BALTIC SECURITY STRATEGY REPORT

What the Baltics Can Offer for a Stronger Alliance

Olevs Nikers and
Otto Tabuns, *Editors*

The JAMESTOWN FOUNDATION

Washington, DC
2019

THE JAMESTOWN FOUNDATION

Published in the United States by
The Jamestown Foundation
1310 L Street NW
Suite 810
Washington, DC 20005
http://www.jamestown.org

The Baltic Security Strategy Project was made possible by funding from the Baltic-American Freedom Foundation (BAFF). For more information about BAFF scholarships and speaker support, visit www.balticamericanfreedomfoundation.org. Additional support for the Project came from The Jamestown Foundation and the Latvian Political Science Association.

For more information on this book of The Jamestown Foundation, email pubs@jamestown.org.

ISBN: 978-0-9986660-5-1

Cover art provided by Peggy Archambault of Peggy Archambault Design.

Jamestown's Mission

The Jamestown Foundation's mission is to inform and educate policy makers and the broader community about events and trends in those societies which are strategically or tactically important to the United States and which frequently restrict access to such information. Utilizing indigenous and primary sources, Jamestown's material is delivered without political bias, filter or agenda. It is often the only source of information which should be, but is not always, available through official or intelligence channels, especially in regard to Eurasia and terrorism.

Origins

Founded in 1984 by William Geimer, The Jamestown Foundation made a direct contribution to the downfall of Communism through its dissemination of information about the closed totalitarian societies of Eastern Europe and the Soviet Union.

William Geimer worked with Arkady Shevchenko, the highest-ranking Soviet official ever to defect when he left his position as undersecretary general of the United Nations. Shevchenko's memoir *Breaking With Moscow* revealed the details of Soviet superpower diplomacy, arms control strategy and tactics in the Third World, at the height of the Cold War. Through its work with Shevchenko, Jamestown rapidly became the leading source of information about the inner workings of the captive nations of the former Communist Bloc. In addition to Shevchenko, Jamestown assisted the former top Romanian intelligence officer Ion Pacepa in writing his memoirs. Jamestown ensured that both men published their insights and experience in what became bestselling books. Even today, several decades later, some credit Pacepa's revelations about Ceausescu's regime in his bestselling book *Red Horizons* with the fall of that

government and the freeing of Romania.

The Jamestown Foundation has emerged as a leading provider of information about Eurasia. Our research and analysis on conflict and instability in Eurasia enabled Jamestown to become one of the most reliable sources of information on the post-Soviet space, the Caucasus and Central Asia as well as China. Furthermore, since 9/11, Jamestown has utilized its network of indigenous experts in more than 50 different countries to conduct research and analysis on terrorism and the growth of al-Qaeda and al-Qaeda offshoots throughout the globe.

By drawing on our ever-growing global network of experts, Jamestown has become a vital source of unfiltered, open-source information about major conflict zones around the world—from the Black Sea to Siberia, from the Persian Gulf to Latin America and the Pacific. Our core of intellectual talent includes former high-ranking government officials and military officers, political scientists, journalists, scholars and economists. Their insight contributes significantly to policymakers engaged in addressing today's newly emerging global threats in the post 9/11 world.

Table of Contents

Preface

Dear Reader,

The Baltic Security Strategy Project was launched to promote Baltic regional security and defense. To achieve this, the project aimed to promote a public discussion on Baltic security, foster synchronization of Baltic security and defense, maintain the issue of Baltic security on the agendas of Baltic allies and partners, as well as help Baltic security experts cooperate among themselves and with experts in the United States.

We brought together experts, professionals and scholars to assess the current state of security cooperation between the Baltic countries and issues we are facing together. In discussing these issues, we generated a set of recommendations for policymakers and produced a kind of roadmap to our strategic partners, NATO and EU.

Since February 2017, the project has held over a dozen public events on Baltic security, gathering 250 participants and 90 security experts, organizing panel discussions in Riga, Brussels, Stanford and Washington, DC, featuring a dozen Baltic and American security, involving five American interns and presenting the results to top decision and opinion makers across the Transatlantic sphere. The conclusions of this process, our findings and recommendations are included in this final report.

This report addresses challenges to Defense and Deterrence, Societal Security and Resilience, Economic Security, and Cyber Security. It focuses on solutions through intra-regional Baltic cooperation that also matter to wider regional security and the broader Transatlantic relationship.

The organizers of the Baltic Security Strategy Project wish to express their gratitude to their key supporters: the Baltic-American Freedom Foundation, The Jamestown Foundation, the US Embassy in Riga, the Association for Advancement of Baltic Studies, the Joint Baltic American National Committee and the Latvian Political Science Association.

In addition, as the project's organizers, we wish to express our gratitude to institutions that provided assistance or advice, and were represented at various project events throughout the last two years. These include the Baltic Assembly, the Saeima of Latvia, the US Congress, and the ministries of defense, foreign affairs, finance, culture and economy of Estonia, Latvia and Lithuania. We also extend our gratitude to the Baltic Defense College, the Riga Graduate School of Law, the National Defense Academy of Latvia, the Military Academy of Lithuania, the University of Latvia, Tallinn University, Texas A&M University and New York University. Furthermore, we wish to thank the Eastern Europe Studies Center at Vilnius University, the International Center for Defense and Security in Estonia, the Hudson Institute, as well as the Prague Security Studies Institute.

The analysis of Baltic defense was delivered by Mr. Glen Grant, Dr. Giedrius Česnakas, Mr. Anthony Lawrence, Col. (ret.) Zdzisław Śliwa, BGen. Ilmārs Lejiņš, Capt. Navy (Ret.) William Combes, Dr. Viljar Veebel, Ms. Ieva Miļūna, Mr. Edgars Poga, Mr. Illimar Ploom, Mr. Mr. Valdis Otzulis, Mr. Liudas Zdanavičius, Kaspars Druvaskalns, Mr. Edvards Seliška and Mr. Dainis Butners.

The analysis of Baltic societal security was delivered by Dr. Žaneta Ozoliņa, Ms. Kārina Pētersone, Mr. Jānis Kažociņš, Ms. Inita Pauloviča, Mr. Andris Mellakauls, Mr. Ēriks Kristiāns Selga, Mr. Edmunds Āķītis, Dr. Ivo Juurvee, Ms. Anne-Ly Reimaa, Ms. Dalia Bankauskaitė, Mr. Simas Čelutka, Ms. Rasa Zdanevičiūtė, Mr. Gatis Pelnēns, Mr. Edvards Seliška, Mr. Kaspars Druvaskalns, Mr. Mart Viires, Mr. Vytautas Keršanskas, Ms. Laima Zlatkutė, Ms. Alina Clay

and Ms. Gunda Reire.

The analysis of Baltic economic security was delivered by Dr. Giedrius Česnakas, Mr. Liudas Zdanavicius, Mr. Jako Reinaste, Mr. Gunārs Valdmanis, Dr. Tadas Jakštas, Mr. Juris Ozoliņš, Mr. Reinis Āboltiņš, Mr. Nerijus Kaucikas, Mr. Dainis Dravnieks, Mr. Osvaldas Šmitas, Mr. Karl Kull, Dr. Arunas Molis, Mr. Romas Švedas and H.E. Aušra Semaškienė.

The analysis of Baltic cybersecurity was delivered by Ms. Piret Pernik, Mr. Edgars Poga, Dr. Tadas Jakštas and Mr. Matthew Thomas.

We thank our experts, sponsors and friends for making this possible!

Olevs Nikers
Otto Tabuns

Introduction

In 2018, Latvia, together with its neighbors Estonia and Lithuania, celebrated its centenary. On the one hand, 100 years is not a particularly long historical period. But on the other hand, it can be considered a solid and useful benchmark for the existence of a country, allowing one to draw the most important lessons from its past and to highlight the achievements of human creativity, passion and commitment demonstrated therein over the years. At first glance, the history of all three Baltic States looks nearly identical. However, each of these nations had their own paths to democracy, stability and well-being. Estonia more decisively opts for competitiveness and openness to the world, and it most closely identifies itself with Northern Europe. Lithuania bears a long historical experience of having been entangled with Poland and the traditions of Central and Eastern Europe. While Latvia, because of its geographical location, believes it most thoroughly belongs to the Baltic Sea and the Baltic region. Despite those above-mentioned geopolitical divergences, one thing clearly ties them very closely together—security. If European history can be considered a history of wars, one can argue that the history of the Baltic States can be looked at through the lens of security.

The destinies of Estonia, Latvia and Lithuania are closely linked to gaining, losing and again re-gaining security. The countries that emerged on the map of Europe at the end of World War I achieved independence thanks to societal mobilization and the manifestation of values their societies were fighting for. The painful years of imperial domination and war were departure points, prompting a speedy recovery, which resulted in building up economic, political, social and military structures. The resulting societal security and stability lasted more than 20 years. However, the first two decades of history of all three countries lacks much evidence of comprehensive or active intra-

regional cooperation practices. In terms of security cooperation among these countries, this period proves that forming regional alliances is not an easy task. Negotiations that started among the Baltic States in early 1920 culminated in the formation of the Baltic Entente in 1934, but this format was not utilized as a security and defense policy tool because of increasing political and military tensions in Europe, as well as the Baltic trilateral grouping's own weakness. Despite the fact that Estonia, Latvia and Lithuania were active internationally and joined the League of Nations, regionally they failed to put forward initiatives that helped them strengthening their security in the long run.

During World War II, three subsequent occupations—beginning with the Molotov-Ribbentrop pact and culminating in the Baltic States' loss of independence after being annexed by the Soviet Union—became painful lessons about how difficult it is for small countries geopolitically located between two power blocs to preserve their sovereignty under pressure from two competing political systems. The Baltics' sovereignty could not be protected via the security policy that was chosen at that time: namely, neutrality. These lessons of history, which led to the suffering of millions of people in the Baltics, ended up driving the security thinking in Estonia, Latvia and Lithuania, after the three regained their independence at the beginning of the 1990s. The famous saying by Benjamin Franklin, "We must all hang together or most assuredly we will all hang separately," thus became a guiding principle for the Baltic States' security policies. That approach resulted in numerous intra-regional security cooperation projects, such as BALTBAT, BALTRON, BALTEFDCOL, BALTSEA, and many others. That strategic thinking in Estonia, Latvia and Lithuania, driven to a large extent by principles of cooperation, served them in preparation for NATO membership.

After joining the North Atlantic Alliance, the security policies of the Baltic States began to be seen first and foremost through a NATO perspective. Intra-regional cooperation lost its unique relevance and

became part of the wider Alliance's landscape. National security and defense policies transformed from classical self-defense to a combined approach—the Baltic States' national defense systems all contained a strong commitment to international peace and stability, which fostered more active participation in international missions and operations alongside other NATO member states.

But Russia's annexation of the Crimean Peninsula and war in eastern Ukraine was a wakeup call to the international community that the rules-based world order was suddenly being questioned. The events in Ukraine and Russia's open demonstration of aggressive behavior invigorated a wide debate in the West regarding how to adapt national security policies to meet the challenges of this new international environment. Russia exhibited overt military aggression against its neighbors twice within a short period of time—in 2008 in Georgia and in 2014 in Ukraine. In so doing, Moscow was asserting to the global community that international laws and norms, as well as political commitments are seemingly no longer relevant and that unilateral action has become one of Russia's security policy principles. The multiplication of threats, risks and challenges posed by a revanchist Russia, which repeatedly demonstrated willingness to engage in so-called "hybrid warfare" as well as apply military force as a tool to "protect compatriots" abroad, clearly indicated to its neighbors that they must reconsider their security policies.

NATO's speedy and resolute adoption of reassurance plans and the creation of Enhanced Forward Presence formations along the Alliance's eastern flank vindicated the Baltic States' decision in the 1990s to join the Transatlantic community's key political-military organization. Yet, at the same time, the destabilizing events in Ukraine, in 2014, raised questions regarding what should be the proper level of intra-regional cooperation in the Baltic area. One of these questions related to the efficiency of defense cooperation and whether the Baltic States coordinate and harmonize their policies and initiatives in such a way so as to most effectively strengthen the

security of their states and societies in a post-Crimea threat environment. Two prevailing opinions on this emerged. The Baltic States' official position was based on the assumption that NATO membership alone is sufficient; separate sub-regional cooperation efforts will not strengthen the security of the Baltic States, but just opposite—it will undermine joint efforts of the Alliance to deter potential future Russian provocations against those countries. Proponents of this argument point to lessons learned from history. The Baltic Entente of the late 1930s was not able, on its own, to protect the independence of Estonia, Latvia and Lithuania; therefore, any Baltic regional defense efforts should be integrally linked to broader NATO's policy. In contrast, some experts and members of the defense community in the Baltic States argued that regional cooperation needs to be utilized more efficiently and adapted to new security landscape.

There is no better way to assess the present situation of regional security cooperation in the Baltic States than by launching a wide, public debate with the participation of politicians, civil servants, representatives of non-governmental organizations and experts. The book *Baltic Security Strategy Report: What the Baltics Can Offer for a Stronger Alliance*" is a result of multiple consultations with a range of security policy stakeholders in order to diagnose regional cooperation in different security sectors and, in the end, to come up with a list of recommendations. The articles presented in this book should not be treated as results of academic research. They are designed as discussion papers that serve as a background for the discussions. Ideas presented in this book, thus, provide "food for thought" for the security and defense policy community. The composition of this collective study reflects the most relevant security sectors for the region: defense and deterrence, societal security and resilience, economic security, as well as cybersecurity. The value of these enclosed articles is in their interdisciplinary character and the diverse experiences of their authors, which enhances the quality of the recommendations. The book will be equally stimulating for researchers, as well as practitioners.

The beginning section of this volume focuses on defense and deterrence, which logically highlights the main priority of the national security policies of the three Baltic States. Glen Grant looks at existing Baltic defense cooperation projects, which underlie the broader benefits of regional cooperation at the political level. However, some of regional efforts could be enhanced, particularly at the operational level. He argues that it is necessary to "bind NATO C4I [command, control, communications, computers and intelligence] structures more closely to the three countries politically and organizationally for an evolving and developing crisis, not just providing NATO support after the problem occurs." He also suggests that the three Baltic States should consider other initiatives such as setting up a common intelligence center, a joint Baltic States Ammunition and Fuel agency, a robust air command and control capability, robust crisis management structures, create a lead nation concept, and many others. Additionally, Grant puts forward several key principles of the Baltic States' cooperation and coordination, which are "a visible deterrent to Russia through capabilities that improve resilience; better political and military management measures for times of crisis; and an actual improvement in military capability that is needed by all three countries and is politically and financially sustainable."

Vaidotas Malinionis discusses the issue of military interoperability. He argues that despite Estonia, Latvia and Lithuania having joined NATO 14 years ago, interoperability among their armed forces remains relatively low. Malinionis considers that a Regional Defense Strategy would help to bridge the existing gaps and improve the efficiency of national and, ultimately, regional defense capabilities.

Ieva Miļūna and Edgars Poga offer a comprehensive overview of the legal aspects of the Baltic States' military cooperation. The article looks at constitutional law in Lithuania, Latvia and Estonia, and questions whether "military cooperation between the three Baltic States is legally possible in the framework of institutional cooperation, common procurement, common maritime and air-defense patrolling

operations, and cross-border civilian cooperation."

