopias They're Made Out to Be." *The Washington Post*, January 16, 2015. https://www.washingtonpost.com/opinions/stop-the-scandimania-nordic-nations-arent-the-utopias-theyre-made-out-to-be/2015/01/16/8f818408-9aa0-11e4-a7ee-526210d665b4_story.html. Accessed November 5, 2017.

Česnakas, Giedrius. "Energy Security Cooperation in the Baltic States: Lessons for the South Caucasus Region" in J. Novogrockiene and E. Siaulyte, editors. *Addressing Emerging Security Risks for Energy Networks in [the] South Caucasus*. Amsterdam: IOS Press, 2017.

Clemmesen, Michael H. "On Baltic Views of the Swedish Declaration of Solidarity," in *Friends in Need: Towards a Swedish Strategy of Solidarity with Her Neighbors*. Stockholm: Royal Swedish Academy of War Sciences, 2012.

Duxbury, Charles. "Sweden Ratifies NATO Cooperation Agreement." *The Wall Street Journal*, May 25, 2016, https://www.wsj.com/articles/sweden-ratifies-nato-cooperation-agreement-1464195502. Accessed November 20, 2017.

Elering. "The Baltic States' Integration to the EU Internal Electricity Market." Accessed November 20, 2017. https://elering.ee/baltic-states-integration-eu-internal-electricity-market.

– . *Eesti elektrisüsteemi varustuskindluse aruanne 2017* [Estonian electricity system security of supply report]. Tallinn, 2017.

Energinet, Fingrid, Statnett, Svenska Kraftnät. *Impact of Baltic Synchronization on the Nordic Power System Stability*. Sundbyberg, Sweden: Svenska Kraftnät, November 2016. http://www.svk.se/siteassets/om-oss/rapporter/impact-of-baltic-synchronization-on-the-nordic-power-system-stability.pdf. Accessed November 5, 2017.

"Estonia to Likely Support Alexela in Paldiski LNG Terminal Dispute." *The Baltic Times*, August 31, 2017-September 27, 2017.

Fingrid. "The proposal regarding a new balancing model made by the Swedish and the Norwegian transmission system operators conflicts seriously with Finland's national decision-making power and the goals of the European Union". June 9, 2017, accessed November 20, 2017. http://www.fingrid.fi/en/news/announcements/Pages/The-proposal-regarding-a-new-imbalance-settlement-model-conflicts-seriously-with-Finland%E2%80%99s-national-decision-making-power-.aspx.

Ilves, Toomas Hendrik. "Estonia As a Nordic Country." Speech at the Swedish Institute of International Affairs, December 14, 1999. http://vm.ee/en/news/estonia-nordic-country. Accessed October 30, 2017.

Jyrinsalo, Jussi. "Baltic Synchronisation towards Nordics: Is It a Real Alternative?". presentation at Elering Security of Supply Conference. Tallinn, Estonia, June 7, 2016.

Kragh, Martin and Sebastian Åsberg. "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case." *Journal of Strategic Studies* 40:6, October 2017: 773-816.

Martyn-Hemphill, Richard. "Finland, Estonia to Lobby Brussels for Gas Linkup." *The Baltic Times*, October 10, 2017. https://www.baltictimes.com/finland__estonia_to_lobby_brussels_for_gas_linkup/. Accessed November 20, 2017.

Purvins, Arturs, Gianluca Fulli, Catalin-Felix Covrig, Aymen Chaouachi, Ettore Bompard, Enrico Carpaneto, Tao Huang, Ren Jian Pi, Anna Mutule, Irina Oleinikova, and Artjoms Obushevs. *The Baltic Power System Between East and West Interconnections: First Results from a Security Analysis and Future Work*. Luxembourg: Publications Office of the European Union and European Commission's Joint Research Centre, 2016. doi: 10.2790/411653. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC100528/reqno_jrc100528_pdf.pdf. Accessed July 2, 2017.

Purvins, Arturs, Tao Huang, Shaghayegh Zalzar, Ren Jian Pi, Gianluca Flego, Marcelo Masera, Gianluca Fulli, Ettore F. Bompard and Angelo L'Abbate. *Integration of the Baltic States into the EU Electricity System: A Technical and Economic Analysis – Final Report (Executive Summary)*. Luxembourg: Publications Office of the European Union and European Commission's Joint Research Centre, 2017. https://publications.europa.eu/en/publication-detail/-/publication/8d3b7da2-562e-11e7-a5ca-01aa75ed71a1. Accessed November 5, 2017.

Rebane, Merike. "Elering: Baltikumi energiavõrgu autonoomset võimekust tuleks tugevdada" [Elering: The Baltic energy grid's autonomous capacity needs to be strengthened]. *Raamatupidamisuudised*, September 20, 2017. http://rup.ee/uudised/majandus-ja-ari/elering-baltikumi-energiav-rgu-autonoomset-v-imekust-tuleks-tugevdada. Accessed November 1, 2017.

Rees, Jasper. "Why the World Fell for Borgen." *The Daily Telegraph*, December 13, 2013. http://www.telegraph.co.uk/culture/tvandradio/10491255/Why-the-world-fell-for-Borgen.html. Accessed November 5, 2017.

Riigikogu. "Vitsut arutab Balti ja Poola kolleegidega transpordi ja energeetika küsimusi" [Vitsub discusses with the Baltic and Polish colleagues transport and energy issues]. October 1, 2017, accessed November 4, 2017. https://www.riigikogu.ee/pressiteated/euroopa-liidu-asjade-komisjon-et-et/vitsut-arutab-balti-ja-poola-kolleegidega-transpordi-ja-energeetika-kusimusi/.

Transparency International. "Corruption Perceptions Index 2016." January 25, 2017, accessed November 5, 2017. https://www.transparency.org/news/feature/corruption_perceptions_index_2016.

Tuohy, Emmet and Kristiina Visnapuu. Nord Pool Spot and the Baltic Electricity Market: *Difficulties and Successes at Achieving Regional Market Integration.* Tallinn: International Centre for Defense and Security, June 2015. https://www.icds.ee/publications/article/nord-pool-spot-and-the-baltic-electricity-market-difficulties-and-successes-at-achieving-regional-m/. Accessed November 8, 2017.

Tuohy, Emmet, Anna Bulakh, and Yuri Tsarik. *Desynch or Sink: A Political Analysis of Baltic Electricity Desynchronization*. Tallinn: International Centre for Defense and Security, 2017. https://www.icds.ee/fileadmin/media/icds.ee/doc/ICDS_Analysis_Desynch_or_Sink_Tuohy-Bulakh-Tsarik_May_2017.PDF. Accessed November 4, 2017.

Tuohy, Emmet. "Polluter or Partner: Estonian Energy Security & Climate Policy." Presentation at the European Climate Policies vs. Energy Security Strategy of Member States: Concerns and Contradictions conference. College of Europe, Warsaw, Poland, January 26, 2015.

Ummelas, Ott. "Baltics Need Own Grid as Russia Pulls Power Plug, Elering Says." *Bloomberg News*, July 4, 2017. http://www.taaviveskimagi.ee/2017/07/balti-riikide-elektrisusteemi-sunkroniseerimisest-euroopaga-intervjuu-bloombergile-08-06-2017/. Accessed November 4, 2017.

Vahtla, Aili. "Lithuania Mulling Power System Synchronization without Estonia, Latvia." *ERR News*, September 13, 2017. http://news.err.ee/618274/lithuania-mulling-power-system-synchronization-without-estonia-latvia. Accessed November 5, 2017.

– . "Minister: Lithuania Ready to Take Lead in Baltic Power Grid Synchronization". *ERR News*, October 2, 2017. http://news.err.ee/633806/minister-lithuania-ready-to-take-lead-in-baltic-power-grid-synchronization Accessed October 3, 2017.