The second group of articles is devoted to societal security and resilience. Ēriks Selga searches for models of "hybrid governance" as a means to mitigate hybrid threats faced by the Baltic States and specifically looks at cyber risks as one of the major challenges. Furthermore, he provides a valuable case study of the National Cyber Security Incident Response Teams in Estonia, Latvia and Lithuania, analyzing both their achievements and drawbacks. One of the conclusions Selga arrives at is the need for horizontal governance instead of vertical government.

A long list of disinformation case studies are offered by Dalia Bankauskaitė and Vytautas Keršanskas. All three Baltic States have been targeted by disinformation campaigns, and the authors look at a series of cases in recent years, starting with the infamous cyberattack on Estonia in 2007. However, it is worth pointing out that many others occurred before 2007. Indeed, the Baltic States have faced Russian disinformation campaigns from the very first days of regaining independence, in the early 1990s. Such assaults in the information space again became more active and visible shortly before EU and NATO enlargement, in 2004, as an attempt to hinder the Baltic States' accession to the both institutions. The article composed by Bankauskaitė and Keršanskas demonstrates the wide diversity of Russian disinformation campaigns; thus, the policy tools designed to mitigate their impact will need to be selected and implemented accordingly, depending on the individual case.

Edmunds Āķītis addresses an important but little investigated issue in the Baltic States—disaster risk reduction and urban resilience. He argues that the issue is becoming more relevant within the EU framework year by year, and the Baltic States are already part of this process. However, Āķītis notes, each country has its own perspective regarding capability assessments, and they lack a common approach. Disaster risk reduction and the capabilities to address it are scattered

across ministries, thus making regional cooperation in case of disasters more complicated and less efficient. He also argues that the role of society in risk reduction is currently not being fully considered, even though the participation of regular citizens in dealing with a crisis is one of the most decisive tools available to a government.

The third section of the book focuses on economic security. Economy is the driver of well-being for both society and the state more broadly. Without solid economic foundations, security cannot be sustained and implemented efficiently. Almost all countries across the globe are concerned about economic security. At the same time each country faces a unique set of elements of risks and threats to its economy. For the Baltic States, such sectors as energy, transport, finance and cyber realm are of particular importance in terms of strategic interests and resilience.

Energy security has long been a particularly sensitive issue due to the Baltic States' dependence on Russian energy resources. And regional cooperation has become recognized as one of the best tools to carry out the diversification of the three countries' energy sectors. Tadas Jakštas rightly reminds that the countries of the Baltic Sea Region have been highly active in building new infrastructure, fostering the integration of their energy markets, and increasing regional energy independence. At the same time, several obstacles have continued to hinder the overall integration process, such as "as data analysis and information sharing, as well as policy coordination, common training and exercises and a lack of understanding of regionalism that undermine regional energy developments." Jakštas puts forward a long list of recommendations, including, notably, the necessity of drafting a joint Baltic Security Strategy that addresses energy and economics.

Aivar Jaeski focuses on transport and infrastructure. Estonia, Latvia and Lithuania have been successful in implementing regional transport projects such as the Via Baltic highway. The present project

Rail Baltica could be considered another important regional initiative with broad security relevance. At the same time, however, there is a lack of "military criteria established and applied for commercial transportation and infrastructure areas in the Baltics," argues the author. He also points to the absence of a common regional perspective on how to develop joint resilience against different threats to Baltic transport networks and infrastructure.

Didzis Kļaviņš, in turn, analyzes the financial sector. All three states suffered from the effects of the global financial crisis of 2008. Recovery was painful for their societies and costly for the governments in terms of the austerity measures taken and their political implications. Kļaviņš identifies the main challenges in this sector, including the amount of non-resident deposits in Baltic banks, foreign direct investments from countries that have interests in strategically sensitive economic domains, and others. He underlines that financial control mechanism introduced by the EU, regional frameworks like the Nordic-Baltic Macroprudential Forum, and national policies can all help mitigate potential risks and increase financial security in the Baltic States as well as the region at large.

The fourth section looks at the least explored yet rapidly emergent domain of cybersecurity. Here, Edgars Poga focuses on various ways to build resilience into the Baltic States' cybersecurity sectors and analyzes the effectiveness of potential avenues of intra-regional cooperation in the cyber domain.

Do the Baltic States need a new strategy to boost regional security cooperation? My answer would be negative, since there are already numerous pre-existing frameworks within European and Transatlantic security architectures that provide for regional cooperation in different formats. But do the Baltic States need new strategic thinking on how to advance more efficient regional cooperation? Here my answer would be positive. The articles presented in *Baltic Security Strategy Report: What the Baltics Can*

Offer for a Stronger Alliance provide a long list of recommendations for how to proceed with more coherent, goal-oriented and efficient regional cooperation that will address the security of all three countries as well as Transatlantic community more broadly.

Žaneta Ozoliņa, professor at the University of Latvia

Looking Strategically at Baltic Security Cooperation

Olevs Nikers, Otto Tabuns

Security threats to the three Baltic States of Lithuania, Latvia and Estonia are at the highest level since the three countries became members of NATO in 2004. After regaining independence in 1991, their approach toward security—whether in the domains of defense, economics, or joining the European Union and the North Atlantic Alliance—stressed a joint regional effort. Yet, despite some successes, such as establishing the Baltic Defense College, a closer look at the three Baltic States' military planning and acquisition processes as well as their overall national security strategies reveals significant shortcomings to such joint efforts in addition to serious divergences in their approaches to security.

Mechanisms for fostering intra-regional military cooperation reached a high point in 1999, with the creation of the Baltic Battalion, consisting of military units of all three Baltic States. The BALTBAT would interact with NATO and be capable of out-of-area deployments. This unit was disbanded following NATO membership, although a new trilateral Baltic Battalion is now being formed within the NATO Response Force (NRF). For the most part, however, and particularly since joining the North Atlantic Alliance, each Baltic State has largely pursued a "go it alone approach" in terms of military defense planning.

Since February 2017, the Baltic Security Strategy Project has aimed to assess defense and deterrence, societal security and resilience, as well as economical security within the three Baltic States. The objective of the project is to gather top scholars and practitioners from across the

region and draft relevant policy recommendations for the use of Baltic and allied decision-makers on both sides of the Atlantic.

Beyond assessing what Latvia, Lithuania and Estonia have done and could do "from the inside," the recommendations are also aimed at the United States, NATO and the European Union for what they can do "from the outside." This external assistance may be crucial to fill the gaps in the security environment of the three Baltic countries and the surrounding region in ways that the Baltic States cannot fulfill by themselves. This approach should go hand in hand with understanding the benefits provided by policy options to the individual Baltic States and their strategic partners.

To address current shortcomings, our group launched a cycle of Seminars—a small pilot project in the fall of 2017 entitled "Effective Security Strategy Models: Lessons from the U.S. and Small States for the Baltics." This project consisted of a series of public seminars across the Baltic States aimed at assessing public interest in the problem outlined above.

Overall, the Baltic Security Strategy Project was implemented in two major stages, consisting of initial seminars across the Baltic States and meetings in Washington, DC, followed by a working group of professionals and experts convened to provide deep analysis of intra-regional defense and security issues.

Stage I

The impetus for this project began in September 2017, when Project Director Olevs Nikers, visited Washington, DC, as a Transatlantic Partnership Fellow. He had numerous meetings with House and Senate staff members on the Hill, members of the National Security Council, as well as several think tanks (Brookings, Heritage Foundation, RAND corp.), acquiring moral support for the project from across the US policymaking community.

One of the key outcomes of the pilot project was a realization that the Baltic States have potential partners in Washington, DC, and in Brussels (NATO & EU) who share these concerns and are eager to obtain more detailed insights into Baltic regional security arrangements in order to help the Baltic States engage in harmonizing their regional defense cooperation.

Following the success of the first set of private meetings, a series of seminars was organized across the Baltic States to discuss the US experience and that of small nations, such as Finland, after 1939 to the present, of developing their own security strategies. The seminars also examined future prospects for closer defense and security cooperation among the Baltic States.

The success of these seminars fostered broader public dialogue and engagement about these issues, as participants looked for ways to expand and continue these discussions into the future. A number of notable topics came up again and again during the Seminars. First, Finland, from whose past there is so much to learn, supports Baltic cooperation within the existing framework (non-NATO). Second, Lithuania stresses that its historical issues in the past with Poland and Germany is something that can be subject to manipulation, but this will not have any effect on collective security. Third Polish and German troops in Lithuania within the Enhanced Forward Presence (eFP) mission is strong proof.

Within the initial stage of the Project, we wanted, first of all to find good examples of defense and security strategy–making tools of other countries that could benefit defense and security planning in the Baltics (primarily the Net Assessment). Second—to capitalize on the widespread general public interest in the Baltic States by creating a broader public discussion on security, defense matters and intra-regional security. Third, as a result of these seminars, to bring to light a wide range of topics of debate and discussions among experts, professionals and academics across all three Baltic States; a new desire

emerged to find ways to address the common regional security challenges in a more concerted—that is, unified—manner.

During the seminars, participants examined key US defense analysis concepts developed by Andrew Marshall and the Office of Net Assessment in the Pentagon. These discussions examined how the Net Assessment concept might be applied to small countries. Key terms and concepts of the Net Assessment process were explored, particularly with regard to how states develop competitive strategies.

The Net Assessment approach permits the Baltic States to confront the frightening facts and figures about its opponent and instead paint a more holistic and realistic picture of what NATO could actually confront in the Baltic region. By instinctively characterizing the threat posed by Russia as a powerful giant, one can easily miss its "feet of clay." Such asymmetric weaknesses are often overlooked as countries estimate their opponents' power. Asymmetries, as well as historical perspectives, are particularly relevant to a potential unified Baltic security strategy.

Will the strengthening of Baltic security cooperation increase deterrence against Russia? Which defense instruments would be appropriate? Is this a road toward much more integrated armed forces of the Baltics or the creation of an individual Baltic Brigade? Is the institutional cooperation sufficient among the Baltic countries, and how can it be made more effective? Should there be any common strategy or more synchronized measures toward financial or cyber threats coming from the East? What about energy and the economy? What about joint procurements and military innovations and science? Should we make a single body of Net Assessment for the Baltics, or implement these tools separately in our countries?

The seminars included lecturers such as Mr. Paul Goble, former Special Advisor on Baltic affairs to the then Secretary of State, and Mr. Roger Robinson, Jr., former senior advisor of International Economic

Affairs to the National Security Council. More than 140 defense professionals, academics, experts, representatives of foreign missions and students participated in these events. Among participants of the seminars were representatives of foreign missions and members of parliament. Security advisor to the President of the Republic of Latvia, Mr. Jānis Kažociņš, participated in the final Seminar event.

Stage II and Method of Analysis

The aim of the second stage of this Project was to engage academics and professionals of the three Baltic States, the US and NATO into developing a tangible product, a study and policy recommendations within four major topics (domains of analysis): (1) Defense and Deterrence, (2) Societal Security and Resilience (3) Economic Security and (4) Cyber Security. According to the objective of the Project, during the second stage from March to December 2018, we developed joint academic and professional advice for decision-makers of the Baltic States (Parliaments and Ministers of Defense of the Baltic States). Simultaneously, this platform is aimed to improve the contents of national defense strategies of each Baltic State with an attempt to develop a more integrated, common military/defense strategy of the Baltic States.

During this stage, seven workshops (two times each per themes 1–3, and one in the Cyber Defense domain) of practitioners, scholars and experts in Estonia, Latvia and Lithuania was convened. The purpose of the panels were to establish a forum of professionals and practitioners (governmental and non-governmental) and scholars/experts from all three Baltic States and oversee their collaboration in two stages—(1) evaluating the status of security cooperation among Baltic countries and (2) developing recommendations for the decision-makers of the Baltic countries with regard to certain policy implementation proposals, as well as develop a publication.

Each workshop paired within one of those issue topics consisted of an "Initial" seminar addressing the problem and then a "concluding" seminar dedicated to discussing ways to solve the problem through practical trilateral cooperation (except for the Cyber Security Domain). Participants at the workshops included practitioners (governmental, non-governmental and private entrepreneurship), scholars and experts from Estonia, Latvia and Lithuania. At the conclusion of each of the seven workshops, a policy memo was written, based upon the key findings and conclusions reached by the workshop participants. Organization of the Workshops was conducted under the umbrella of the Latvian Political Scientists Association, in close cooperation with the Center for Security and Strategic Research at the National Defense Academy of Latvia and The Jamestown Foundation in the United States.

Experts and professionals from the three Baltic States were invited to submit their assessment papers prior to the initial workshop meetings and pre-recommendation papers prior to the concluding workshop. The content of these papers is reflected in this Report. Specifically, Experts were asked to provide answers to the following questions throughout the Project in their assessment and pre-recommendation papers within particular domains of analysis:

1. What is the current state of intra-regional cooperation?

2. What are the main issues of intra-regional cooperation?

3. What are the main gaps for intra-regional cooperation?

4. How you would assess institutional intra-regional cooperation?

5. What would you recommend to improve intra-regional cooperation overall and in the field of your expertise?

6. What are your suggestions to overcome major issues and gaps of intra-regional cooperation?

7. How should the existing mechanisms for intra-regional cooperation be utilized in the future?

8. What implications does enhanced intra-regional cooperation bring to the institutional interaction and allied partnerships?

On the one hand, the Baltic Security Strategy Project is looking backwards to the lessons learned and addresses challenges the Baltic countries will probably face in the future. As noted by Dr. Žaneta Ozoliņa, when speaking at the US Congress in December 2018, the Baltic States sometimes suffer from the "stereotype of triplets," whereby the outside world looks at them as three identical sisters or brothers. But these are three individual countries with their own interests and concerns. However, there are lot of issues that tie the Baltics together, foremost of which, unfortunately, are their shared threat environment and similar threat perceptions.

* * *

Numerous earlier studies on Baltic cooperation predate this particular Project. Yet, what sets our approach apart is that it does not rely exclusively on Latvians writing about Latvia, Estonians about Estonia and Lithuanians about Lithuania. Rather, it seeks to cover a broad swath of security domains, and each of the participating experts considers the issue of Baltic cooperation from his or her own unique angle. Until now, whenever Baltic cooperation was discussed, the remedy to any and all obstacles would inevitably be, "let's have more cooperation." But this project is not about just pushing additional cooperation; it is about strengthening existing cooperation by building different partnerships as well as links with the Transatlantic Community and the United States in particular

1. DEFENSE AND DETERRENCE

1.1. Expert Assessment

Olevs Nikers, Otto Tabuns, Anthony Lawrence, Zdzisław Śliwa, William Combes, Glen Grant, Giedrius Česnakas, Viljar Veebel

The Baltic States (B3) face credible military security challenges. Compared to the neighboring Russian forces in the Western Military District and the Kaliningrad exclave, the militaries of the individual Baltic States are at a disadvantage when it comes to manpower as well as the quantities of their arms, airspace protection and naval fleets. For these reasons, the North Atlantic Treaty's (NATO) Enhanced Forward Presence (eFP) multinational battalions operating in the Baltic States and Poland play a key strategic role as a deterrence measure. The deployment of allied troops in the Baltic States strengthens the security and deterrence capabilities of both the regional countries and the broader Alliance.

The core military security problem for the Baltic States is the lack of cooperation and coordination between these states. The three countries have three different models of military. Not all Baltic States have military attachés in one another's capitals. Intra-regional cooperation on arms procurement is yet to show success. Illustratively, the Baltic States recently failed to agree to purchase air-defense systems jointly and ended up fielding three separate systems.

This indicates just one of the areas where lack of defense coordination translates into missed opportunities, despite consensus among the majority of project experts that any attack on the Baltic States would be unlikely to single out any one of them—rather all three would

targets of aggression. Despite generally being perceived as one unified region, whether by the United States, NATO, the European Union or Russia, the Baltics themselves are often unable or unwilling to act as one or plan their defense accordingly. Their individual plans are unlikely to be cost effective. While distrust at the top political and military levels among them prevents deeper cooperation in security matters.

To date, the Baltic States have largely sought cooperation with bigger allies in the wider Baltic region, rather than amongst themselves. Lithuania has prioritized military cooperation with Poland, as the latter plays a strategic role in protecting the free passage through the Suwałki corridor for all the Baltic States and Germany. Estonia, meanwhile, maintains strong political and military cooperation with Finland, which is not a NATO member. The drive to partner with allies outside the immediate region is rational, as they have more capabilities and greater power than all three Baltic States combined.

Currently, the Baltics are focused on the development of their land forces, while air forces, except for air-defense systems of different levels, and navies are neglected. This might create significant problems during a conflict as it will be difficult to ensure the successful arrival of allies to the region. Military cooperation becomes more successful when decisions are taken at the NATO level. This suggests that an actor wielding more powerful resources and defense capabilities is instrumental to bringing about cooperation between the Baltic States.

In order to understand better where we stand and why, we have to look at the past two decades. From the outset, we have to acknowledge that defense cooperation among the Baltic States has actually been quite close since the early 1990s. This is due to historical reasons—1) lessons learned from the 1930s and 1940s; 2) self-portrayal and thus perception in West of three states as one item; and 3) the common political-military path chosen in the mid-1990s to join Euro-Atlantic

institutions. This internal willingness was coupled by an important factor—unwritten "rules" from outside—if the Balts want to be members of "the club," there are a set of regional actions that must first be accomplished do. This dual approach was continued in the 2000s—focusing on international solidarity as well as far-away expeditionary operations—fully integrating into the military-political problems of that time while maintaining their joint position as a means to access NATO. Overall, the Baltic States managed to absorb maximum benefits from that period—both in preparing their military personnel (fighting abilities, cooperation with other Allies, knowledge of the planning process, etc.) and politically. We managed to create two layers of cooperation (and they still do function)—political-operational as well as practical. At the practical level the three Baltics States developed a joint air-surveillance system BALTNET, common counter-mining Baltic Naval Squadron (BALTRON), as well as a Baltic Battalion (BALTBAT) unit that took part in or was on stand-by every four years with the NATO Response Force. Moreover, our senior and highest officers, together with other allied and Partnership for Peace (PfP) forces, are upgrading they knowledge at the Baltic Defense College (BALTDEFCOL). Military units participate in each other's national exercises.

At the political level, there are issues related to the above-mentioned projects as well as relations with allies. The delivery of joint messages is constantly being discussed among the Baltic States' ministers, chiefs of defense/chiefs of staff, policy directors, commanders of all services, as well as special operations forces (SOF) and voluntary force commanders, who hold meetings at least twice per year. The system is both vertical and horizontal; questions of smaller significance are resolved "on the spot," while more important issues are pushed "up the ladder" to higher decision-making levels. A good practical example of this process is the quick exchange of information among the B3 regarding cyber incidents and even perceived preparations for a cyberattack on information systems and networks. These were high achievements for requirements of that time.

At the beginning of the 2010s, the Baltic States found themselves in deep financial and socio-economic crises, and defense was one of the first areas to be cut back. But fortuitously, at that time, Russia was not actively prodding for weaknesses in the Baltic States, as it was preoccupied with other regions, and economically was doing rather well. Latvia's defense establishment showed particular resilience during the gradual recovery, undertaking the start of mechanization of the army (one of basic needs for all land force–oriented countries). At the same time, the B3 realized they needed to have deeper operational-level harmonization allowing for a gradual synchronization of national defense plans; hence, they established a Baltic Combined Joint Staff element (non-permanent), where intelligence, planning and logistical specialists can work together.

The regional security environment changed drastically in 2014, with Russia's invasion of Ukraine. The Kremlin saw Ukraine as its "internal issue" and the West (both Europe and the United States) as weak, and thus unlikely to react. The latter's unified condemnation and passage of gradually escalating responses, therefore, surprised Moscow to some extent. Regardless, the West believed Russia might not stop with just its intervention in Ukraine and accepted the Baltic States' narrative about Russian intentions. As a result, NATO quickly undertook reactive steps, including enforcing the Baltic air policing mission in spring 2014–although this was primarily a political signal. For their part, the B3 re-concentrated their resources on enabling enhanced NATO presence on their territory.

Russia mistakenly did not fully understand the dynamics driving decision-making in NATO and the Baltic States. At the same time, and regardless of Russian actions, the financial situation in the region soon started to rebound, allowing for an influx of new resources (even overtaking the pre-crisis defense budgets). This process was sped up by political-military events in the region set in motion by Russia's invasion of Ukraine. The demonstrated resilience by the Baltics and their Allies have halted any possible further Russian aggressive or

expansionist ambitions. This Alliance resilience is now easily visible by, for example, the fact that NATO members persistently train with Baltic troops (via the eFP mechanism).

The Baltic States, meanwhile, need to understand that it took (and still is taking) time to change the political thinking in Western countries sufficiently to convince their governments to agree to deploy trip-wire forces in the Baltics. Militarily, both allies and the Baltics themselves see such localized force presence in very practical terms—as steady, tactical, operational training of units, and interoperability of equipment. *Inter alia*, taking into account the renewed growing importance of non-military instruments (economic, informational, etc.), it helped to overcome the thinking that Western allies might choose to strike a deal with the Russians "behind the Baltic States' backs." The Baltics' defense agendas over the past several last years have been absolutely intertwined with larger NATO issues—realistic plans, the necessity for cross-border activities (both in peace time and crisis time) inside allied territory, allied presence and projects in the Baltic States, and so on. As such, there are no pure "national" exercises anymore—all are now being carried out in a national+allied/eFP format.

Regarding the perspective of Baltic State capabilities, equipment and priorities, developments are occurring (and will continue for the foreseeable future) "in the same book, but not on the same page." This is influenced by financial considerations (Latvia was hardest hit by the financial crisis) as well as different levels of mechanization (or in the Lithuanian case—motorization; also due to geography/environment). Additionally, the Baltics have differing air force development focuses—on rotary versus fixed wing craft. And disparities exist in what role voluntary forces have for the overall defense posture (in Estonia for example). Against this background, the B3 is concentrating on exercises, national plan coordination, and working on the interoperability of their three relatively different systems. Cooperation in the defense domain has been among the most

successful areas among the B3. Still, to some extent, Latvia, Lithuania and Estonia are reaching the limits of what they can do in a bottom-up approach. Information exchange coordination is good; but views still diverge on, for example, needed equipment. If we further integration is, in fact, desirable—despite the inherent loss of part of each country's freedom of unilateral action—a political top-down approach will be needed. So far, the B3 have not felt such a need. Nevertheless, the adversary is always learning quicker than we think. The adversary knows that in any long conflict ("hot" or "cold'), we continue to heavily rely on allied capabilities. That said, this reliance in no way should be seen as diminishing the value and achievements of the B3 militaries themselves—either at the practical level (for example ISTAR assets) or at the strategically operational decision-making process level. Still, B3 policy is admittedly "reactive"—we are not so much policy makers, but rather reacting to events.

So there are two paths we have to follow: (1) Further development of NATO/allied presence in the Baltics. Russia is not particularly concerned about this development from an "ideological" perspective (it feels it is sufficiently resilient in that sense); rather, Moscow is much more apprehensive that (driven by Russia's own actions) its geopolitical adversary (NATO) is building up a military presence within the Russian "sphere of interests." We have to bear in mind that the North Atlantic Alliance's 29 members still have (and will continue to have) differing views of the relationship with Russia, and we will not change they thinking, nor are they likely to change the Baltics' perception. (2) The B3 must continue to develop our military capabilities— reaching 2 percent of GDP and securing allied presence is one thing, another is to keep it. And here we have a further set of questions: Should the B3 reach out predominantly to Nordic partners and/or Poland? How and how closely should we proceed in terms of relations with these actors? How will the Baltics "win a battle": with engineers or concentrated firepower? What is the role of voluntary forces during conflict? Are conscripts the way to build a professional army? Where do resources for a draft come from? If we see the Baltic

States area as one unified region, are we able to also operate in such a manner? Do we possess an adequate joint surveillance picture and coastal defense in the maritime domain?

As 2008/09 showed, resilience must be built outside military-defense abilities, and capabilities mirror society to some extent. Therefore, long-term economic and social balance in B3 will be key.

Protecting and securing their access to the Baltic Sea and the freedom of navigation in this sea is vital to the security of Estonia, Latvia, and Lithuania. Thus, contributing to these goals should be their contribution to NATO and the European Union as well as important inherent elements of their national strategies. Unfortunately, that is not the case.

Of course, Estonia, Latvia and Lithuania are all separate, sovereign nations, with differing political and social priorities. Nevertheless, we propose and still believe that if they cooperated more in the maritime domain, they could accomplish more toward achieving regional maritime security by banding together—and at less cost to each individually.

Coastal powers and naval powers have different priorities. The coastal power's main concern should be its maritime security, as will be defined below. In addition to a robust maritime security capability, a naval power needs to be able to project force and establish sea control beyond its Exclusive Economic Zone.

By primarily concentrating on its own maritime security, a coastal power can coordinate its naval and constabulary capabilities to ensure they are up to the state-on-state sea denial challenge that would be the ultimate test of their effectiveness. Additionally, the financial, equipment, logistical and manpower requirements to maintain a navy-centric state's power projection and sea control capabilities are too expensive for most small countries and would deflect resources

from the their key maritime security capabilities.

The ability of the Baltic States to deter an adversary from launching a military attack on their territories has unquestionably increased with the arrival, and the placing under local command, of the three NATO Enhanced Forward Presence (eFP) contingents. In addition to significantly boosting warfighting capability in the region, these 'tripwire' forces bring with them a more credible promise of a NATO response to any aggression against the three states.

Military deterrence (and the ability to defend) would certainly be increased if the eFP units were to be augmented, or if additional US force elements were to be brought to the region under the European Deterrence Initiative. Capabilities in the air and maritime domains where, in the medium term, the Baltic states capacity to act will likely remain very limited, would be a notable improvement. On land, meanwhile, NATO brigades/brigade combat teams would send a more powerful deterrent message than do battalions.

However, not all Allies share the threat perception of those on the eastern flank, and there appears to be little appetite within the Alliance to further develop the present eFP configuration. Unless there is a major degradation in their security situation, the Baltic States should not count on substantial increases to the US or NATO footprint in their region. To enhance their defense and deterrence, the three states will need to do more for themselves.

The overall balance of forces would likely allow NATO to eventually prevail in a conventional conflict with Russia. But Russia's military strength in the Western Military District and its aggressive military modernization program give it a short-term advantage in the Baltic region. Prudent defense planning in all three Baltic States thus includes "surprise attack" scenarios, which would entail a period of fighting alone before allied reinforcements could arrive.

To avoid these scenarios, the Baltic States aim first and foremost to deter by denial, i.e. to have, militarily, the ability to inflict sufficient pain on an adversary as to dissuade him from attempting an attack. Such a strategy requires both military capability and the demonstrated ability to employ it effectively. So far, to the extent they have been tested, both elements have proven adequate. Moreover, limited defense cooperation among the three states also means that both these elements are weaker than they might be. Baltic Defense Cooperation can enhance interoperability between participants' armed forces, reduce duplication and waste, provide better value for money in acquisition, and allow states to acquire capability that they could not acquire alone. The three Baltic States are natural candidates for defense cooperation programs. Their size, geostrategic position, and stage of development of their defense forces—aspects recognized to contribute to successful defense cooperation—make them far more similar than they are different.

The three states have a good record of coordinating policy positions, for example with regard to Baltic Air Policing, or in their approach to the NATO Wales and Warsaw summits. However, aside from the flagship initiatives of the 1990s (BALBAT, BALTNET, BALTRON and BALTDEFCOL), when outside pressure and assistance heavily encouraged cooperation, the three states have achieved little together when it comes to concrete projects.

While there have been opportunities for common defense acquisition programs (recent examples include self-propelled artillery, infantry fighting vehicles, and short-range air-defense systems) the three states have apparently been unable to generate sufficient political will to work together and overcome the challenges that inevitably arise in multinational defense cooperation.

Trust, probably the most important factor in successful defense cooperation, is missing at all levels. Strong notions of sovereignty, differences in strategic culture, and a lack of alignment of defense

planning also stand in the way of cooperation.

For the Baltic States to improve their defense and deterrence postures, these deficiencies should be addressed together—particularly, in capability acquisition. While the three states will soon all be at the 2 percent level of defense spending, even this will provide little in cash terms in a notoriously expensive market. Together, their spending currently amounts to less than 1 percent of the total spending of European NATO. Greater efficiency in capability acquisition—not only in purchase prices, but also in common arrangements for training, maintenance, upgrade, etc.—should be sought through greater cooperation in the region in defense planning, to synchronize programs in order to provide the conditions for common acquisition, and to reduce duplication and waste. Additionally, cooperation is need for operations. Greater coordination or integration of operational units as well as joint operational planning will allow for a more effective employment of force. While the integration of land forces is likely to be challenging, the integration of Baltic naval units, following the example provided by the Belgian and Dutch navies, may be an achievable ambition. Presently, in the event of a major conflict, the three states will be fighting separately. While there is some transparency in their defense plans, there does not appear to be (as far as can be assessed on an unclassified level) coordination between these plans.

Without advance thinking about regional defense and the exercising of coordinating arrangements, the three states' ability to effectively employ force in a regional conflict will be limited.

Defense cooperation across Europe is widely recognized to be inadequate, and the Baltic States should not be singled out for criticism. But in the security environment post-Afghanistan and post-Ukraine, the balance between security consumption and security provision in the three states has shifted in the direction of consumption. The more the three states can do to help themselves, the

greater the likelihood that they will continue to receive support from the rest of the Alliance. The Allies expect cooperation—note, for example, that the 2018 US National Defense Authorization Act (NDAA) authorizes up to $100 million through the European Deterrence Initiative to Estonia, Latvia and Lithuania on the condition that this is spent on a joint program (in this case, the three states agreed to purchase ammunition together).

Real deterrence requires long-term vision linked with capability buildup—and not only among the three Baltic States, but also within the whole NATO alliance, based on a united understanding of consequences in the broader term. Therefore, effective deterrence is an output of common, intra-regional and international, solidarity and cohesion. For NATO, it necessitates clear understanding and consensus of 29 countries by recognizing that regional challenges are not regional in nature, as they are capable of changing the current security environment in all of Europe, including the possibility of undermining transatlantic relations, which have been fundamental for the common security. In the past, initiatives have been proposed to create common regional units and merge their capabilities to use them more effectively. However, these structures proved to be only temporary (e.g., BALBAT), designed expressly to show unity and willingness to join international structure together (first and foremost, NATO).

But having achieved that goal, the three Baltic countries again started to put the accent on national priorities, eschewing further cooperation with their neighbors. The Balts have been separately developing their own armed forces, including in the procurement of weapon systems despite sharing a common operational area. Close intra-regional coordination in the Baltic is paramount since any attack on or occupation of a Baltic State automatically has important negative implications on the security situation of its neighbors.