Veskimägi, Taavi "Varustuskindluse tagab toimiv regionaalne energiaturg" [Security of supply is ensured by a functioning regional energy market]. Presentation at the Elering Security of Supply conference. Tallinn, Estonia, June 6, 2017.

– . "EL-i puhta energia paketi kaudu saab Eesti tõusta energiasüsteemide digitaliseerimise globaalseks liidriks" [Through the EU's clean energy package, Estonia can become a global leader in the digitization of energy systems]. *Eesti Päevaleht*, June 20, 2017. http://epl.delfi.ee/news/arvamus/taavi-veskimagi-el-i-puhta-energia-paketi-kaudu-saab-eesti-tousta-energiasusteemide-digitaliseerimise-globaalseks-liidriks?id=78619782. Accessed November 4, 2017.

Chapter III

Applebaum, Anne. "Germany's Election Gives the Country a Reality Check." *The Washington Post*, September 27, 2017. https://www.washingtonpost.com/news/global-opinions/wp/2017/09/24/germanys-election-gives-the-country-a-reality-check/?utm_term=.d6b0bbac00cd. Accessed October 5, 2017.

Balcer, Adam, and Paweł Zerka. *Hard Love, Actually: Polish-German Relations and a 'Multi-Speed' Europe – a View from Warsaw.* Warsaw: WiseEuropa, 2017. http://wise-europa.eu/wp-content/uploads/2017/03/170323-Hard-Love-actually.pdf. Accessed September 5, 2017.

Boffey, Daniel. "EU Will Hit Poland with Deadline to Reverse Curbs on Judicial Freedom." *The Guardian*, July 23, 2017. https://www.theguardian.com/world/2017/jul/22/eu-will-hit-poland-with-deadline-to-reverse-curbs-on-judicial-freedom. Accessed September 10, 2017.

Briançon, Pierre, and Joshua Posaner. "Angela Merkel and Emmanuel Macron rekindle German-French romance." *Politico*, July 13, 2017. https://www.politico.eu/article/angela-merkel-and-emmanuel-macron-rekindle-german-french-romance/. Accessed September 5, 2017.

Bugarič, Bojan. *Protecting Democracy and the Rule of Law in the European Union: The Hungarian Challenge.* London: The London School of Economics and Political Science, 2014. http://www.lse.ac.uk/europeanInstitute/LEQS%20Discussion%20Paper%20Series/LEQSPaper79.pdf. Accessed September 15, 2017.

Buras, Piotr, and Adam Barcel. "An Unpredictable Russia: the Impact on Poland." *European Council on Foreign Relations*, July 15, 2016. http://www.ecfr.eu/article/commentary_an_unpredictable_russia_the_impact_on_poland. Accessed September 5, 2017.

Buras, Piotr. "Europe and Its Discontents: Poland's Collision Course with the European Union." E*uropean Council on Foreign Relations*, September 2017, http://www.ecfr.eu/page/-/ECFR230_-_EUROPE_AND_ITS_DISCONTENTS_-_POLANDS_COLLISION_COURSE_WITH_THE_EU_.pdf. Accessed September 18, 2017.

Cunningham, Benjamin. "5 Takeaways from Slovakia's Elections." *Politico*, June 3, 2016. http://www.politico.eu/article/slovakia-fico-asylum-migrants-elections-nazi-nationalists/. Accessed July 25, 2017.

– . "Visegrád's Illusory Union". *Politico*, September 6, 2016. http://www.politico.eu/article/poland-hungary-czech-republic-slovakia-Visegrads-illusory-union-bratislava-summit-eu-migration-orban-fico-sobotka-szydlo/. Accessed July 25, 2017.

Day, Matthew. "Mass exodus of Polish army's top ranks in protest over political interference from government." *The Telegraph*, February 17, 2017. http://www.telegraph.co.uk/news/2017/02/17/mass-exodus-polish-armys-top-ranks-protest-political-interference/. Accessed September 15, 2017.

"Dialogue of the deaf between Vilnius and Warsaw." *The Economist*, February 10, 2012. https://www.economist.com/blogs/easternapproaches/2012/02/poland-and-lithuania. Accessed September 2, 2015.

Erlanger, Steven and Marc Santora. "Poland's nationalism threatens Europe's values, and cohesion." *The New York Times*, February 20, 2018. https://www.nytimes.com/2018/02/20/world/europe/poland-european-union.html. Accessed February 21, 2018.

"EU Should Drop Russia Sanctions, Slovak PM Says after Meeting Putin." *Reuters*, August 26, 2016. http://www.reuters.com/article/us-ukraine-crisis-slovakia/eu-should-drop-russia-sanctions-slovak-pm-says-after-meeting-putin-idUSKCN1111A1. Accessed August 26, 2017.

Grabbe, Heather, and Stefan Lehne. "Defending EU Values in Poland and Hungary." *Carnegie Europe*, September 4, 2017. http://carnegieeurope.eu/2017/09/04/defending-eu-values-in-poland-and-hungary-pub-72988. Accessed September 18, 2017.

Greenslade, Roy. "Polish journalists protest at state control of public broadcasting." *The Guardian*, January 11, 2016. https://www.theguardian.com/media/greenslade/2016/jan/11/polish-journalists-protest-at-states-control-of-public-broadcasting. Accessed September 15, 2017.

– . "Polish president urged not to sign controversial media law." *The Guardian*, January 7, 2016. https://www.theguardian.com/media/greenslade/2016/jan/07/polish-president-urged-not-to-sign-controversial-media-law. Accessed September 15, 2017.

Gressel, Gustav. *Fellow Travellers: Russia, Anti-Westernism, and Europe's Political Parties*. London: European Council for Foreign Relations, July 2017. http://www.ecfr.eu/page/-/ECFR225_-_FELLOW_TRAVELLERS1.pdf. Accessed October 5, 2017.

Groszkowski, Jakub. "Prime Minister Fico's Russian card." *OSW*, July 2015. https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-07-01/prime-minister-ficos-russian-card. Accessed August 25, 2017.

Győri, Lóránt, Péter Krekó, Jakub Janda, and Bernhard Weidinger. *Does Russia interfere in Czech, Austrian and Hungarian elections?* Budapest: Political Capital, 2017. http://www.politicalcapital.hu/pc-admin/source/documents/western_experiences_eastern_vulnerabilities_20171012.pdf. Accessed October 24, 2017.

Hegedűs, Dániel. The Kremlin's Influence in Hungary: *Are Russian Vested Interests Wearing Hungarian National Colors?* Berlin: DGAP, 2016. https://dgap.org/en/article/getFullPDF/27609. Accessed June 12, 2017.

Human Rights Watch. "Russia: Government vs. Rights Groups, Human Rights Watch." September 8, 2017, accessed September 10, 2017. https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle.

Karnitschnig, Matthew, and Jan Cienski. "Warsaw's EU spat stalls German-Polish engine." *Politico.eu*, January 14, 2016. https://www.politico.eu/article/warsaws-eu-spat-stalls-german-polish-engine-poland-government-media-law/. Accessed September 2, 2017.

Lassen, Christian Kvorning. "Russian Liaisons with the Czech Republic." *Charter 97*, May 16, 2016. https://charter97.org/en/news/2016/5/16/204504/. Accessed August 26, 2017.

Laurinavičius, Marius. "Time for a reset of Polish-Lithuanian relations?" *Europe's Edge*, December 10, 2015. Accessed September 2, 2017.

Lavinder, Kaitlin. "Are France and Germany the last hope for the EU?" *The Cipher Brief*, June 28, 2017. https://www.thecipherbrief.com/are-france-and-germany-the-last-hope-for-the-eu. Accessed September 2, 2017.

Lewicki, Grzegorz. "The Three Seas Initiative will strengthen Europe." Visegrad Insight, July 3, 2017. http://visegradinsight.eu/the-three-seas-initiative-will-strengthen-europe/. Accessed September 5, 2017.

"Lithuanian PM hails progress in relations with Poland." *The Baltic Course*, August 17, 2017. http://www.baltic-course.com/eng/baltic_states/?doc=132292. Accessed September 5, 2017.

Mesežnikov, Grigorij, and Radovan Bránik. *Hatred, Violence, and Comprehensive Military Training: The Violent Radicalisation and Kremlin Connections of Slovak Paramilitary, Extremist, and Neo-Nazi Groups*. Budapest: Political Capital, 2017. http://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_country_study_SK_20170428.pdf. Accessed July 25, 2017.

Meyer, Gabriel. "Putin Hiding Under a Czech Candle." *Daily Caller*, January 12, 2015. http://dailycaller.com/2015/12/01/putin-hiding-under-a-czech-candle. Accessed August 20, 2017.

Norwegian Helsinki Committee. *Full-fledged democracy under attack in Hungary*. September 30, 2013. http://www.osce.org/odihr/106129?download=true. Accessed September 15, 2017.

Overfield, Cornell. "Built to Last: Coalition Formation and German-Russian Relations after the Election," *Foreign Policy Research Institute*, October 2, 2017. https://www.fpri.org/article/2017/10/built-last-coalition-formation-german-russian-relations-election/. Accessed October 8, 2017.

"Politico Server: Babiš is Most Powerful Man in Czech Republic." *Prague Daily Monitor*, October 30, 2015. http://www.praguemonitor.com/2015/10/30/politico-server-babiš-most-powerful-man-czech-republic. Accessed August 29, 2017.

Rapoza, Kenneth. "How Washington is fighting for Russia's old Europe energy market." *Forbes*, May 2016. https://www.forbes.com/sites/kenrapoza/2016/05/17/washingtons-european-energy-security-boondoggle. Accessed July 30, 2017.

Rettman, Andrew. "Hungary veto sets scene for EU battle on Poland." *EUObserver*, December 21, 2017. https://euobserver.com/justice/140385. Accessed December 21, 2017.

Schenkkan, Nate. "PiS uses media control to bring Poland to heel." *Emerging Europe*, July 19, 2017. http://emerging-europe.com/voices/voices-politics/pis-uses-media-control-to-bring-poland-to-heel/. Accessed September 15, 2017.

Serhan, Yasmeen. "Hungary's Anti-Foreign NGO Law." *The Atlantic*, June 13, 2017. https://www.theatlantic.com/news/archive/2017/06/hungarys-anti-foreign-ngo-law/530121/. Accessed August 21, 2017.

Shuster, Simon. "How Russian Voters Fuelled the Rise of Germany's Far-Right." *Time*, September 25, 2017. http://time.com/4955503/germany-elections-2017-far-right-russia-angela-merkel/. Accessed October 24, 2017.

Stephens, Philip. "Viktor Orban's Hungary Crosses to Europe's Dark Side." *The Financial Times*, July 12, 2017. https://www.ft.com/content/2032f1c2-66e5-11e7-8526-7b38dcaef614. Accessed August 20, 2017.

Špalková, Veronika and Jakub Janda, *Activities of Czech President Miloš Zemanas the Kremlin's Trojan Horse*. Prague: European Values, 2018. http://www.europeanvalues.net/wp-content/uploads/2018/01/Activities-of-Czech-President-Milo%C5%A1-Zeman.pdf. Accessed January 29, 2018.

"The Lisbon Treaty, Article 2". Accessed August 21, 2017. http://www.lisbon-treaty.org/wcm/the-lisbon-treaty/treaty-on-european-union-and-comments/title-1-common-provisions/2-article-2.html.

Tsolova, Tsvetelia, and Pawel Sobczak. "In stinging attack, France's Macron says Poland isolating itself in Europe." *Reuters*, August 25, 2017. https://www.reuters.com/article/us-france-centraleurope/in-stinging-attack-frances-macron-says-poland-isolating-itself-in-europe-idUSKCN1B5128. Accessed September 2, 2017.

Wenerski, Lukasz and Michal Kacewicz. *Russian Soft Power in Poland: The Kremlin and pro-Russian organisations*. Budapest: Political Capital, 2017. http://www.politicalcapital.hu/pc-admin/source/documents/PC_NED_country_study_PL_20170428.pdf. Accessed August 26, 2017.

World Nuclear Association. "Nuclear Power in the European Union." Accessed September 10, 2017. http://www.world-nuclear.org/information-library/country-profiles/others/european-union.aspx.

Zaborowski, Marcin. "Poland's inward turn." *Visegrad Insight*, January 8, 2018. http://visegradinsight.eu/polands-inward-turn/. Accessed January 8, 2017.

Zalan, Eszter. "MEPs vote to start democracy probe on Hungary." *EUobserver,* May 17, 2017. https://euobserver.com/political/137943. Accessed September 15, 2017.

Chapter IV

ABB. "ABB NordBalt". Accessed June 28, 2017. http://new.abb.com/systems/hvdc/references/nordbalt.

Corera, Gordon. "Why intelligence sharing still has a long way to go." *BBC News*, January 1, 2016. http://www.bbc.com/news/world-europe-35154640. Accessed August 20, 2017.

De La Baume, Maïa and Giulia Paravicini. "Europe's intelligence 'black hole'." *Politico*, March 12, 2015. https://www.politico.eu/article/europes-intelligence-black-hole-europol-fbi-cia-paris-counter-terrorism/. Accessed August 20, 2017.

Elering. "Isolated Operation Study: The Isolated Operation of the Baltic States". Accessed July 5, 2017. https://elering.ee/en/isolated-operation-study-isolated-operation-baltic-states.

– . *Eesti elektrisüsteemi varustuskindluse aruanne 2017* [Estonian electricity system security report]. Tallinn, 2017. https://elering.ee/sites/default/files/public/Elering_VKA_2017.pdf . Accessed September 30, 2017.

ENTSO-E. "ENTSO-E Map". Accessed June 23, 2017. https://www.entsoe.eu/map/Pages/default.aspx.

– . *Nordic and Baltic Grid Disturbance Statistics 2015*. Brussels, 2016. https://www.entsoe.eu/Documents/SOC%20documents/Nordic/HVAC2015_2016_12_01.pdf. Accessed August 20, 2017.

– . *Nordic and Baltic HVDC Utilitisation and Unavailability Statistics 2014*. Brussels, 2015. https://www.entsoe.eu/Documents/Publications/SOC/Nordic/HVDC_Report_DISTAC_2015_10_27.pdf. Accessed August 20, 2017.

European Commission. *Joint Framework on Countering Hybrid Threats: a European Union response.* JOIN (2016)18 final. Brussels, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018. Accessed November 1, 2017.

Fingrid. *Nordel's Guidelines for the Classification of Grid Disturbances.* August, 2009. http://www.fingrid.fi/fi/voimajarjestelma/voimajarjestelmaliitteet/S%C3%A4hk%C3%B6n%20toimitusvarmuus/2015/Nordel_Guidelines_Classification_Grid_Disturbances_2009.pdf. Accessed July 2, 2017.

Government of Sweden. *Final reports on deepened defence cooperation between Finland and Sweden.* http://www.government.se/globalassets/government/dokument/forsvarsdepartementet/final-reports-on-deepened-defence-cooperation-between-finland-och-sweden.pdf. Accessed August 20, 2017.

Higgins, Andrew. "Increasingly Frequent Call on Baltic Sea: 'The Russian Navy is Back' ". *The New York Times*, June 10, 2015. https://www.nytimes.com/2015/06/11/world/europe/intrusions-in-baltic-sea-show-a-russia-challenging-the-west.html. Accessed August 10, 2017.