An important factor in all three Baltic States is their territorial defense

forces, which are a key element needed to build societal resilience due to their close link with the civilian population. The importance of territorial defense forces stems from them being volunteer forces dedicated to fighting on their own terrain and implementing the deterrence-by-denial concept. The voluntary character enhances civil-military cooperation and reinforces a state's comprehensive approach to defense. Currently, Baltic territorial defense forces include the Estonian Defense League (Kaitseliit), Women's Home Defense (Naiskodukaitse), Young Eagles (Noored Kotkad) and Home Daughters (Kodutütred); the Latvian National Guard (Zemessardze); and the Lithuanian National Defense Volunteer Forces. However, these forces are organized and subordinated in different ways in all three countries, making joint cooperation and coordination exceedingly difficult.

The region has already experience non-conventional attacks. Notably, Estonia was targeted by a coordinated mass cyberattack in 2007, and all three Baltic countries have come under pressure in the energy domain and continue to be experience pressure from information warfare. Each country took a direct step to face these non-military threats by hosting a Center of Excellence to improve national, regional and NATO responses. Namely, these are the NATO Cooperative Cyber Defense Center of Excellence (CCD COE) in Tallinn (2008), the NATO Energy Security Centre of Excellence (ENSEC COE) in Vilnius to (2012) and the NATO Strategic Communications Centre of Excellence (STRATCOM COE) in Riga (2014).

The situation brings to mind a statement mentioned during an ABCD conference in Tallinn: "We were looking so hard for partners abroad that we forgot to look for partners here in Baltic region." All three countries are independent entities with their own priorities in foreign policy, economy, armed forces buildup, etc. This must be recognized, as it is an important factor influencing cooperation. Furthermore, defense and deterrence are often understood within the military domain. But non-military domains require a whole-of-government

approach toward both each single nation as well as within intra-regional configurations.

Enhanced Forward Presence has already proven the Alliance's decisiveness in wanting to send a strong political message. For the civilian population and decision makers, it feel like sufficient deterrence; yet, that may not prove true in a real crisis, depending on the circumstances. One issue is the need to preserve continuity of those rotational deployed troops when the threat perception starts to diminish. This will require all three Baltic States to raise the issue constantly using all possible fora, but also to look for other countries to raise their voice in concert about their shared perception of the threat. NATO Force Integration Units (NFIU) will also need to be raised to facilitate the deployment of major NATO units (such as the Very High Readiness Joint Task Force, VJTF) and to make them more effective. The B3 must try, in common effort, to enhance closer cooperation of eFPs and NFIUs within their region.

Allies' decisions to support the region in case of conflict could come too late. This is especially the case since NATO eFP battalions deployed in 2017 are not capable of dealing with direct aggression, despite their hopefully strong deterrence effect. Standing forces would be a more appropriate solution, but that would require allocation of additional troops and funds by the contributing countries. To facilitate a stronger presence, significant investment by the Baltics as Host Nations is required as current infrastructure is not allowing deployment and stationing extended presence. National initiatives must be reinforced by recognition of the growing need for both intra-regional and international cooperation. Cooperation among the Baltic countries is not a new topic: it was initiated after the three republics regained their independence in 1991, with a variety of outcomes (BALBAT, BALTRON, BALTNET). Some of these trilateral initiatives disappeared and some continued, though with limited value. On the other hand, the education of B3 military and civil servants at the Baltic Defense College should be maintained since it facilitates better

understanding among the three countries as well as supports networking between their respective security and defense communities.

To help bolster the B3's limited naval and air force capabilities, one useful option might be to create a common service among them—e.g., a joint naval squadron. Positive movement in this direction was undertaken in 2015, at a tripartite meeting of the Latvian, Lithuanian and Estonian defense ministers, who focused on common air-defense requirements and unified infrastructure projects designed to facilitate longer deployments of allied forces to the region. Additionally, a meeting of the ministers of defense of Latvia and Lithuania and a joint communiqué in 2016 proved the will to synchronize their procurements of military equipment.

Cooperation is still an issue, mainly due to the limited number of projects planned and executed together. That aspect must be taken under consideration as the fate of all the three countries will be similar in the case of aggression. Thus, trilateral initiatives represent the only viable means to successfully meet such challenges. This must be underpinned by visible cooperation that shows the Baltic States' will and ability to act in a united manner. In turn, that will enhance combined Host Nation Support capacities, which must be further strengthened by revised legal regulation allowing for faster movement of military assets into and across the region—including the creation of a so-called "NATO Schengen Zone." The military value of intra-regional projects such as Rail Baltica and Via Baltica should be more actively promoted within the EU as a common European interest beyond just the economic sphere. Meanwhile, NATO decisions are of great importance but a lot must be done to ensure that their outcome (on-the-ground units) will stay in place in the coming years since the security situation is still not stable and could be shaken easily if an adversary were to undertake such a decision.

The Baltic countries paid a price by participating in all major NATO

operations abroad with their limited capabilities. Indeed, this was an important reason for why the B3 shifted their national resources away from territorial defense and toward creating expeditionary capabilities—this was required to fight arm-in-arm with NATO partners in order to show the Balts' credibility and reliability to the rest of the Alliance. That fact must be highlighted.

In general, the multinational integration approach must be based on the assumption that a common voice is stronger than that of any single country alone. The territorial defense forces of the B3 are organized and subordinated differently in each country; they do not cooperate, thus preventing an easy pooling of their capabilities. The closer cooperation of the Estonian Defense League, Latvian National Guard and the Lithuanian National Defense Volunteer Forces as well as an exchange of their respective experiences related to terrain, capabilities, tactics, and threat assessment would support better intra-regional coordination. It would enhance not only the Baltics' deterrence posture but would contribute to stronger resilience of their populations.

The group of BSSP experts involved in this year-long project identified the following as the biggest challenges facing the Baltic States: joint procurements, joint operational planning, a comprehensive maritime security strategy, major shortages in Air Defense, cross-governmental civilian cooperation, cooperation on defense research and innovations, and weak intra-regional political will. When finding solutions, national and intra-regional aspects of capability-building on each of these elements is important to consider.

Good examples do exist of Baltic cooperation grounded in commonalities and limited by differences between the Baltic countries—these should be taken into account and analyzed for future development. However, the in analyzing what has been achieved so far, the group of BSSP experts came to an important conclusion: current state of cooperation among the B3 is still lacking, and the

content of this cooperation must more fully embrace sub-regional defense and deterrence.

Each of the Baltic States greatly improved its national capabilities after 2014 in response to the realistic threat posed by Russia's aggressive foreign policy—as illustrated by its invasion of Ukraine and annexation of Crimea. However, one remaining challenge today is that the Baltic States' defense strategies are largely land-based and thus have significant air and maritime gaps. For example, the Lithuanian defense budget, despite being the quickest growing in the world following 2014, provides no major investment in air or maritime defense.

Another challenge is the evident lack of intra-regional governmental cooperation on defense and deterrence. The underlying reasons for the lack of cooperation are poor inter-governmental trust and little political will. Recommendations to mediate these challenges include working together in four target areas: Acquisition, Defense Planning, Operations, and Operational Planning.

NATO Allies expect the Baltic States to cooperate with one another on defense and deterrence issues, while at the same time opposing greater NATO influence and activity in the region, especially not until intra-regional cooperation improves. Specifically, the Enhanced Forward Presence initiative by NATO was lauded by all BSSP participants, and this initiative will continue to play an important role in Baltic defense in the years to come.

As the Baltic States will be expected to withstand aggression without additional aid from NATO Allies in the first moment of an offensive, this situation further underscores the need for the Baltic States to develop greater intra-regional defense cooperation as well as maritime and air capabilities.

As noted above, greater coordination in the political sphere is

necessary among the Baltic States. Some competition naturally exists to appear "the best" when communicating with Allies, and each country's national security strategy and resource planning formula differs. Building a small coalition of willing high-level officials to reiterate the vital importance of Baltic defense in Washington could be a positive step forward. Some BSSP experts suggested that the Baltic States should also develop deeper cooperative ties with regional partners such as Poland. Other suggestions included coordinating military exercises and cross-border operations. Meanwhile, bolstering civilian capabilities and resilience across the Baltic States is important because the reality of maritime- and land-based threats from Russia are not on the radar for everyday citizens, and support for NATO forces in the region can be improved. One approach to remedy this situation is to bolster strategic communication both through NATO and in each B3 country so that societies can more properly conceptualize that real threats from the East exist. Host Nation Support (HNS) could be an avenue through which interoperability is developed, civil-military ties are established and, therefore, deterrence is better achieved.

1.2. Defense and Deterrence In-Depth Analysis

Glen Grant, William Combes, Anthony Lawrence, Edgars Poga

Introduction

Baltic defense cooperation has arguably been one of the greatest political and social success stories for the three Baltic States (B3) since they regained independence. The Estonian defense minister in 2002, Juri Luik, called it the "flagship of our defense system."[1] The Baltics are at one time both quite different but also share important similarities. On one hand, they have no common linguistic and cultural features. On the other, they share a common geography and a traumatic recent shared history. In truth, the initial impetus for a common regional identity, particularly in the realm of defense cooperation, came not from the B3 themselves but from the international community, which found it easier to try and deal with one larger entity rather than three smaller ones. Internal politicians supported this strongly, selling it as important on two fronts: for improved relationships with the assisting nations, and for providing better overall defense and deterrence. Strong arguments included that the three countries faced a common enemy and were in the same operational space, that it would assist development of NATO interoperability and standards (which it did), and that it would help bring the countries into NATO. Lastly, and though it may sound trite, *it seemed like a good idea at the time*.[2] It still does.

[1] "Baltic Defence Cooperation," Ministry of Foreign Affairs of the Republic of Estonia. Last modified June 10, 2014.

[2] Ibid.

However, despite all the obvious benefits, Baltic military cooperation has never been a popular theme amongst many military officers of the B3. The differing defense concepts of the countries, in particular the influence of Finland on Estonia, has radically differentiated the Estonian Defense forces from their Latvian and Lithuanian counterparts. The Estonian national emphasis on territorial and total defense meant that cooperative ventures, with the exception of the Defense College and later air policing (discussed below), were treated quite differently by each country. The differing concepts often made coordinated cooperation difficult if not impossible. The three states also looked more often to outside countries (and usually different ones) for working military cooperation, not to the other two. This conceptual division extended to the development of each state's volunteer forces. These forces, aimed at bringing the military closer to society, are now organized and subordinated in a different way in each country. As a result, they have few opportunities in the way of tactical cooperation for using their military capabilities in any joint fashion. **The first logical conclusion is that for cooperation to be successful it has to be at the managerial or operational level, not unit level, as the national defense systems are unlikely to change after years of individually focused development.**

At the same time, the Baltic countries have arguably not created the synergies or value from cooperation that they could have and perhaps that NATO planners assume they have. For example, each country treated membership in the Baltic Battalion (BALTBAT) differently. Estonia loaned a professional company from the Scouts battalion, whilst the other two initially used conscripts (later professionals). Although deployed on international operations at the company level in Bosnia-Herzegovina, BALTBAT was seen more as a tool for gaining NATO membership and interoperability than as a specific defense capability. That said, it did provide high-quality training for officers and a close learning interaction with international military advisers. Both paid off handsomely later in improved national capabilities.

However, the battalion was never designed or seen as a proper working unit for the Baltic States' defense. It was seen as unable to enhance national fighting capability so was deemed a financial burden, detracting from the development of national forces. It was arguably designed to fail from the outset. The Baltic Naval Squadron (BALTRON) also started with an exciting flourish. The opening ceremony had serious international support, especially from Germany, the United Kingdom and Sweden, and the party in Tallinn's Old Town ran all night. BALTRON had national centers of excellence for joint training, for example for learning skills like diving and signals. This was a positive idea as the numbers of trainees in each country at any given time were rarely sufficient to run their own national-only courses. But many initiatives foundered due to budgets and bureaucracy, and the defense ministries often appeared to lack energy to overcome the problems. In 2016, Estonia decided to leave the project, needing the finances to focus instead on the standing NATO mine-countermeasure squadron. It is a point worth asking why all three countries did not try themselves to cooperatively change BALTRON into a standing NATO squadron, which would have given them excellent command opportunities. This single-nation focus appears symptomatic of the national development of all three states.

Other Baltic cooperation has been with BALTCIS, strongly supported by Germany, as well as BALTPERS and BALTMED, both initiated and supported by Sweden[3]. As with other cooperative ventures, these have increased operational capability of the three countries, but they have not developed the trilateral capability at the strategic or operational level.

One beacon of light with respect to successful Baltic military cooperation remains the Baltic Defense College, in Tartu. It is a point of pride for all three states. It is also now valued internationally for providing excellent military education, to officers and civilians, at the

[3] Ibid.

operational and strategic levels. But even after nearly two decades of B3 officers working, socializing, and collaborating together on courses that highlight the methods and importance of cooperative, joint and combined operations and strategies, it has failed to stimulate actual cooperation at the operational and tactical levels. Politically, the main focus remains on individual national priorities.

Now, nearly thirty years after regaining independence and facing a sustained and growing Russian threat, B3 cooperation is beginning to be re-energized in areas like Host Nation Support (HNS), air defense, support infrastructure and, possibly, equipment procurement. But there is now a critical need to take the various discussions occurring at the legislative level of the Baltic Assembly (cooperation amongst parliaments), other governmental structures, defense ministry meetings, as well as the B3 biannual Military Committee, chiefs of staff (COS) and single service commanders' meetings, and turn them into new hard capabilities.

At its 2018 Brussels Summit, NATO pledged to improve readiness in terms of battalions, air squadrons and ships and also agreed to create a military "Schengen" in Europe. These improvements will all have a positive effect on the security of the Baltic States, but none of these pledges will assist during the first moments of a potential conflict or reduce the threat from the heavily fortified Kaliningrad enclave. The three states may well have to wait for reinforcements to fight past this. The need for enhanced capability and improved cooperation until reinforcements arrive, whether that is in 30 days, or longer, remains for all three.

Principles of Cooperation and Coordination

History shows that cooperation and coordination will only work when there are powerful benefits to each country that both enhance and transcend its national interests. Key principles for B3 cooperation and coordination should include:

- A visible deterrent to Russia through capabilities that improve resilience;
- Better political and military management measures for times of crisis; and
- An actual improvement in military capability that is needed by all three countries and is politically and financially sustainable.

Additionally, experience from past Baltic cooperative attempts show that measures must not run counter to the main land-centric fighting concept of each of the individual Baltic countries. However, that still leaves opportunities to deliver a positive operational boost to air and naval capabilities, particularly through additional technical solutions and broader international cooperation.

Also, any capability that can generate faster combat capabilities than the current general NATO reinforcements or from allies Sweden and Finland, such as better use of the National Guard or Reserves, has strong merit.

Political and Crisis Management Measures

Improved political resilience is vital as political coherence of the B3 can be both a strong deterrent capability and a possible weak link. The key to improved resilience is the timeliness and coordination of crisis-management decision-making instruments within the three national political and military institutions, and a joint approach toward NATO in a crisis. The Baltics cannot afford one politically weaker or slower link in this chain. A common set of standards is required in decision-making, laws and rules in order to prevent individual national weaknesses that can be easily exploited by Russia. The three Baltic States need a common (or a least not an uncommon) legal framework that takes full account of the rapid speed with which Russian aggression could develop. If Russia attacks, there will be no time for

slow parliamentary discussions, bringing presidents back from trips abroad to sign orders, or to enact throw-back Soviet ideas like selecting supreme commanders. What exists now and works is what will be available.