Huhtanen, Jarmo. "Suomi tilaamassa neljä uutta sotalaivaa 1,2 miljardilla eurolla – Tutkimusapua taistelualuksiin saatu USA:sta" [Finland to spend over €1.2 billion on four new ships to its fleet – the US has provided research help for combat ships]. *Helsingin Sanomat*, October 4, 2016. http://www.hs.fi/kotimaa/art-2000002923944.html. Accessed August 15, 2017.

International Institute for Strategic Studies. *The Military Balance 2016*. Abigdon: Taylor & Francis, 2016.

"Lithuania Plans Fence on Russian Kaliningrad Border". *BBC News*. January 17, 2017. http://www.bbc.com/news/world-europe-38635737. Accessed August 20, 2017.

"Lithuanian Military Allowed to Shoot Down Unwanted Drones". *Delfi*, September 13, 2017. https://en.delfi.lt/lithuania/defence/lithuanian-military-allowed-to-shoot-down-unwanted-drones.d?id=75744453. Accessed September 21, 2017.

"Lithuania-Sweden Power Link Offline Again Due to Cable Fault". *The Baltic Course*, February 14, 2017. http://www.baltic-course.com/eng/energy/?doc=127621. Accessed August 20, 2017.

LitPol Link. "Summary." Accessed July 2, 2017. http://www.litpol-link.com/about-the-project/summary.

Lyman, Rick. "Ukraine Crisis in Mind, Lithuania establishes a Rapid Reaction Force". *The New York Times*, December 19, 2014. https://www.nytimes.com/2014/12/20/world/europe/lithuania-assembles-a-force-as-it-readies-for-whatever-russia-may-bring.html. Accessed August 10, 2017.

McGrath, Bryan. "NATO at Sea: Trends in Allied Naval Power". *National Security Outlook*, No 3. Washington DC: American Enterprise Institute for Public Policy Research, 2013. http://www.aei.org/wp-content/uploads/2013/09/-national-security-outlook-no3-september-2013_1420494099.pdf. Accessed October 20, 2017.

Ministry of Energy of the Republic of Lithuania. "Electricity Link LitPol Link." Accessed July 2, 2017. https://enmin.lrv.lt/en/strategic-projects/electricity-sector/electricity-link-litpol-link.

Molis, Arūnas and Justinas Juozaitis. "Baltic Plug Into [the] European Electricity Network: Perspectives of Success". *Humanities and Social Sciences Latvia* 25:1, Spring-Summer, 2017. https://www.lu.lv/fileadmin/user_upload/lu_portal/apgads/PDF/Humanities_and_social_sciences_2017_1__internetam.pdf. Accessed July 12, 2017.

Murphy, Martin, Frank G. Hoffman, and Gary Schaub Jr. *Hybrid Maritime Warfare and the Baltic Sea Region.* Copenhagen: Centre for Military Studies, 2016. http://cms.polsci.ku.dk/publikationer/hybrid-maritim-krigsfoerelse/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf. Accessed August 1, 2017.

Murumets, Jaan. *Eesti Merejulgeolek: Uuringu raport* [Estonia's Maritime Security: Research Report]. Tartu: Estonian National Defense College, 2015. http://www.ksk.edu.ee/wp-content/uploads/2016/12/ossasional_5_avalik_veeb.pdf. Accessed November 13, 2017.

"New Finnish law prohibiting unidentified militia comes into force". *YLE*, July 15, 2017. https://yle.fi/uutiset/osasto/news/new_finnish_law_prohibiting_unidentified_militia_comes_into_force/9725169. Accessed August 20, 2017.

"Poland to Build Territorial Defense Force by 2019". *Deutsche Welle*, November 14, 2016. http://p.dw.com/p/2SffY. Accessed August 10, 2017.

Purvins, Arturs, Gianluca Fulli, Catalin-Felix Covrig, Aymen Chaouachi, Ettore Bompard, Enrico Carpaneto, Tao Huang, Ren Jian Pi, Anna Mutule, Irina Oleinikova, and Artjoms Obushevs. *The Baltic Power System Between East and West Interconnections: First Results from a Security Analysis and Future Work.* Luxembourg: Publications Office of the European Union and European Commission's Joint Research Centre, 2016. doi: 10.2790/411653. http://publications.jrc.ec.europa.eu/repository/bitstream/JRC100528/reqno_jrc100528_pdf.pdf. Accessed July 2, 2017.

Retmann, Andrew. "Security fears prompt fences on EU-Russia Border". *EUobserver*, August 28, 2015. https://euobserver.com/justice/130037. Accessed October 20, 2017.

Riigikantselei [State Chancellery]. *Riigikaitse arengukava 2017-2026* [National Defense Development Plan 2017-2026]. Tallinn, 2017. https://riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf. Accessed November 12, 2017.

Ronström, L., M. L. Hoffstein, R. Pajo, and M. Lahtinen. "The Estlink HVDC Light Transmission System". Presented at "Security and Reliability of Electric Power Systems", CIGRÉ Regional Meeting. Tallinn, Estonia, June 18-20, 2007. https://library.e.abb.com/public/c9f4e1c6068fb993c125731d004612b2/Estlink%20HVDC%20Light%20transmission%20system.pdf. Accessed June 28, 2017.

"Russia a 'risk' to undersea cables, defence chief warns." *BBC News*, December 15, 2017. http://www.bbc.com/news/uk-42362500. Accessed December 15, 2017.

Snyder, Jennifer, and Neil Rondorf. "About Submarine Power Cables". International Cable Protection Committee, November, 2011. https://www.iscpc.org/documents/?id=1755. Accessed August 2, 2017.

State Border Guard Service at the Ministry of the Interior of the Republic of Lithuania. Accessed August 22, 2017. http://www.pasienis.lt/index.php?1713774498.

Stoicescu, Kalev, and Henrik Praks. *Strengthening the Strategic Balance in the Baltic Sea Area.* Tallinn: International Centre for Defense and Security, 2015. https://www.icds.ee/fileadmin/media/icds.ee/failid/Kalev_Stoicescu__Henrik_Praks_-_Strengthening_the_Strategic_Balance_in_the_Baltic_Sea_Area.pdf. Accessed October 20, 2017.

The Finnish Border Guard. "The Border Guard in figures". Accessed September 4, 2017. https://www.raja.fi/facts/the_border_guard_in_figures.

Virbickas, Daivis. "Baltic Generation Adequacy 2017–2032". Litgrid, presentation, June 1, 2017. http://www.litgrid.eu/uploads/files/dir377/dir18/17_0.php. Accessed June 20, 2017.

Chapter V

50Hertz Transmission GmbH. *Annual Report 2016: A Successful Energy Transition – for a Sustainable World.* Berlin, 2016. http://www.50hertz.com/Portals/3/Content/Dokumente/Medien/Publikationen/2016/50Hertz_GB_Gesamt_E_Web.pdf. Accessed August 1, 2017.

Antonakakis, Manos, Tim April, Michael Bailey, Matthew Bernhard, Elie Bursztein, Jamie Cochran, Zakir Durumeric, J. Alex Halderman, Luca Invernizzi, Michalis Kallitsis, Deepak Kumar, Chaz Lever, Zane Ma, Joshua Mason, Damian Menscher, Chad Seaman, Nick Sullivan, Kurt Thomas and Yi Zhou. "Understanding the Mirai Botnet." 26th USENIX Security Symposium, 2017. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf. Accessed August 1, 2017.