NATO arguably has not helped in this coordinating process. Little has been done in the way of direction to cooperate politically or militarily. Despite their closeness, each country has its own NATO Force Integration Unit (NFIU) to facilitate deployment of major NATO units for and from the Very High Readiness Joint Task Force (VJTF). NATO has already supported and encouraged enhancements within the three countries, but these remain independent of each other militarily in command terms; and some support, for example from Canada, is bilateral and not from the Alliance. This may create more political problems for member states and NATO if, for example, only one country is attacked, or all three face "hybrid" threats that unbalance the coherence of this part of NATO. **Thus, there is a vital need to bind NATO command, control, communications, computers and intelligence (C4I) structures more closely to the three Baltic countries politically and organizationally for an evolving and developing crisis—not just providing NATO support after the problem occurs.**

One key requirement is a need for closer cooperation for national security and intelligence agencies, especially military intelligence. This is vital since a hybrid-style scenario could see each of the three attacked in a totally different way. Three possibly alternative views to NATO in a crisis would create delay and could prove fatal. **One common intelligence center for NATO based within the B3 could be highly effective for building trust, for better national and NATO decision-making, and for early advice to contributing third countries. It would also bring quicker engagement with close partners Poland, Denmark, Finland and Sweden.** Arguably, this coordination must include deployed Allies full time within the

organization. A single joint crisis center would also make sense both for NATO and member states in terms of binding and political coherence, but this may be politically a step too far.

Defense Management

The three Baltic States have a strong record of coordinating policy positions at key times. They coordinated well in regard to Baltic Air Policing, or in their approach to the Wales (2014) and Warsaw (2016) summits. Also, in 2017, all three Baltic countries uniquely concluded a "military Schengen" agreement for simpler and faster movement of NATO allied Forces within B3, a move that NATO now wants to implement throughout Europe. The importance of this 2017 agreement should not be underestimated. However, aside from the flagship initiatives of the 1990s (BALBAT, BALTNET, BALTRON and BALTDEFCOL), when outside pressure and assistance heavily encouraged cooperation, the three states have achieved little else together when it comes to concrete projects.

Certain opportunities existed for common defense acquisition programs (recent examples include self-propelled artillery, infantry fighting vehicles, and short-range air-defense systems), but the three Baltic neighbors have apparently been unable to generate sufficient political will to work together and overcome the challenges that inevitably arise in multinational defense cooperation.

Trust, probably the most important factor in successful defense cooperation, is missing at all levels. Strong notions of sovereignty, differences in strategic culture, and a lack of alignment of defense planning also stand in the way of cooperation. Any increased joint capabilities and abilities need to be publicly demonstrated to Russia, meaning that already-existing joint capabilities need to be coordinated at the regional level. Instead of determining and meeting the individual needs of Estonia, Latvia or Lithuania, a politically clear focus on the regional level is needed. In this regard, problems in one

of the Baltic countries in developing its military resources are and should actually be a common concern for all three Baltic countries. Should this idea of joint efforts not be acknowledged and adopted swiftly enough in the Baltic region, help should be provided by NATO in the form of guidelines to local politicians of how to jointly plan, train and develop military capabilities.

While the three states will soon all reach the 2 percent level of defense spending, even this will provide little capability in cash terms in a notoriously expensive market. Together, B3 spending currently amounts to less than 1 percent of the total spending of European NATO. Greater efficiency in capability acquisition—not only in purchase prices, but also in common arrangements for training, maintenance, upgrades, etc.—should be sought through greater cooperation in the region in defense planning to synchronize programs. The challenge is that all three countries tend to use long-term plans and programming tools with hardened legal frameworks that discourage rapid change. Greater flexibility of planning is needed in order to provide the conditions for common acquisition and to reduce duplication and waste. Modest results have already come from ammunition procurement. **Setting up a B3 Ammunition and Fuel agency is a key area where enhanced capability could be sought, and this could be expanded to other common procurement areas if successful.**

The Military-Operational Space

The present-day ability of the Baltic States to deter an adversary has unquestionably increased with the arrival and placing under local command of the three NATO Enhanced Forward Presence (eFP) contingents. In addition to significantly boosting war-fighting capability in the region, these "tripwire" forces bring with them a more credible promise of a NATO response to any aggression against the three states. However many contributing countries are sending

only token tripwire forces into the Baltics, which although possibly bringing value to extended deterrence (and today there is no surety of this at all) they do little to improve the actual war-fighting capability. Indeed, they may actually harm the operational coherence needed to fight effectively. Also, the fact that these various battalions are each deployed to a single country, not to all three, could add serious political challenges for contributing states if only one Baltic country is singled out for aggression. The need for NATO unification to a common operational battlespace is vital.

Military deterrence (and the ability to defend) would certainly be increased if the eFP were to be augmented or, especially, if additional US force elements were to be brought to the region under the European Deterrence Initiative. Capabilities in the air and maritime domains, where the capacity to act is limited, would be a notable improvement. On the land, meanwhile, deployment of NATO brigades or brigade combat teams would send a more powerful deterrent message than do battalions. A serious question also remains about whether land-force contributions provide the best eFP package. **For example an eFP air-defense unit, instead of more infantry troops, would provide, pound for pound, not only a greater capability enhancement but arguably also much better deterrence.**

However, not all allies share the threat perception of those on the eastern flank, and the appetite within the Alliance to further develop the present eFP configuration in terms of coherence is fragmented. In place of a full NATO initiative, a group of Allies have pushed forward with the creation of a new Baltic-focused regional command.[4] At the Brussels Summit, Denmark, Latvia and Estonia agreed to establish a new Northern Multinational Division Command, with Canada, the

[4]"NATO Has a New Baltic Command Structure," *DefenseNews,* July 11, 2018, https://www.defensenews.com/smr/nato-priorities/2018/07/11/nato-has-a-new-baltic-command-structure/.

UK and Lithuania also signing on as "contributing countries." Although not as high level as the recently created Command focused on the Atlantic Ocean, the group will provide continuous operational overview of the regional activities, manage the two to four brigades under its command, and coordinate exercises and operations for the region. The HQ will be split into two hubs: one located in the Latvian city of Adazi, approximately 25 kilometers from Riga, and one in the central Danish region of Karup. But the fact that Lithuania did not wholeheartedly join the other two states in this venture only highlights the challenges of B3 operational cooperation. Equally, the lack of the United States in this proposed HQ also draws into question the readiness for deployment into the Baltic States of the US brigade in Poland. There is yet no clarity if this will be a deployable HQ capable of working and commanding the militaries of all three countries in war or just another coordinating office.

Arguably, despite enhancements, the principle aim to deter by denial still fails the obvious measure of deterrence because the three do not have enough lethal capabilities in any one country to ensure deterrence by defense. This is arguably made worse by the lack of a unified command-and-control (C2) network. At present, the lethal capabilities on the ground do not meet the levels required, thus reinforcing the need for either capability improvement or stronger extended deterrence from NATO. Based on current operational planning, the three Baltic States will be fighting separately. While there is some transparency in their defense plans, there does not appear to be (as far as can be assessed on an unclassified level) coordination between these plans. Critically, to be fully effective, NATO support requires coordinated B3 crisis management processes, enhanced Host Nation Support and a coordinated B3 approach—not as now, the single nation approach to reinforcement.

The integration of land forces is likely to be challenging, but the integration of Baltic naval units, following the example provided by the Belgian and Dutch navies, may be an achievable ambition. The

Baltic Air Forces rely totally upon NATO. The HNS support of airfields has been a priority, but actual combat aircraft can only come from outside countries within NATO or Sweden or Finland. **This is one operational capability where swift political action to gain enhanced crisis-response measures for immediate combat aircraft reinforcement as part of trilateral plans will have a serious deterrent effect.**

Land Forces

The Baltic States' ground troops potentially face three Russian armies. This is an impossible task to deal with for the three Baltic countries alone. But the key aim in any ground conflict for them is to buy time and inflict losses. Greater coordination or integration of the Baltic States' operational units will allow for more effective employment of ground forces, especially when National Guard and reserve forces are fully included. This would be best coordinated by the new NATO Multinational Headquarters (NMH). The primary task is to make the Joint Operational Area fully operational as a coherent geographical area, not three separate and distinct battle spaces as now. This would be achieved by coordinated plans and exercises. That said, the work of the NMH is unlikely to replace the day-to-day responsibilities, command and control (C2), nor freedom of action of national forces.

The new NMH should become the hub for NATO command reinforcement and local forces' operational and tactical thinking. Although, to avoid costly duplication of effort, there will be a serious need to realign the roles between the NMH, national forces and the NFIUs. Additionally, the NMH should be used as an agent for transformation and synergy amongst the Baltic States' structures and tasks as well as contingency planning and readiness, especially amongst the National Guard and reserve forces, while at the same time preserving national sovereignty. Organizing exercises to rehearse different phases of war will be essential. Furthermore, the NMH can

lead on functions such as identifying crisis-management weaknesses as well as needs for joint training and exercises. It can become a single point of operational contact for allied interaction and cooperation rather than the multiplicity of organizations that exist now. The challenge will be agreeing on command relationships and trust building between the three countries' political and military decision-makers and the NMH Commander.

Two key operational shortfalls are the lack of an operational reserve of at least brigade size, capable of deploying where needed most and deploying a weapon system with longer ranges capable of deep strike. Whilst the second may raise political eyebrows on the grounds that NATO is purely defensive, Russia does not appear to believe this or care. Deterrence would be well served.

Air Defense

Air defense is the most critical military capability shortfall in the Baltic States. The very limited capabilities of the three states in this area create vulnerabilities not only for themselves, but also for NATO in its planning to defend the Baltic region and the Nordic countries behind. Because of these circumstances, the issue of Baltic air defense is covered in greater detail here.

Although overall NATO air assets are greater in number and quality than Russia's, Russia holds a substantial local advantage in the air domain in northeastern Europe. Russia's Western Military District alone is home to some 27 combat air squadrons, 6 battalions of attack helicopters, and a division of airborne infantry.[5] Russia has deployed

[5] Richard Sokolsky, "The New NATO-Russia Military Balance: Implications for European Security," *Carnegie Endowment for International Peace*, 13 March 2017, http://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222, accessed 10 July 2018; Defense Intelligence Agency (USA), *Russia. Military Power* (Defense Intelligence Agency, 2017), 55 (available from

Iskander ballistic missiles close to its western border and in Kaliningrad, and will augment the Baltic Fleet with corvettes armed with Kalibr cruise missiles during 2018.[6] It has also built a sophisticated ground-based air-defense capability centered on the long-range S-400 system.[7]

The Baltic States, meanwhile, have developed an air surveillance, command-and-control network that, while it is integrated into NATO's air- and missile-defense system, essentially provides solely a peacetime capability. They have also acquired a limited number of short-range, ground-based air-defense systems and retain a number of legacy anti-aircraft guns. In addition to these local assets, NATO occasionally exercises air-defense units in the region and provides the Baltic air-policing and enhanced air-policing missions—while these are not air-defense missions, they do ensure persistent, albeit limited, NATO combat air presence in the Baltic States.

In a conflict with Russia, however, local capabilities would be wholly inadequate to meet the air threat, leaving the Baltic States and the North Atlantic Alliance vulnerable to the effects of a fast-moving air campaign. Maneuver forces, including Allies deployed under eFP, would likely be prevented from reaching their objectives by attacks from the air. Mobilization, especially important for Estonia, which relies on conscription to build its wartime force structure, would be

---

http://www.dia.mil/News/Articles/Article/1232488/defense-intelligence-agency-releases-russia-military-power-assessment/, accessed 12 July 2018).

[6] Roger McDermott, "Russia's Military Precision Strike Capability Prioritizes Iskander-M," *Eurasia Daily Monitor* 14(82), https://jamestown.org/program/russias-military-precision-strike-capability-prioritizes-iskander-m/, accessed 10 July 2018; Välisluureamet (Estonian Foreign Intelligence Service), *International Security and Estonia 2018*, (Tallinn: Välisluureamet, 2018), 19 (available from https://www.valisluureamet.ee/security_environment.html, accessed 12 July 2018).

[7] "Russia's Western Military District to Get Four S-400 Missile Systems this Year," *TASS*, January 13, 2017. http://tass.com/defense/924840, accessed 10 July 2018.

disrupted. Key strategic locations, including national capitals, military infrastructure, and C2 nodes would also be vulnerable. Crucially, NATO's large-scale reinforcement of the region, on which its plans for the defense of the Baltic States rely, would be threatened by the destruction of air and sea ports, and the exposure of air, land and sea transport routes. Effective air defense in the Baltic region is thus not only essential for the three states themselves, but for the rest of NATO, too. Without it, deterrence is weakened.

However, building a comprehensive, layered air-defense system would be prohibitively expensive for the three. Long-range air-defense weapons systems, whether air-, sea-, or land-based, are far beyond their financial reach. Even medium-range ground-based systems, in which Lithuania has begun to invest with the acquisition of two batteries of the Norwegian Advanced Surface to Air Missile System (NASAMS), and which Estonia and Latvia have recognized a need for but have not yet included in their defense plans, will put a significant strain on Baltic defense budgets. If the Baltic States are to develop the air-defense capability they urgently need, they will have to look to NATO and the Allies for assistance. And the three states themselves will need to cooperate closely in order to demonstrate their own commitment, make best use of scarce resources and ensure interoperability. The small size of the Baltic States and the high speed of air operations make it almost essential that the airspace above the three states should be managed as a single operating area.

Broadly speaking, an air-defense system can be thought of as a combination of sensors, weapons systems or effectors, and a command, control and communications (C3) network to integrate the sensors and weapons, as well as conduct battle management functions. For air-defense sensors, the three Baltic States have invested in a network of long-range air-surveillance radars. Surveillance of their airspace now meets, and sometimes exceeds, NATO minimum military requirements. This capability must be maintained as technology evolves, and some attention should be paid

to filling gaps in order to allow better detection and tracking of slow, low-level targets. Nonetheless, Baltic air surveillance is generally in good shape.

The same cannot be said, however, of the air command and control (C2) capability, developed collaboratively by the three states alongside the radar network under a framework known as the Baltic Air Surveillance Network (BALTNET). This capability, consisting of C2 nodes in each of the three states connected via secure communication links to each other and to the rest of NATO's integrated air and missile defense system, falls short in several areas.[8] The communications network has only limited redundancy and is thus unable to guarantee the high availability and high reliability required for air command and control in times of crisis. There is insufficient technical capacity and insufficient trained personnel—in particular fighter allocators, surface-to-air missile (SAM) allocators and data link managers—to allow the air C2 nodes to operate on a continuous basis and to take over battle management functions from each other if these are disrupted at the live node. NATO-standard connections (Link 16 terminals) are also insufficient to allow incoming NATO assets, such as airborne early warning aircraft (AWAC) or long-range ground-based air-defense systems to integrate readily into the Baltic air C2 environment. In short, the three states have developed a peacetime air C2 system capable of supporting Baltic Air Policing operations but inadequate to support NATO's defense of Baltic airspace in times of crisis.