Björck, Fredrik, Martin Henkel, Janis Stirna and Jelena Zdravkovic. "Cyber Resilience – Fundamentals for a Definition". In *Advances in Intelligent Systems and Computing*, Vol. 353, edited by Janusz Kacprzyk, 311–6. Springer, 2105. doi: 10.1007/978-3-319-16486-1_31, https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition. Accessed August 1, 2017.

BSA. "Country: Germany". *EU Cyber Security Dashboard: A Path to a Secure European Cyberspace*. London, 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_germany.pdf.

– . "Country: Sweden". *EU Cyber Security Dashboard: A Path to a Secure European Cyberspace*. London, 2015. http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_sweden.pdf. Accessed August 1, 2017.

– . *EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace*. London, 2015. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf. Accessed August 1, 2017.

CyberGreen Institute. Accessed August 1, 2017. https://www.cybergreen.net/.

Cybersecurity Foundation. "About Cybersecurity Foundation". Accessed August 1, 2017. https://www.cybsecurity.org/en/home-page/.

"Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union". *Official Journal of the European Union*, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.194.01.0001.01.ENG. Accessed August 1, 2017.

Energy Expert Cyber Security Platform. *Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector.* Report, February 2017. https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf. Accessed August 1, 2017.

Energy Security Portal. Accessed August 1, 2017. https://www.energisakerhetsportalen.se/.

European Energy – Information Sharing & Analysis Centre. Accessed August, 1 2017. http://www.ee-isac.eu/.

European Union Agency for Network and Information Security. "CSIRTs by Country – Interactive Map". Accessed August 2017. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

Federal Ministry of the Interior. *CIP Implementation Plan of the National Plan for Information Infrastructure Protection*. Berlin, 2005. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile. Accessed August 1, 2017.

– . *National Plan for Information Infrastructure Protection.* Berlin, 2005. http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf. Accessed August 1, 2017.

– . *National Strategy for Critical Infrastructure Protection.* Berlin, 2009. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP-Strategy.pdf?__blob=publicationFile. Accessed August 1, 2017.

Federal Office for Information Security. "Organisational Chart". Last updated September 14, 2017, accessed September 19, 2017. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/org_chart_IFG_pdf .

– . *The State of IT Security in Germany 2016.* Berlin, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3. Accessed August 1, 2017.

Finnish Communications Regulatory Authority. "CERT-FI service description (RFC 2350)". Last modified April 4, 2017, accessed August 1, 2017. https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices/cert-fi/rfc2350.html.

Finnish Information Security Cluster. Accessed August 1, 2017. http://www.fisc.fi/en/.

Fraunhofer Institute for Secure Information Technology. "Trusted Core Network: Hardware-based Security for Industrial IT Networks". Accessed August 1, 2017. https://www.sit.fraunhofer.de/en/tcn/.

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (Fraunhofer IOSB). *Annual Report 2015/2016*. Karlsruhe, 2016. https://www.iosb.fraunhofer.de/servlet/is/62654/ANNUAL-REPORT-Fraunhofer-IOSB-2015_2016.pdf . Accessed August 1, 2017.

"Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" [Law to increase the security of information technology systems (IT Security Act)], *Bundesgesetzblatt Federal Law Gazette*, No. 31, 2015, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start= //*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1506502999550. Accessed August 1, 2017.

Government Centre for Security. *The National Critical Infrastructure Protection Programme*. Warsaw, 2015. http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf. Accessed 1 August 2017.

Goździewicz, Wiesław, Cyprian Gutkowski, Lior Tabansky and Robert Siudak. *Security Through Innovation: Cybersecurity sector as a driving force in the national economic development.* Krakow: The Kosciuszko Institute, 2017. http://www.ik.org.pl/wp-content/themes/ik/report-img/security-through-innovation.pdf. Accessed August 1, 2017.

Grance, Tim, Joan Hash, Steven Peck, Jonathan Smith and Karen Korow-Diks. *Security Guide for Interconnecting Information Technology Systems.* Gaithersburg, MD: National Institute of Standards and Technology, US Department of Commerce, 2002. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf. Accessed August 1, 2017.

"Hackers may attack the energy sector. Poland is arming itself". *Business Alert*, June 14, 2017. http://biznesalert.com/hackers-may-attack-energy-sector-poland-arming/. Accessed August 1, 2017.

Healey, David, Sacha Meckler, Usen Antia and Edward Cottle. *Cyber Security Strategy for the Energy Sector*. Brussels: European Parliament, 2016. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf. Accessed 1 August 2017.

Holfeldt, Roger. "National Cyber Security Exercise (NİSÖ 2012): Conducting the exercise and main lessons learned." Swedish Civil Contingencies Agency (MSB), presentation, 2012. https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/roger-holfeldt-msb-sweden-the-national-cyber.pdf. Accessed August 1, 2017.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). *Cyber-attack Against Ukrainian Critical Infrastructure*. Alert (IR-ALERT-H-16-056-01). Washington DC, February 25, 2016. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01. Accessed August 1, 2017.

Informationssakerhet.se. "Stöd för systematiskt arbete med informationssäkerhet i organisationer" [Support for systematic work with information security organizations]. Accessed August 1, 2017. https://www.informationssakerhet.se/.

International Telecommunications Union. "Global Cybersecurity Index". Accessed August 1, 2017. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx.

ipaddress.live. "IP Address Range Usage in Finland". Accessed October 1, 2017. https://www.ipaddress.live/ip-address-finland.php.

– . "IP Address Range Usage in Germany". Accessed October 1, 2017. https://www.ipaddress.live/ip-address-germany.php.

– . "IP Address Range Usage in Poland". Accessed October 1, 2017. https://www.ipaddress.live/ip-address-poland.php.

– . "IP Address Range Usage in Sweden". Accessed October 1, 2017. https://www.ipaddress.live/ip-address-sweden.php.

JYVSECTEC. "JYVSECTEC Cyber Range: RGCE and solutions". Accessed August 1, 2017. http://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range1.pdf.

Kriz, Danielle. "Poland expands leadership role in cybersecurity". *Paloalto Networks Blog*, October 11, 2016. https://researchcenter.paloaltonetworks.com/2016/10/gov-poland-expands-leadership-role-on-cybersecurity/. Accessed August 1, 2017.

Laupichler, Dennis. "Smart Meter Gateway". B*SI Magazine* 1, 60–61, 2017. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Magazin/BSI-Magazin_2017-01.pdf?__blob=publicationFile&v=4. Accessed August 1, 2017.

Mattioli, Rosella, Konstantinos Maulinos. *Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors*. European Union Agency for Network and Information Security (ENISA), 2015. https://www.enisa.europa.eu/publications/maturity-levels/at_download/fullReport. Accessed August 1, 2017.

Media_OfficeDocument/_6ee7b656-3831-4b88-9473-bda78dfbc690&_t_hit.pos=3.

Microsoft Corporation. *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Finland*. Redmond, WA, 2017. http://download.microsoft.com/download/0/5/A/05AF93AF-BBF9-4754-B86A-2ACCA03610AC/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Finland.pdf. Accessed August 1, 2017.

– . *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Poland*. Redmond, WA, 2017. http://download.microsoft.com/download/C/B/0/CB0DB5F5-7D10-4538-9B7B-180F89A7F9C6/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Poland.pdf . Accessed August 1, 2017.

– . *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Germany*. Redmond, WA, 2017. http://download.microsoft.com/download/8/3/7/837488C4-D42D-47E5-820B-92DE154FDFD3/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Germany.pdf. Accessed August 1, 2017.

– . *Microsoft Security Intelligence Report Vol. 22, January through March 2017: Sweden*. Redmond, WA, 2017. http://download.microsoft.com/download/D/C/F/DCFD5A9E-98C2-4E91-8DB2-93E7385B93A9/Microsoft_Security_Intelligence_Report_Regional_Threat_Assessment_Sweden.pdf. Accessed August 1, 2017.