Thus, the Baltic States need first to collectively focus their attention upon creating a robust air command-and-control capability. Redundancy needs to be built into communications networks, both within and beyond Baltic territory, and **command-and-control nodes**

[8] Sir Christopher Harper, Anthony Lawrence, and Sven Sakkov, *Air Defence of the Baltic States* (Tallinn: ICDS, 2018), 15-16 (available from https://icds.ee/air-defence-of-the-baltic-states/, accessed 11 July 2018).

need to be upgraded with the necessary trained personnel and equipment to allow for continuous operations with incoming NATO assets and the ability to rotate battle management functions. The Baltic States have, through BALTNET, successfully cooperated in developing the present surveillance, command and control network. It makes clear sense that they should continue to do so to enhance this capability. Some work in this area has begun with an agreement among the three air force chiefs to create a BALTNET Future Configuration—it is essential that this project is given the fullest political support. Responsibility for upgrading the air command-and-control network will lie largely with the three Baltic States, but funding opportunities from NATO's Security Investment Program should certainly be investigated.

With robust air surveillance, command and control in place, it would make sense to invest further in air-defense weapons systems. As a priority, existing short-range ground-based systems, whose present standalone status greatly complicates the management of air defense, should be fully integrated into the Baltic air command-and-control network. This means better C3 systems. The three states should then increase their air-defense weapons coverage, following Lithuania's lead by investing in medium-range ground-based systems. This will allow local area-defense capability, rather than the point-defense capability currently possible. It will undoubtedly be an expensive venture, perhaps requiring a reconsideration of force development priorities—Lithuania's 2017 acquisition of two NASAMS batteries, including training, additional equipment, logistical support and system integration, for example, was reported to have cost some €109 million.[9] To keep costs to a minimum, as well as to build interoperability, the three states should, to the greatest extent possible, acquire and operate these systems in cooperation—common

[9] Robin Hughes, "Lithuania, Indonesia Sign for NASAMS," *IHS Jane's Missiles and Rockets*, October 31, 2017, http://www.janes.com/article/75322/lithuania-indonesia-sign-for-nasams, accessed 12 July 2018.

acquisition, maintenance, logistics support and training should all be pursued.

Even with robust air surveillance, command and control, and short- and medium-range ground-based systems in place, however, the Baltic States will still be a long way short of the layered, integrated air- and missile-defense system necessary for a comprehensive defense of their airspace: they will need assistance from NATO and the Allies. While the permanent stationing of NATO air-defense assets in the Baltic region is unlikely to be supported in the present circumstances, NATO should step up its exercising of such assets here. The presence of airborne and deployable air command-and-control capability, long-range ground-based missile systems, and fighter aircraft offers valuable training for both incoming and local personnel, and conveys an important deterrence message—in particular if such assets are able to readily "plug and play" with enhanced local air command and control. Air-defense units should also be deployed to the Baltic States for longer periods, for example alongside the enhanced Forward Presence battalions or through the US European Deterrence Initiative.

NATO should also exercise the more general reinforcement of the Baltic region—initially, at least, on a small scale and with an air-domain focus—and the step-by-step transition to a Baltic air-defense posture in times of crisis.[10] Further, as the speed of an air campaign could overwhelm defenses before the Alliance has time to fully react, the Supreme Allied Commander Europe should be empowered to stand up the Joint Force Air Component, a skeleton capability that will be reinforced to provide crisis-time air command and control at NATO's HQ Air Command, without specific authority from the North Atlantic Council. Consideration should also be given, as Baltic

[10] Frank Gorenc, "Deterrence and Collective Defence," in *Joint Air Power Following the 2016 Warsaw Summit. Urgent Priorities*, ed. the Joint Air Power Competence Centre (Kalkar: The Joint Air Power Competence Centre, c.2017), 92 (available from https://www.japcc.org/portfolio/airpowerafterwarsaw/, accessed 12 July 2018).

air command and control is enhanced, to transitioning the NATO air-policing mission to an air-defense mission.[11]

The three must be ready to work together to build up their existing, acutely lacking air defenses. But a complete air-defense solution to defend both their territories and protection of NATO's reinforcement of the region in times of crisis is far beyond their means. **A collaborative Baltic arrangement, together with a shared, coherent approach with NATO and individual Allies can, however, substantially enhance air defense and deterrence in the Baltic States**.

Maritime

For the Baltic States, like other maritime nations, protecting and securing access to and from the sea is vital to security and sovereignty. Maritime security efforts are also important contributions to a key NATO and European Union border zone. As such, maritime security considerations should be a significant element of common national security and defense strategies. Unfortunately, today they are not given the priority they deserve

Effective maritime security needs a common **strategy**. This would outline the maritime situation, the threats, and the importance of the maritime domain to the national economy and security, and identify how to tackle the maritime missions. This strategy would identify the investments required to ensure maritime domain awareness, capable and responsive operational centers, and coordinated or shared joint procurement.

---

[11] Philip M. Breedlove, "Toward Effective Air Defense in Europe," Atlantic Council Issue Brief, February 2018, 5 (available from http://www.atlanticcouncil.org/publications/issue-briefs/toward-effective-air-defense-in-northern-europe, accessed 12 July 2018).

Cooperation in the maritime domain could accomplish more at less cost individually. The strategic needs cover three basic missions: to protect and control the country's maritime natural resources (including port and harbor access), to defend against and repel violations of territorial waters, and to defend against an invasion from the sea by intra- and inter-state cooperation.[12] The first two missions further include additional maritime security dimensions of trade protection, resource management, smuggling prevention, terrorism prevention, disaster management, and oceanography.[13]

Key enablers are a capable maritime domain awareness to identify the threat, a maritime command and information center in order to process the threat and to direct appropriate action to counter the threat, disaster and threat response plans to allow these actions to be implemented rapidly, as well as, lastly, the national legal authorities to employ these capabilities.

The Russian Naval Baltic Fleet is not particularly large. It is, however, large enough to maintain the *status quo*, harass other military and civilian activity on the sea, and to take surprise offensive actions. The Baltic States do not have the capability to deny Russian forces from projecting power from the sea. They are each susceptible to the type of naval tactics Russia used against Georgia in the 2008 Russo-Georgian War.

The Russian fleet stationed at Kronstadt and Baltiysk includes[14] 2

---

[12] R. Hobson, T. Kristiansen, *Navies in northern waters 1721–2000*. (London: Taylor Francis Group, 2006).

[13] D. Sloggett, *The Anarchic Sea: Maritime Security in the Twenty-First Century*. (London: Hurst & Company, 2013).

[14]International Institute for Strategic Studies, 2017. *The Military Balance 2017*. (London: Routledge/Taylor & Francis Group, 2017). All subsequent military force numbers are taken from this source.

tactical submarines (SSK), 8 surface combatants (consisting of 2 destroyers and 6 frigates), 23 patrol and coastal combatants, 12 mine-warfare and mine-countermeasure vessels, 4 amphibious tank-landing ships, and 9 smaller amphibious craft.
Russian regional naval air forces and missiles are also formidable in size and power. They are covered in the Air/Air-Defense paragraphs above. They have the capacity to alone cause untold damage if focused on a single attack point.

In comparison to the number of ships Germany, Finland, Sweden, Poland and Denmark have permanently stationed in the Baltic, the number of Russian naval forces in the region do not appear particularly overwhelming. And if you then compare all of the available European allied naval forces to Russia's, the balance appears to even more heavily in the European Union members' favor (note, this includes all countries' vessels from the reserves and services such as coast or border guards with a defined paramilitary role):

Table 1: Baltic Littoral Region Naval Forces (Other Than B3)

	Germany	Finland	Sweden	Poland	Denmark	Total EU	Russia
Submarines	6		5	5		**16**	2
Destroyers	7				3	**10**	2
Frigates	8			2		**10**	6
Patrol and Coastal	12	70	147	22	63	**344**	23
Mine Warfare	33	15	10	20	6	**98**	12
Amphibious	2	51	11	10		**81**	11
Logistics/ Support	26	7	18	21	13	**88**	?

As of July 2018

But numbers do not tell the whole story. Russia has sufficient forces to initiate naval support to any land or air aggression against the Baltic States (also Finland or Sweden). The majority of the Baltic Sea

countries' forces are, for the most part, designed, operated and deployed for the defense of their own territory. Also, there are public doubts about the immediate serviceability of the combat ships of Poland[15] and Germany.[16] Similarly, the Baltic States, even with their naval assets pooled, lack the sea-borne weaponry to deny a Russian naval task group access to anywhere they wish. They would have to rely upon NATO or allies being quick enough.

One key capability requirement will be the ability to document and prove the facts of any Russian aggression for the international community, particularly in light of expected Russian disinformation and propaganda that will downplay both their aggression and any attempt to portray such a move as not being at the request or in support of local or national governments. With the current maritime capabilities, this will prove challenging.

Currently the three do not have full, integrated and shared awareness across the surface, subsurface and air (discussed above) domains. Each has some of the capabilities shared, to varying degrees, by a multitude of national agencies, with mixed success, for use across the spectrum of peacetime and wartime operations and contingencies.[17] The record of intra-state and inter-state agency sharing of this picture in the Baltic is mixed. It was stated recently that NATO had a complete air and maritime picture of the Baltic Sea for the first time during

[15] "The Modernisation of the Polish Navy According to the Poland's Strategic Concept for Maritime Security," *Pulaski Foundation.* Accessed on December 3, 2018, https://pulaski.pl/en/analysis-the-modernisation-of-the-polish-navy-according-the-polands-strategic-concept-for-maritime-security/.

[16] "Can the German Navy be Saved?" *Real Clear Defense,* https://www.realcleardefense.com/articles/2018/02/19/can_the_german_navy_be_saved_113075.html.

[17] Chris Barrows, *Estonian MDA TTX Report,* April 2017.

BALTOPS 2017.[18] This is something that should not only have happened before, but should be a regional 24/7 capability.

Even if they had the forces and capability at their disposal to successfully and completely detect and deny Russian naval forces access to territorial waters, there is no command structure currently in place to direct the appropriate level of armed force in a timely matter. For this, an operations center with the authorities to direct action across the breadth of the Baltic Sea is necessary. One that spans the Baltic States' territorial waters would a good first step. Although one with participation of the Baltic Sea Region and based in the Baltic States would be even better. This would require the participation of NATO, Sweden and Finland—cooperation that is building steadily. However, some high-end naval warfare missions can only be accomplished by NATO forces, in truth, by the United States. A standing operations center would facilitate the planning, rehearsal and implementation of this NATO maritime reinforcement.

Host Nation Support

At its core, Host Nation Support (HNS) has been used by NATO countries as an operational tool in order to ensure force projection overseas. But so far, it has largely not been considered part of the wider security strategy for incoming forces nor as part of deterrence. What is needed is for HNS to be part of each State's security strategy or at least to consider visible HNS as a credible deterrent. In this case, it also needs to be seen not only as a coordinated part of a three-state strategy but to actually be that single strategy. Three separate visible strategies show the enemy clearly that it is not facing a coordinated opponent. In order to understand how HNS can supplement deterrence, it is

[18] Lee Willett, "NATO Generates Baltic Integrated Air-Maritime Picture for First Time," *Janes 360*. Accessed on December 2, 2018, http://www.janes.com/article/71439/nato-generates-baltic-integrated-air-maritime-picture-for-first-time.

necessary to look at how HNS relates to defense. Usually, each state tends to ensure its own territorial integrity and sovereignty through the development of self-defense capabilities. In the case of the Baltic States, there are three differing strategies rather than a common HNS core. This is exemplified by the nationalistic efforts (and visible PR) and costs of having three separate military airfields. Additionally, each state currently has a separate NATO Force Integration Unit (NFIU) to facilitate timely deployment and smooth logistics of major NATO units for and from the Very High Readiness Joint Task Force. However, by having three organizations—at arms' length from NATO and independent from the MODs—in a crisis, this support may actually complicate not enhance HNS plans.

Several examples exist regarding how capability gaps are mitigated by the allied forces presence in the Baltic States. The most serious has been air policing, a capability the Baltic States lack. The capability gap is mitigated by providing Host Nation Support in the form of military airports with an appropriate level of ground support. The eFP also brings heavy armored units and artillery to supplement the Baltic States' armed forces, and this needs considerable national support. Sustaining this NATO forward defense requires an HNS strategy to maintain the deterrence. The Baltic States have to pay for and develop the reception facilities, barracks, warehouses and other infrastructure.

During the Cold War, NATO trained to bring forces from the US and Canada in order to reinforce European Allies. The Reinforcement for Germany (REFORGER) military exercises' main aim was rapid deployment on short notice by deploying ten divisions within ten days. A major part of this was testing and exercising the national support. Today, however, NATO lacks HNS exercises as there is no standing Joint Logistic Command to ensure and coordinate deployments of allied forces into the region. The NFIUs simply do not have the resources or capacity to compensate for this. The North Atlantic Alliance has identified this gap and, in order to mitigate the problem, NATO defense ministers in February 2018 agreed to

establish new logistic commands to ensure force mobility, sustainment and reinforcement. However, implementing this new structure will take time, and this means that the Alliance and the Baltic States lag behind schedule on coordinated HNS linked to a NATO reinforcement strategy.

Cyber[19]

It is clear that cyberwarfare is grossly more complicated than was first realized. Previously, in its simplest form, it was seen in terms of an operation to hack into government and business computers/servers to do damage, to steal information or to identify weaknesses. The 2007 cyberattack on the Estonian government was a prime example of this. Then, it became clear that attacks on the "Internet of things" included critical and highly vulnerable national capabilities like electronic voting stations, energy assets and medical facilities. But the most recent revelations that online social media is being used to sway elections and undermine democracy take cyber to a whole different level. This is a new hybrid warfare threat and needs not only a technical "computer-based" response but a multi-disciplinary approach. It is also a mistake to separate cyber from preparing for technical-communications-attack capabilities that Russia will bring to the battlefield. As noted by US Army Colonel Liam Collins, "[E]lectronic warfare is combined with cyber warfare, information operations, and artillery strikes."[20] It is altogether now a more complex mix. The Baltic States need to cooperate more closely with Ukrainian and US forces to understand how this Russian capability is evolving in Ukraine and Syria.

Cyber development likely needs a new government structure that

[19] Also please see above section on **The Military-Operational Space.**

[20] Tom Ricks. "The Future of Information Warfare is Here - And the Russians are Already Doing It," *Task & Purpose*, July 31, 2018.

crosscuts several ministries and organizations. The challenge for the three Baltic States will be to identify how to improve and augment structures they already have, like the national Computer Emergency Response/Readiness Teams (CERT) and cyber units in the National Guard, to provide political support and reinforce and coordinate the policy needs of the three, whilst also giving them authority and skills to deal in the wider international space. The Baltics also need to create a coordinated approach when dealing with the new NATO Cyber Operations Center. But one key point must underpin all thinking: cyber is now a fundamental part of Russian hybrid warfare. Any weaknesses of a policy, legal, technical, military, social or financial nature **will** be exploited operationally. In many regards, the three Baltic States are at the cutting edge of cyber understanding; but in terms of coordinated crisis management policy, military and public organizations and general public awareness, they still have much work to do.

A key need exists to develop cybersecurity capacity through education in both the public and private sectors.[21] This includes the need to develop university curricula to develop middle-rank experts.[22] Education could help remove the focus and burden from the national

[21] Lithuania—https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf;
Estonia—https://ccdcoe.org/multimedia/national-cyber-security-organisation-estonia.html;
Latvia—https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss & http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF?regnum=455415

[22] The creation of university curricula that could provide dedicated professionals to the field has been and still remains the aim of all three Baltic States. Indeed, the current Latvian Cyber Security Strategy notes: "Create a common Baltic University study program to combine regional educational resources to prepare strong and qualified experts."