Ministerstwo Rozwoju [Ministry of Development], *Responsible Development Plan*. Warsaw, 2016. https://www.mr.gov.pl/media/14873/Responsible_Development_Plan.pdf. Accessed August 1, 2017.

Muurinen, Mira. "Continuity management is day-to-day work". *Fingrid – Corporate Magazine* 3/2014: 10–11. http://www.fingrid.fi/en/news/News%20liitteet/Magazines/2014/Fingrid_3_2014_EN.pdf. Accessed August 1, 2017.

"National Cybersecurity Center launched in Warsaw". *Radio Poland*, July 5, 2016. http://www.thenews.pl/1/9/Artykul/260202,National-Cybersecurity-Center-launched-in-Warsaw. Accessed 1 August 2017.

NordBER (Nordic Contingency Planning and Crisis Management Forum). *Energy shortage - Coordinated handling of a potential disturbance in the Nordic power system*. Reykjavik, September 9–10, 2015. http://www.energimyndigheten.se/globalassets/trygg-energiforsorjning/el/energy-shortage---coordinated-handling-of-a-potential-disturbance-in-the-nordic-power-system.pdf. Accessed August 1, 2017.

Nordea. "Press release: Nordic banks collaborate on fighting cybercrime". Last updated April 10, 2017, accessed 1 August 2017. https://www.nordea.com/en/press-and-news/news-and-press-releases/press-releases/2017/04-10-08h00-nordic-banks-collaborate-on-fighting-cybercrime.html.

Oehme, Richard. "Cyber security in Sweden – With focus on National Collaboration forum and of security of electricity supply". Accessed August 1, 2017. http://www.svk.se/siteassets/om-oss/remissvar/svenska-kraftnats-svar-pa-eu-consultation-paper-on-risk-preparedness-plans.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCfg==&_t_q=cyber&_t_tags=language:en, siteid:40c776fe-7e5c-4838-841c63d91e5a03c9&_t_ip=195.80.118.242&_t_hit.id=SVK_WebUI_Models_.

Polskie Sieci Elektroenergetyczne. "Certificates". Accessed August 1, 2017. http://www.pse.pl/index.php?dzid=178&did=1305.

– . *Development Plan for Meeting the Current and Future Electricity Demand for 2016-2025*. Konstancin-Jeziorna, 2015. http://www.pse.pl/uploads/kontener/Development_Plan_for_meeting_the_current_and_future_electricity_demand_for_2016-2025.pdf. Accessed August 1, 2017.

Puolustusministeriö [Ministry of Defense]. "Viides kansallinen kyberharjoitus järjestetään toukokuussa" [A fifth national cyber exercise will be held in May]. Last modified March 16, 2017, accessed August 1, 2017. http://www.defmin.fi/ajankohtaista/tiedotteet?9_m=8296.

Rinaldi, Steven M., James P. Peerenboom and Terrence K. Kelly. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies". *IEEE Control Systems Magazine*, December, 2001: 11–25. http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf. Accessed August 1, 2017.

Rossow, Christian. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse". Network and Distributed System Security Symposium, 2014. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/01_5.pdf. Accessed August 1, 2017.

Runsten, Jim, Ida Häggström and Vencel Hodák. "Cybersecurity". Synch Advokat AB, 2017. https://gettingthedealthrough.com/area/72/jurisdiction/38/cybersecurity-sweden/. Accessed August 1, 2017.

SPARKS – Smart Grid Protection Against Cyber Attacks. "Overview". Accessed August 1, 2017. https://project-sparks.eu/.

"Stuxnet: Computer worm opens new era of warfare". CBS News, June 4, 2012. http://www.cbsnews.com/news/stuxnet-computer-worm-opens-new-era-of-warfare-04-06-2012/. Accessed August 1, 2017.

Sutinen Heli. "Cyber Exercises for Operators in the Industry Sector was Piloted". *JYVSECTEC – Jyveskyla Security Technology*, February 21, 2017. http://jyvsectec.fi/en/media/. Accessed August 1, 2017.

Swedish Civil Contingencies Agency (MSB). "News from the Industrial Information and Control Systems Programme". Last modified June 19, 2017, accessed August 1, 2017. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-programmet-for-industriella-informations--och-styrsystem/Utbildningstillfallen-i-november/.

– . *Action Plan for Protection of Vital Societal Functions and Critical Infrastructures*. Karlstad, 2014. https://www.msb.se/RibData/Filer/pdf/27412.pdf. Accessed August 1, 2017.

– . *Guide to Increased Security in Industrial Information and Control Systems*. Karlstad, 2014. https://www.msb.se/RibData/Filer/pdf/27473.pdf. Accessed August 1, 2017.

– . *Handling Serious IT Incidents: National Response Plan, interim version, March 2011*. Karlstad, 2011. https://www.msb.se/RibData/Filer/pdf/26085.pdf. Accessed August 1, 2017.

– . "Private Public Partnership". Presentation, 2015. https://www.viestintavirasto.fi/attachments/esitykset/Richard_Oehme_Presentation_Fi_2015-11-04.pdf. Accessed August 1, 2017.

Swedish Defense Research Agency (FOI). "CRATE – Cyber Range and Training Environment". Accessed August 1, 2017. https://www.foi.se/en/our-knowledge/information-security-and-communication/information-security/labs-and-resources/crate---cyber-range-and-training-environment.html.

Svenska Kraftnät. *Svar på frågor i Consultation Paper on risk preparedness in the area of security of electricity supply*. D-nr: Svk 2015/1612, Ert d-nr: dnr M2015/2810/Ee. September 14, 2015. http://www.svk.se/siteassets/om-oss/remissvar/svenska-kraftnats-svar-pa-eu-consultation-paper-on-risk-preparedness-plans.pdf (accessed August 1, 2017).

– . *Annual Report for 2015.* Stockholm, 2016. http://www.svk.se/siteassets/om-oss/organisation/finansiell-information/annual-report_2015.pdf. Accessed August 1, 2017.

– . *Annual Report for 2016.* Stockholm, 2017. http://www.svk.se/siteassets/om-oss/organisation/finansiell-information/annual-report-svenska-kraftnat-2016.pdf. Accessed August 1, 2017.

TF-CSIRT Trusted Introducer. "Searchable Team Database". Last modified November 3, 2017, accessed November 3, 2017. https://www.trusted-introducer.org/directory/teams.html.

The Stockholm International Summit on Cyber Security in SCADA and Industrial Control Systems. October 23–26, 2017, accessed November 2, 2017. https://cs3sthlm.se/.

UP KRITIS. *Public-Private Partnership for Critical Infrastructure Protection*. Bonn, 2014. http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile. Accessed August 1, 2017.

Wessing, Taylor. "The German IT Security Law – Fact Sheet". Lexology, July 22, 2016. https://www.lexology.com/library/detail.aspx?g=0ca121a8-319f-4125-94cb-682d3a9343a4. Accessed August 1, 2017.

Vingerhoets, Pieter, Maher Chebbo and Nikos Hatziargyriou. *The Digital Energy System 4.0* (Smart Grids European Technology Platform, 2016). https://www.etip-snet.eu/wp-content/uploads/2017/04/ETP-SG-Digital-Energy-System-4.0-2016.pdf. Accessed August 1, 2017.

VTT Technical Research Centre of Finland Ltd. "Cyber Security". Accessed August 1, 2017. http://www.vttresearch.com/services/digital-society/cyber-security.