CERTs and national cyber-defense structures by having cyber "ambassadors" across Baltic society able to work on policy, law and organizational education. NATO, in turn, calls for "the development of partnership[s] with industry and academia from all Allies to keep pace with technological advances through innovation."

There is a critical need for Baltic governments to engage society more widely on cyber issues through business experts, non-governmental organizations (NGO), universities and think tanks. At the last DSS Cyber Seminar, in October 2017, the author noted that there were few Baltic government officials of any seniority in the audience. This may be for many good reasons, but it is not an encouraging sign when a once-a-year state-of-the-art cyber conference from international business experts is ignored.

Improving cyber-defense training for military personnel at all levels is absolutely essential. A common study curriculum for commanders is needed on cyber warfare. This could be achieved by widening the objectives of BALTDEFCOL to include a common cybersecurity curriculum.[23]

Baltic officials working in cyber management at all levels must understand national and international crisis management structures. Attendance of officials during Cyber Europe exercises organized by ENISA6 should be encouraged and funded. However, there is not a good record of coordination across the three Baltic States. Lithuania, Latvia and Estonia must work closely to avoid overlap with projects established by NATO, the EU, the OptoElectronics and Communications Conference (OECC), the Organization for Economic Cooperation and Development (OECD), and other organizations. This requires the development of a clear Baltic strategic

[23] "Cyber Terrorism and Information Warfare seminar," Baltic Defence College. Accessed on December 2, 2018, https://www.baltdefcol.org/?id=480.

policy framework tied closely to NATO cyber and intelligence structures and to the three national crisis management systems. It is clear that there should be either a single focus for all three states or a single national point of contact (POC) within each country to coordinate policy, development and exercises. This POC must be closely linked to operational structures but also have authority to crosscut governments and internationally.

A serious need additionally exists across all three Baltic States to harmonize the relationships between governments and society on cyber issues. An attack on the infrastructure of one—for example on energy or transport infrastructure—could easily affect all. It is clear that as well as coordinating operational activities, each country needs the single POC not just for governmental-level cooperation but also for the general public, businesses, academia and international actors to communicate with. This should be over and above the technical capabilities provided by the national CERTS. This point of contact should likely also have the public education portfolio.

However, with the current growing understanding that Russia is attacking many countries through social media to target national social vulnerabilities, it is clear that separating the activities of technical hacking from understanding strategic communications in terms of crisis management is a mistake both at the national and international level. The challenge for Baltic cooperation is understanding the need to coordinate the operational aspects of cyber activities, which need to be treated as a military domain in the same way as land, air and maritime spheres.

Policies will need to be considered in a much wider perspective than just nationally. The lessons are clear. "Nordic countries rank higher than the Continental [European] 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."[24] Internationally, successful cooperation in this sphere has already been shown with the voluntary Nordic Defense Cooperation (NORDEFCO) initiative. This grouping recognizes the prioritization of EU, NATO and United Nations obligations. It also provides a forum for ministers actively cooperating on the coordination of joint capability development**.** NORDEFCO's achievements can provide useful lessons-learned for B3 intra-regional cooperation. Another important project to look at is "NB8," which brings together the eight Nordic-Baltic countries of Sweden, Lithuania, Latvia, Estonia, Finland, Iceland, Norway and Denmark. NB8 was launched by the NATO StratCom Center of Excellence in Riga and covers the softer informational side of cyberwarfare.

Cooperative law presents a challenge to both the B3 and for their neighbors. In this regard, the crisis management laws of the Baltic States need more coherence and international input. A regional cyber threat assessment is needed, as are guidelines for crisis management before new law is written.[25] Important lessons learned are already available from sources such as the Council of Europe's Convention on Cybercrime (Budapest Convention on Cybercrime), the ICDS Energy geopolitics assessment study and other products, as well as the "Tallinn Manual," developed by the Cooperative Cyber Defence Center of Excellence (CCD COE).[26] These should be coordinated with

---

[24]Emmet Tuohy et. al., *The Geopolitics of Power Grids,* ICDS (Tallinn: ICDS, 2018), accessed on November 4, 2018, https://www.icds.ee/fileadmin/media/IMG/2018/Publications/ICDS_Report-The_Geopolitics_of_Power_Grids-E_Tuohy_et_al-March_2018.pdf.

[25] "Developing collaborative and cohesive cybersecurity legal principles," NATO CCD COE. Accessed December 3, 2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2015%20Developing%20Collaborative%20and%20Cohesive%20Cybersecurity%20Legal%20Principles.pdf.

[26] "Pressing Pause: A New Approach for International Cybersecurity Norm Development," NATO CCD COE, Accessed December 3, 2018,

lessons from the Helsinki-based COE on Hybrid Warfare.

Way Ahead

Defense cooperation across Europe is widely recognized as a challenging undertaking; and the Baltic States should not be singled out for criticism. They have actually been more successful at this than most. But in the wake of the wars in Afghanistan, Georgia and Ukraine (Crimean annexation and Donbas), the balance between the B3 providing security for others or being consumers of security has now shifted firmly in the direction of consumption. Thus, the more the three states can do to help themselves, the greater the likelihood that they will continue to receive positive support from the rest of the Alliance. But in the complex security environment of today, the Baltics need to take an even wider view and ground themselves, their crisis responses structures, as well as their policies and laws more firmly in a regional context. This applies especially to cyber defense, which is geopolitical and geophysical by nature. No country can act alone without risking critical isolation. The challenge is that the Baltic States need to rethink their operational strategy and concepts urgently and with stronger regard to regional allies, NATO and the EU. There is a vital need to build trust with Finland and Sweden; and only complete and open operational cooperation will accomplish this. Regional forums for cooperation and coordination exist, but they have been used more as tools for peacetime messaging than for building hard defense and deterrence. They need to be reviewed and utilized.

The Allies assume and expect cooperation—note, for example, that the 2018 US National Defense Authorization Act allowed up to $100

---

https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2014%20Pressing%20Pause.%20A%20New%20Approach%20for%20International%20Cybersecurity%20Norm%20Development.pdf and Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global, Cybersecurity, 110 AM. J. INT'L L. 425, 469 (2016).

million through the European Deterrence Initiative for the B3 on the condition that this was spent on joint programs. In this case, the three states agreed to purchase ammunition. Bullets are important; but the nature of the threat now is so much more multi-faceted and in need of deeper strategic thought.

Nonetheless, the big challenge now appears to be who will lead the changes needed. The three countries have shown little willingness for radical solutions themselves, preferring to stick to well-worn national plans and programs. The creation of the new divisional headquarters shows the strength of NATO as a collection of like-minded countries, but the lack of full endorsement from some key countries highlights the weakness of the Alliance as a change-driving agency. The NATO command structure is simply too political and diplomatic to solve complex problems like this. It also highlights that the three Baltic States are still dangerously split in operational thinking. In the first instance, they should apportion leadership to the strongest Baltic country in each discipline. But as the threat is regional, it may be sensible and trust building to include others more closely in developing change.

That said, other NATO countries may not be of much help in terms of leading such change. The US is sending mixed messages. Meanwhile, the United Kingdom is distracted with BREXIT; and though it seems committed to European security, it may in fact be overcommitted around the world as its military continues to shrink. Denmark appears to be driving the new HQ in the Baltic region but has little political strength for tri-country engagement. Germany has its own military worries. France is too far away, and Poland lacks both the political and military experience as well as confidence to drive home hard arguments. Sweden and Finland may still not feel sufficiently engaged with NATO to take lead roles—or then again, they might, if asked by all three Baltics together. These are dangerous times for the Baltic States, requiring strong solutions. Hopefully, B3 politicians recognize the danger and act—quickly and in concert.

1.3. Interoperability as a Matter of Survival

Vaidotas Malinionis

Benjamin Franklin's admonition that "we must indeed all hang together, or most assuredly we shall all hang separately" was insightful during the American Revolution and is relevant today for Western democracies facing both "hybrid" threats and the possibility of conventional military conflict. However, to mitigate future threats, the Baltic States and Poland have to find agreement on a common regional, long-term Defense Strategy. This would guarantee full utilization of strategic depth for the North Atlantic Treaty Organization (NATO) via the establishment of long-term development goals, consistent budgeting, and regional interoperability of military and nonmilitary sectors at all levels.

It has already been fourteen years since the Baltic States joined NATO, but a difficult and challenging path for defense systems development in each state has complicated the improvement of interoperability between even these closest of neighbors. This gap has frustrated efforts to leverage greater advantage from Alliance membership for effective and efficient national self-defense. This situation must be seriously evaluated and addressed for improved national and regional defense.

All young officers studying military tactics are familiar with the importance of identifying and mitigating the risks of gaps between units (platoons, companies, battalions). An adversary is always eager to identify these gaps and exploit them. Gaps are less protected, coordinated and defended—they can make the difference between defeat and victory on the battlefield. Gaps are always a weak point, especially if one is ill prepared for the fight. This principle works for units at every level and is equally valid for NATO countries.

An individual national defense approach is an expensive, risky and uncertain business. Consequently, Baltic and other Central and Eastern European states rightly put great effort into joining NATO. However, being a member of a defense organization does not guaranty absolute security, especially if membership in NATO is considered the end state of national security. All members of the Alliance must develop and implement an interoperable and reliable defense system that can be effectively integrated with other members of the Alliance. It was this belief that led NATO newcomers to strive to adjust their security programs and improve interoperability with the rest of the NATO community. That process began many years before officially joining the Alliance. These measures included new command structures, doctrines, tactics, command-and-control-and-communications (C3) systems as well as logistical systems. Entire defense programs have been adjusted for the sake of interoperability. To emphasize and support interoperability, military personnel from the Baltic States and Poland, along with their allies, have been trained at NATO military schools and training centers along with universities and war colleges located in NATO and/or EU member states, including the US, Germany, the UK, France, Denmark, Poland, Sweden and Norway. This effort has created the necessary preconditions for NATO's effective chain of command and planning system. These efforts have proved their effectiveness during Expeditionary Operations and Peace Support Operations. Troops from the Baltic States and Poland have participated in Alliance operations in Iraq, Afghanistan, Kosovo, Somalia, Mali, etc.

But for reliable national and regional defense on the Alliance's eastern flank this is not sufficient. Beside the well-established and exercised NATO chain of command, close horizontal coordination and thorough interoperability between NATO neighbors is crucially important as well. Proper interoperability and a common operational readiness among the Baltic States and Poland, as well as the other allies in the region, will be an effective force multiplier for collective defense.

The democratic countries of the Baltic States and Poland have similar constitutions, defense strategies, and command and control systems. All four states have regular and active reserve forces and two of them, Estonia and Lithuania, have conscription. They are organized according NATO standards, and the vertical NATO chain of command is well established. But one particularly problematic issue remains: each country is developing its own Defense Strategy, which partially neglects the strategies of its NATO closest neighbors.

Unsurprisingly, the lack of a commonly accepted, long-term regional Defense Strategy will lead to a reduction of NATO's strategic depth. This is already visible. For example, each Baltic State is purchasing a different model of Infantry Fighting Vehicle (IFV). Lithuania invested the largest sum in its history for defense acquisitions when it agreed to the Boxer platform. Estonia invested in the CV90, and Latvia is purchasing the UK-produced CVR. Poland has its own agenda as well—with its relatively sizeable national defense industry complex, it is capable of supplying the Polish Armed Forces with its own homemade military hardware. Thus, unsurprisingly, it tends to use different weaponry in comparison to many of its regional NATO neighbors; for example, it produces and supplies its own troops with the Rosomak IFV. Differences are also visible in the acquisition of howitzer artillery systems: Lithuania has purchased the PZH 2000, while Estonia acquired Korean made K9s, etc. The presence of competing weapons systems in the region come with some obvious problems, including the need for different types of ammunition and logistics to operate and maintain them. This reduces the maneuver capability within NATO's territory and is much more expensive for each Baltic country.

Other negative implications must also be overcome. For example, the establishment of a NATO "military" Schengen Zone, enabling the free movement of military troops, logistics, and weapons between NATO countries is essential. We hope that in the nearest future this will be agreed and implemented among NATO members. This step will

improve NATO's strategic depth in Europe. But to maximize such a benefit, each country must be able to fully implement it. In this regard, we have some serious challenges—Lithuania, Latvia and Estonia still use the 1,520 mm gauge railway they inherited under the Soviet system. This is highly problematic since it is not interoperable with the Polish 1,435 mm standard gauge railway system. In case of a crisis, this disparity in rail road systems will greatly slow down NATO troop movement throughout the region, while it could be very effective for organized movement from Russia. Another transit infrastructure example is the roads. The roads between Lithuanian and Poland are much narrower and underdeveloped in comparison with the road system that connects Belarus and Russia. Therefore, the necessity of proper coordination and planning is obvious, and it must be done at all regional and national levels (not purely military). Failure to properly address these kinds of transit problems reduces NATO strategic depth in Europe for maneuver, mobility and logistics, which is vitally important for the effective defense of the region and the entire Alliance.

Building a common regional Defense Strategy is not an easy task. But with the right amount of political will in the region, it is possible. While coordinating national-level decisions across the region is difficult, Lithuania and Latvia provide positive examples. Thanks to the development of sufficient political will, the countries finally achieved the NATO goal to allocate 2 percent of GDP to defense (Estonia had long met this goal already). This all sounds optimistic, but one should remember that this 2 percent burden for defense is a peacetime NATO requirement; but can so-called Hybrid War be considered "peacetime?" Also, just recently, Lithuania's main political parties made an attempt to agree on a national long-term Defense Strategy. Not all sides agree on this proposal, but the majority do. Of course, an attempt is not equivalent to actually passing a long-term Defense Strategy—but the effort must at least be appreciated.

Franklin's quotation "we must indeed all hang together, or most

assuredly we shall all hang separately" is absolutely relevant in the Baltics today given the circumstances in the region. The improvement of regional interoperability via a long-term Regional Defense Strategy is crucial. It will be a force multiplier for NATO defensibility and will make deterrence more credible. However, to achieve this goal, the right level of regional political will to unite the effort is essential. This is a vital precondition before a Regional Defense Strategy can be formulated. Five years ago, this idea would have been thought impossible; but since then, this issue has become a matter of survival. The states of the region simply do not have another choice. Thus, this goal no longer appears unachievable. A common Defense Strategy in the region will build upon the horizontal interoperability between NATO neighbors as well as on the confidence in the continuity of national defense development. Therefore, recent national efforts among Alliance members to improve defense capability makes us feel more optimistic for a secure and prosperous future of the Transatlantic community.

1.4. Legal Aspects of Defense Cooperation

Ieva Miļūna, Edgars Poga

Introduction

The Baltic States' military cooperation is largely dependent on state sovereignty considerations but must also take into consideration their commitments to international organizations, mainly, the North Atlantic Treaty Organization (NATO) and the European Union. Against this background, military cooperation between the three Baltic States is legally possible within the framework of institutional cooperation, common procurement, common maritime and air-defense patrolling operations, and cross-border civilian cooperation. But it has to be stressed that this can take place within the framework of deterrence and not in case of an active armed conflict and defense. For the three Baltic States, it is not possible to have an integrated army in the operational and command sense.