Annex A: Affiliations of Interviewees and Respondents to Requests for Information*

Belarus
Ministry of Energy

Czechia
Ministry of Industry & Trade
Ministry of Foreign Affairs
ČEPS a.s.
ČEZ Group

Denmark
Ministry of Climate & Energy
Danish Energy Agency
Energinet A/S

Estonia
Ministry of Economic Affairs & Communication
Ministry of Foreign Affairs
Estonian Defense Forces
Elering AS

Finland
Ministry of Economic Affairs & Employment
Finnish Defense Forces
University of Helsinki
Fingrid Oyj

Germany
Ministry of Foreign Affairs
Stiftung Wissenschaft und Politik (SWP)

Hungary
Budapest Institute of World Economy
Regional Center for Energy Policy Research (REKK)
MAVIR Zrt.

Lithuania
President's Office
Ministry of Energy
Ministry of Foreign Affairs
AB Litgrid
Vytautas Magnus University
NATO Force Integration Unit Lithuania
NATO Energy Security Centre of Excellence

Norway
Ministry of Foreign Affairs
Ministry of Petroleum and Energy (e-mail communication)
Statnett SF

Poland
Ministry of Energy
Ministry of Economic Development
Ministry of Foreign Affairs
Polskie Sieci Elektroenergetyczne S.A.
Forum Energii
European Border and Coast Guard Agency (FRONTEX)

Russia
Independent energy and political consultants
RusEnergy

Slovakia
Ministry of Economy (e-mail communication)
Slovenská elektrizačná prenosová sústava (SEPS), a.s. (e-mail communication)

Sweden
Ministry of Foreign Affairs
Ministry of Defense
Svenska Kraftnät

*Includes international organizations based in each country, as well as also individuals formerly affiliated with the listed national and international organizations (currently retired or employed in fields related to the studied subject matter). In total, 66 individuals were interviewed, in person or via email, or responded to our requests for information via email.

Annex B: Electricity Interconnectors to the Baltic States

Annex C: Summary of Advantages, Disadvantages, and Risks

Scenario	Advantages	Disadvantages	Key risks	Scenario probability
Continental Grid: 2-lines	(1) Coherence of memberships in security & defense organizations (NATO, EU) of key countries for synchronization; (2) Political heavyweights and drivers of European integration (esp. Germany, France) are part of the area; (3) Strong understanding of the synchronization issue in security terms by Poland and Poland's robust stance vis-a-vis Russia; (4) Relatively low cost, greater size and availability of security and defense capabilities for CEIP; (5) Strong market trading potential; (6) Size and stability of the grid; (7) The grid's experience with integrating new members; (8) Security and defense focus on the "Suwałki Gap" & external EU border in its vicinity; (9) Interconnectors confined to one domain (land) which is easier to control and protect than the maritime dimension; (10) Less time and lower cost of recovery in case of damage.	(1) Varying degrees of transparency, governance quality, cooperation across the area; (2) Polarized political environment, rise of populism and Euroskepticism in some key countries (V4, Germany); (3) Weakness of independent institutions and the rule of law in some key countries; (4) Russia's influence-building through politics and economy (incl. energy sector); (5) State interventionism and protectionist policies in Poland towards the electricity market; (6) Indifference to the issue of synchronization by countries further "upstream"; (7) Further investments required to strengthen interconnections between Poland and its neighbors as well as within Germany; (8) Lack of whole-of-society and whole-of-government approaches and cooperation in cyber security.	(1) Potential for worsening of Poland's bilateral relations (esp. with Lithuania, Germany) – possibly also due to Russia's "active measures" – which could affect solidarity during security crisis (i.e. low perceived value of defending synchronization interconnectors); (2) Significant deterioration of the political environment, institutions and rule of law in V4, thus increasing uncertainty about behaviors in crisis situations or creating a "security vs. common values" dilemma for the Baltic states; (3) Confrontations with the EU authorities driven by Euroskeptic attitudes, thus causing financial and political risk to infrastructure projects; (4) Russia's use of acquired influence and potential leverages to disrupt unity and crisis solidarity; (5) Potential intelligence & police cooperation failures in the Schengen area; (6) Physical attacks on interconnectors using drones, special forces, or proxies (e.g. organized crime); (7) NIMBY activation against infrastructure expansion (e.g. construction of the 2nd line).	**LOW** in the short to medium term, given the opposition of Poland. This could change to **HIGH** in the longer term in case of a change in policy by Warsaw and/or additional incentives/or political persuasion from the EU as well as from more market-oriented players in the area (Germany, some of the V4 countries).
Continental Grid: 1-line	-Same as **(1) to (4)** and **(6) to (8)** above, **plus** (1) Shortest time needed for synchronization, allowing the closing of the "window of vulnerability" without resorting to prolonged isolated functioning of the Baltic grid.	-Same as **(1) to (7)** above, **plus** (1) Restricted trading potential with the rest of the area; (2) Lack of physical resilience (redundancy) in linkages to the rest of the area.	-Same as **(1) to (6)**, **plus**: (1) Highly negative psychological and political impact of a one-off physical attack; (2) In case of constant disruption, resorting very frequently to isolated operation.	**MEDIUM**, given the reluctance of some synchronization players in Estonia and Latvia to endorse this option. It would become **VERY HIGH** should this be seen more widely in the Baltic states **as an interim step towards a 2-line solution** and a way to mitigate the impact of Russia's BRELLxit with a sense of urgency by all three Baltic capitals (and should no technical evidence emerge showing that this is an unsustainable solution).

Scenario	Advantages	Disadvantages	Key risks	Scenario probability
Nordic Grid	(1) Political stability, rule of law, transparency, and good governance (including strength of independent institutions and regulators); (2) Non-confrontational relations with EU authorities; full implementation of Commission regulations and directives; (3) Relatively low penetration by/and vulnerability to Russia's influence-building measures; (4) Strong Nordic security and defense cooperation, including Swedish-Finnish cooperation in the maritime domain; (5) Small size of the "community of practice" which facilitates trust-building, cooperation, and decision-making; (6) Market-friendly in terms of electricity trading, including the positive experience of the Baltic states' participation in the Nord Pool Spot electricity market; (7) Possibility to build resilience through redundancy (i.e. more than just 1-2 interconnectors); (8) Strong emphasis on digitization of the electricity sector management, which could produce economic benefits; (9) Strong commitment to the overall transition to a low-carbon economy with increased use of renewables and other green solutions such as Carbon Capture and Storage and emissions reductions; (10) Strong whole-of-society /public-private cooperation culture in cybersecurity.	(1) Membership incongruence in security and defense organizations (EU, NATO); (2) Non-aligned status of Sweden and Finland, as well as the latter's cautious management of its relations with Russia; (3) Absence of a security/ geopolitical perspective concerning the Baltic synchronization issue and low likelihood that undersea CEI connecting with the Baltic states would be a sufficiently high priority; (4) Overall lack of interest, even skepticism, concerning inclusion of the Baltic states into the area and the amount of effort and political capital that would be required to change that; (5) Absence of experience of integrating new members; (6) Lower frequency quality; (7) Difficulties (legal, technical, organizational) of controlling the maritime domain and ensuring adequate undersea CEIP, which adds to the challenges of CEIP in the land domain (the overland part of the undersea interconnectors); (8) Lack of national maritime civilian and military capabilities (especially in Estonia) and high cost of developing and maintaining them; (9) Insufficient attention to and presence of NATO / allied maritime capabilities in the Gulf of Finland in peacetime; (10) Long time and high cost required for recovery of damaged undersea infrastructure; (11) Longer timeline (i.e. longer exposure to the "window of vulnerability" after a potential Russian BRELLxit) and higher cost of synchronization.	-Same as **(5)** and **(6)** under "Key risks to the Continental Grid 2-line option", if targeted against overland parts of the submarine interconnectors, **plus**: (1) Russia's clandestine/ camouflaged naval action to damage submarine interconnectors in international waters; (2) Harassment of the repair ships in the international waters to delay recovery of submarine interconnectors; (3) Failure of the TEU and TFEU solidarity mechanisms or/and NATO Article 4 process if attacks on the undersea CEI are anticipated or occur but cannot be managed by national authorities; (4) Inaction of Finland or Sweden, which lack the back-up of the NATO Article 5 guarantee as an ultimate deterrent in case of crisis escalation to a military confrontation threshold, should the submarine synchronization interconnectors be targeted by Russia in international waters; (5) Creation of new additional vulnerabilities to cyber-attacks against CEI as the digitization agenda is implemented; (6) Russia's "active measures" to sabotage the project politically within the Baltic states and discredit it more generally in the Nordic countries during a prolonged "window of vulnerability" (until at least 2030); (7) Disruption to consumers stemming from the need to adapt to the lower frequency quality of the Nordic grid; (8) Synchronization project cost escalation due to the inexperience of the grid in terms of integrating new members; (9) Collapse of the Baltic unity and cooperation (including in other spheres), should this scenario continue to be regarded as preferable only in Estonia and Latvia.	**LOW**, given the lack of enthusiasm of the Nordics and Lithuania's opposition. Unlikely to change, **unless compelling technical evidence emerges** that a 1-line Continental option is impossible **and** the political agreement of Warsaw for a 2-line option remains beyond reach. Then this would become a **MEDIUM** probability scenario.

Annex D: Score Comparison of Synchronous Areas

Dimension	Continental Area	Nordic Area	Key reasons for a higher score for a given area
External political resilience	4	3	-NATO membership of countries at both ends of the synchronization link and the Alliance's deterrence/re-assurance effect; -Poland's strong policy vis-à-vis Russia and recognition of the security/geopolitical dimension of synchronization, willingness to support it; -Concentration of geopolitical "heavyweights" (Germany, France).
Internal Political Resilience	2	3	-Rule of law, transparency, good governance, (incl. independence of institutions such as judiciary and public media, low corruption); -Higher socio-political cohesion, lower prevalence of radical Euro-skeptic political actors and values; -Lower extent of penetration and influence by Russia through the internal political, economic and societal actors.
Economic Resilience	4	2	-Larger size, greater stability and frequency quality; -Larger integrated electricity market potential as part of the Energy Union; -Lower cost and greater speed of implementing synchronization; -Greater security of supply.
Physical Resilience	3 (2)*	2	-States' full authority over and better ability to control land domain, lesser extent of legal "gray zone"; -Confinement of security challenges to one domain (land) rather than two (land/maritime); -High attention to the Suwałki Gap from national governments and international authorities; -Less time and lower cost of detecting and repairing damage; fewer opportunities to obstruct or disrupt repair efforts.
Cyber Resilience	2	3	-Better-developed action plans for cyber security for energy sector and critical infrastructure; -More developed collaboration culture between state, public and private actors in cyber security; -Lower amount of malware-affected websites in key countries for synchronization; -Higher average scores in Global Cyber Security Index.
TOTAL	**15 (14)***	**13**	

Scale: from 0 (complete lack of resilience) to 5 (perfect resilience)
*In case of a one-line scenario

About the Authors

Hayretdin Bahşi

Hayretdin Bahşi received his PhD from Sabancı University (Turkey) in 2010. He was involved in many R&D and consultancy projects on cyber security as a researcher, consultant, trainer, project manager, and program coordinator at the Informatics and Information Security Research Centre of the Scientific and Technological Research Council of Turkey between 2000 and 2014. Currently, he is a senior researcher at the Centre for Digital Forensics and Cyber Security at Tallinn University of Technology. His research interests include critical information infrastructure security and cyber situational awareness systems.

Anna Bulakh

Anna Bulakh is a non-resident research fellow at the International Centre for Defense and Security, based in Kyiv. Her research areas cover energy security and regional security in the area of the EU's Eastern Neighborhood, particularly in Ukraine. Bulakh previously conducted research at the Prague Security Studies Institute. She completed the International Relations and European Integration training program for young diplomats, civil servants, and researchers from the Eastern Partnership countries at the Estonian School of Diplomacy before serving as a resident ICDS research fellow from 2013-2017. She holds an MA in Political Science and International Relations from University Fernando Pessoa in Porto, Portugal.

Tomas Jermalavičius

Tomas Jermalavičius is a research fellow and head of studies at ICDS. Prior to joining ICDS in 2008, he worked at the Baltic Defense College (BALTDEFCOL), first as deputy director of the College's Institute of Defense Studies in 2001-2004, and later as dean of the college in 2005-2008. In 1998-2001 and in 2005, he was a civil servant at the Defense Policy and Planning Department of the Lithuanian Ministry of National Defense. At ICDS, he focuses on the issues pertaining to defense policy and strategy, defense innovation, regional security cooperation and societal resilience. He holds a BA in political science from the University of Vilnius, an MA in war studies from King's College London, and an MBA degree from the University of Liverpool.

Artūras Petkus

Artūras Petkus joined the Strategic Analysis Division of the NATO Energy Security Centre of Excellence in 2015 as head of division. His main areas of responsibility are carrying out energy security related analysis on a strategic level; developing methodological and theoretical approaches for assessing energy security risks and threats; and contributing to the development of the NATO SACT Strategic Foresight Analysis Report as well as the Framework for Future Alliance Operations Report.

Nolan Theisen

Nolan Theisen is head of the Energy Program at the GLOBSEC Policy Institute in Bratislava (Slovakia). Before arriving at the Institute he worked for three years as an analyst at the Regional Centre for Energy Policy Research (REKK) in Budapest, handling projects from the public and private sector with a focus on the Central and Eastern European region. His areas of expertise include energy geopolitics, security of supply, regional market integration, gas infrastructure analysis, and EU renewable energy policy. Nolan received an MA in international economics with a focus on energy from the University of California in 2011.

Yuri Tsarik

Yuri Tsarik is co-founder of the Center for Strategic and Foreign Policy Studies in Minsk (Belarus) and head of its Russia Studies Program. Previously, he worked at the Information-Analytical Center of the President's Office and at the Ministry of Information of the Republic of Belarus. He was a Think Visegrád Fellow at the Institute of Foreign Affairs and Trade (Hungary, 2016) and a permanent Member of the Joint US-Russia Working Group on Afghan Narcotrafficking at the EastWest Institute (USA, 2015-2017).

Emmet Tuohy

Emmet Tuohy is senior research fellow at the Estonian Center for Eastern Partnership (ECEAP), where he focuses on political/strategic dynamics in the EaP countries, especially Ukraine and Moldova, as well as on the security and energy dimensions of the EU's Eastern Partnership program itself. Before moving to ECEAP, he served as a resident research fellow at ICDS – where he continues to contribute on a non-resident basis – and as associate director of the Center for Eurasian Policy at the Hudson Institute. He is a graduate of the School of Foreign Service at Georgetown University in Washington, DC.

Julia Vainio

Julia Vainio is an energy security expert at the NATO Energy Security Centre of Excellence in Vilnius, Lithuania. She joined the CoE in February 2017 as a Finnish representative. Vainio holds a master's degree in International Relations from the University of Turku. Her field of interest includes gas and electricity sector developments in the Baltic Sea region, geopolitical implications of energy transformations, and emerging threats in the field of energy security. Prior to joining the NATO ENSEC CoE, Vainio worked in academia.

Follow us on:
facebook.com/ICDS.Tallinn
Twitter: @ICDS _ Tallinn
linkedin.com/company/3257237

International Centre for Defence and Security
63/4 Narva Rd., 10152 Tallinn, Estonia
info@icds.ee, www.icds.ee

ISSN 2228-0529
ISBN 978-9949-9972-8-2 (pdf)