NATO's Enhanced Forward Presence (EFP), which was established in the region in 2016, will coexist with the Baltic States' initiatives. The EU's Permanent Structured Cooperation (PESCO) reinforces the thinking of a common military within the EU region, but does not have a substantial impact on the Baltic States' common military cooperation initiatives.

This chapter will address the constitutional law aspects of the three Baltic States with regard to military cooperation. Then, it will assess the questions of status of forces in another State's territory as well as the legal immunities of these armed forces. Moreover, it will examine the crucial cooperation aspect of common procurement policies and procedures. Furthermore, the issue of transfer of authority and operational planning will be discussed. The chapter will then examine

maritime and air-defense patrolling operations. Finally, the institutional cooperation between the three Baltic States will be assessed. The chapter concludes with recommendations and conclusions with regard to the legal aspects of the Baltic States' military cooperation.

Constitutional Law Aspects

As the three Baltic States are free, autonomous and sovereign entities, their military cooperation largely depends on international law instruments (international agreements, memorandums of understanding) concluded between them on the basis of their interests and theory of consent. It is of crucial importance to mention Article 2 of the United Nations Charter, which stipulates the principles of sovereign equality of States and non-intervention in internal affairs of another State. Since national armed forces are an organ of a state, this means that, without a decision of the respective sovereign power base (either the parliament or the people), the unification of the three Baltic States' armed forces cannot occur. The constitutional laws of the Baltic States as well as international law do not permit military activities of a foreign state on the soil of another without the host's consent. In the case of Lithuania, its Constitution even stipulates that in implementing a foreign policy, Lithuania shall follow the universally recognized principles and norms of international law.[27] Similarly, the Constitution of Estonia establishes that "[g]enerally recognized principles and rules of international law are an inseparable part of the Estonian legal system."[28]

[27] Article 135 of the Constitution of the Republic of Lithuania, available at: <http://www3.lrs.lt/home/Konstitucija/Constitution.htm>, last accessed 12 August 2018.

[28] Article 3 of the Constitution of the Republic of Estonia, available at: <https://www.president.ee/en/republic-of-estonia/the-constitution/>, last accessed 12 August 2018.

The sovereign competence and decision of each of the Baltic States would allow them to create a common military or common defense forces at a command and operational level in order to react in a case of an active armed conflict. The constitutions of the three Baltic States prescribe that their national legislatures take strategic decisions with regard to the national armed forces and their response to an external military threat. So in other words, to create a common Baltic army, the issue will have to be decided by the national parliaments. For example, in Estonia, the parliament has to pass and amend the Peace-Time National Defense Act and War-Time National Defense Act.[29] Also, in Latvia, the Parliament determines the size of the Armed Forces during peacetime.[30]

In all three Baltic States, the president is the supreme commander of the national armed forces.[31] In Estonia[32] and Lithuania,[33] the president is assisted by the National Defense Council. In the case of Lithuania, it is specified that the government, the minister of national defense and the commander of the national armed forces are responsible to the parliament for the administration and command of the National Armed Forces.[34]

In cases of an active armed conflict, the parliament of each of the Baltic States—mostly at the proposal of the president—has the

[29]Article 104 of the Constitution of Estonia.

[30] Article 67 of the Constitution of the Republic of Latvia, available at: <http://www.saeima.lv/en/legislation/constitution>, last accessed 12 August 2018.

[31] Article 127 of the Constitution of Estonia, Article 42 of the Constitution of Latvia, Article 140 of the Constitution of Lithuania.

[32] Article 127 of the Constitution of Estonia.

[33] Article 140 of the Constitution of Lithuania.

[34] Article 140 of the Constitution of Lithuania.

competence to declare a state of war against an act of aggression and order mobilization.[35] However, in Estonia, the Constitution prescribes that the president may declare a state of war and order mobilization without even awaiting a resolution by the legislature.[36]

Since the decision to create a common Baltic States military concerns three sovereigns, it should be governed by international agreements. According to the constitutions of each of the Baltic States, the national parliament in every case is empowered to ratify international treaties.[37] The Constitution of Lithuania, in particular, stresses that treaties of a defensive nature related to the defense of the state shall be ratified by the parliament.[38] A similar provision is prescribed by the Constitution of Estonia.[39] Thereby, the governments of the Baltic States cannot enter international agreements that are in conflict with their constitutions[40]; and without the acceptance of their parliaments, they cannot create common operational and command military structures.

In principle, the Baltic States' military cooperation can be governed by memorandums of understanding (MoU). However, contrary to existing practice in Latvia, in case they govern the Baltic States'

---

[35] Articles 65, 78 and 128 of the Constitution of Estonia, Articles 43 and 44 of the Constitution of Latvia, Articles 67, 84 and 142 of the Constitution of Lithuania.

[36] Article 128 of the Constitution of Estonia.

[37] Article 65 of the Constitution of Estonia, Article 68 of the Constitution of Latvia, Article 67 of the Constitution of Lithuania.

[38] Article 138 of the Constitution of Lithuania.

[39] Article 121 of the Constitution of Estonia.

[40] See also: Article 123 of the Constitution of Estonia, Article 105 of the Constitution of Lithuania.

common military command-and-control (C2) structures, they have to be ratified by the Baltic States' parliaments according to the legal reasoning provided above. These kinds of MoUs will determine the purpose and principles of military cooperation, state investment, common military C2 and transfer of it to the commander of another state, as well as jurisdictional issues and the use of force.

It may be possible that during an active armed conflict, a common organ of the three Baltic States is created, similar to the Coalition Provisional Authority that was established in Iraq, in 2003. In this case, it will have to comply with Article 68, paragraph 2 of the Constitution of Latvia, which states that, upon entering into international agreements, Latvia may delegate a part of its state institution competencies to international institutions, but that it has to have a quorum of 2/3 of members of parliament present at the session and 2/3 voting for this agreement. This aspect will be further analyzed below, in the subsection "Institutional Cooperation."

Status of Forces in Another State's Territory

In cases when foreign armed troops are stationed or moving through another state's territory, Status of Forces Agreements (SOFA) have to be concluded. NATO SOFAs[41] can be used as a model because they stipulate obligations to respect the host State's laws, criminal and disciplinary jurisdiction and compensation of damage.

Usually, SOFAs take into account the states' interests and positions with regard to the applicable international and national laws. These kinds of treaties will also have to be ratified by the Baltic States' parliaments. For example, the Constitution of Lithuania specifically

[41] Agreement between the Parties to the North Atlantic Treaty regarding the Status of their Forces, available at:
<https://www.nato.int/cps/en/natohq/official_texts_17265.htm>, last accessed 12 August 2018.

stipulates that the international treaties on the presence and the status of the Armed Forces of Lithuania on the territories of foreign states are ratified by the legislature.[42]

The potential SOFA concerning the Baltic States' common military cooperation will determine whether the host or the home state's laws apply in cases of troops being stationed in another Baltic State's territory. In addition, the issues of applicable laws to exercise criminal and disciplinary jurisdiction will be determined. With regard to possible damage and similar issues, compensation will be established as a matter of state and individual responsibility.

Moreover, the three Baltic States need to emphasize the importance of establishing a "military Schengen area" in their communication with NATO and the EU, as it would enable more effective force movement for already established EFP (especially, if they are involved in an active armed conflict) and national forces through another Baltic State's territory.

Immunities

The immunities of the Baltic States' national armed forces members will have to be regulated in international agreements between them. These will be questions of jurisdiction of one or another Baltic State with regard to issues of violations of international law and the prospects of state immunity for certain claims and immunities of individuals for criminal offenses and international crimes. These agreements will govern the immunities of military and civilian personnel as well as supporting personnel, in addition to their property, funds and assets to be subjected to either civil or criminal jurisdiction of the respective Baltic State.

[42] Article 138 of the Constitution of Lithuania.

Common Procurement

The Baltic States can establish common procurement procedures for the acquisition of technology and weapons. Under current international legal frameworks, there are no obstacles for that. It would, thus, be efficient to agree on the procurement of equipment and to create common schools to provide training and common platforms of maintenance, except for the implementation of common C2.

Procurement in the military field is governed by EU Directive 2009/81/EC of the European Parliament and the Council of July 13, 2009, on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defense and security.[43] It lays the foundation for general defense procurement, which has been brought forward by the European Defense Agency.

Of crucial importance is the necessity to develop either an institution or an agency that would tackle the issues of common procurement of ammunition, fuel and other necessities for the Baltic States' armed forces. The said agency or institution would be formed by experts or project managers from the respective Baltic State defense ministries, specifically in the field of procurement. As noted by Latvian Land Forces commander Colonel Ilmārs Lejiņš, "Said institution/agency could serve as a catalyst for national bureaucracy, achieving synergy in interaction with NSPA and other international actors using a more long term approach. Weapons and platforms may be different, but in most cases ammunition is the same."

[43] Directive 2009/81/EC of the European Parliament and of the Council of 13 July 2009 on the coordination of procedures for the award of certain works contracts, supply contracts and service contracts by contracting authorities or entities in the fields of defense and security, available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009L0081>, last accessed 12 August 2018.

Additionally, there is a necessity to have a bottom-up approach (tactical-strategic) across the Baltic States' structure, which would allow for effective procurement efforts to be put forth and for efficient cooperation projects to be established. The Baltic Defense College (BALTDEFCOL) could be used as a platform for such a procurement approach.

Transfer of Authority, Operational Planning

The transfer of authority, operational planning and common C2 are the most sensitive aspects in light of the Baltic States' sovereignty concerns. If pursued, this would take place within the legal framework of Operational Plans (OPLAN), which determine: 1) the international mandate established by international agreement between the Baltic States, the applicable law, self-defense issues and international humanitarian law principles; 2) detailed rules on the use of force; and 3) progress of operation or operational order. The creation of one Supreme Military Commander over the troops of all three Baltic States would raise discussions at the national parliaments, defense ministry HQs and society.

The Baltic States' armed forces will have to observe both the NATO Rules of Engagement (RoE) as well as national ROEs. Of course, the national RoEs may be influenced by particular national laws and interests.

Politically, the transfer of authority and operational planning could be stipulated through the development of either a command-and-control structure or an HQ, which would operationalize the Joint Operation. They will not replace national responsibilities or freedom of National Armed Forces but will become an information HQ for operational and tactical conversations and planning. The primary aim of such a structure would be the operationalization and synergy of the Baltic States' national structures. The said HQ can be tackled via the framework of the NATO 360-degree security approach or on the basis

of the three Baltic States' existing structures, such as BALTDEFCOL or the Baltic Assembly.

Maritime and Air-Defense Patrol Operations

Maritime cooperation and joint operations should take place in accordance with the main principles of the law of the sea and the United Nations Convention on the Law of the Sea (UNCLOS). Article 30 of the UNCLOS treaty prescribes that if a warship of another state does not comply with the coastal state's demands in the latter's territorial waters (which is 12 nautical miles from the coast), it can be asked to leave the territorial waters immediately. In accordance with Article 31 of UNCLOS, the flag state shall bear responsibility for any loss or damage to the coastal state that results from non-compliance with the coastal state's demands.

Strategically, the Baltic States should establish a common maritime patrol operations plan. As part of this plan, they will also need to deal with issues transfer of authority, operational planning and C2, as discussed in the previous chapter. Especially, this concerns the cases of a possible active armed conflict at sea. In such an event, it may be of crucial importance for the Baltics to cooperate with the non-NATO countries bordering the Baltic Sea, namely, Sweden and Finland.

With regard to air-defense patrol operations, currently, the NATO air-policing mission is regulated by MoUs. Also, the Baltic States have concluded an to carry out the research and analysis of future air-policing after 2018.[44]

[44] Memorandum of Understanding between the Ministry of Defense of the Republic of Latvia, the Ministry of Defense of the Republic of Estonia and the Ministry of National Defense of the Republic of Lithuania concerning a Common Analysis of the Options of Air Policing in the Baltic States after 2018, available at: <https://likumi.lv/ta/id/198243-memorandum-of-understanding-between-the-ministry-of-defence-of-the-republic-of-latvia-the-ministry-of-defence-of-the-republic-o...>, last accessed 12 August 2018.

Cross-Border Civilian Cooperation

For the purposes of cross-border civilian cooperation, it is necessary to develop a trilateral Baltic States' policy involving laws, procedures and doctrines linked to crisis management. This may also entail the utilization of NATO military command structures for effective crisis management involving civilians.

It would be advisable to use NATO recommendations with regard to areas of regional shortcomings—thus, enhancing intra-regional cooperation. Such an approach promises to improve the capacity of the three Baltic States individually while retaining their sovereignty, but fostering cooperation in the common security areas.

Institutional Cooperation

Each of the Baltic States should tackle its own area of expertise. For example, for Latvia it is Strategic communication, for Estonia—Cyber defense, for Lithuania—Energy security, as exemplified by the NATO Centers of Excellence on their respective territories. An intra-regional approach should enforce their strengths while tackling shortcomings during peacetime and in the middle of a crisis.

NATO's presence and help with incentives fostering intra-regional cooperation should be emphasized both during the policy development phase and afterward, thus, using it as a cover for not only the organization's effectiveness, but also regional security.

For active armed conflict, it is possible to establish a common organ, akin to the Coalition Provisional Authority in Iraq, established in 2003. Such an organ would deal not only with administrative issues, but also common operational C2. It would be a C2 structure or an HQ, which would operationalize the Joint Operation, as discussed above ("Transfer of Authority, Operational Planning").

Way Ahead

At present, the Baltic States' constitutions do not permit creating common military forces in the sense of a shared army. For this purpose, constitutional amendments would first have to be made.

International law agreements can govern the cases of status of forces in another state's territory, the applicable law and immunities. However, in case of an active armed conflict, they will largely be dependent on the constitutional amendments of the Baltic States and the legal interests that each of them will try to protect. Also, the transfer of authority and common operational C2 are sensitive enough, but highly advisable to be discussed at the current stage.

The Baltic States can still effectively collaborate militarily with regard to institutional cooperation, common procurement, common maritime and air-defense patrolling operations and cross-border civilian cooperation. For an active armed conflict situation, this will reinforce the strengths of the Baltic States to resist any external threat or destabilizing force.

1.5. Expert Recommendations

1. Create a common Baltic defense strategy.
2. Create a common strategy for use of national guards and reserves.
3. Develop an intra-regional Host Nation Support (HNS) system. Improve communication/cooperation with civilian side of HNS and beyond. Work with NATO to create a common reinforcement and HNS strategy.
4. Form a Joint B3 Crisis Secretariat with associated staff, infrastructure and communications. Standardize the crisis-management policies, procedures, processes and laws across all three states. Improve cooperation on cross border operations in crisis and pre-crisis "gray" times.
5. Synchronize defense terminology between Estonia, Latvia and Lithuania.
6. Synchronize communication toward allies and partners, raising their awareness of B3 national and intra-regional capabilities and limits. Give NATO a common set of requirements for support.
7. Form a two star headquarters (HQ) to manage joint operational area. Establish a Mobile Division HQ, promoting a flexible response, planning to be proactive.
8. Review investments in Defense Infrastructure, prioritizing mobile over static.
9. Promote joint procurement by establishing common procurement procedures across B3 national legislations, creating a B3 common market for military industry. Create a joint B3 Ammunition Agency and a joint B3 Fuel Agency linked to other NATO agencies.
10. Create a B3 "Military Schengen" as a precursor to the European Military Mobility Initiative
11. Improve joint Baltic system of situational awareness and early

warning.

12. Enhance maritime defense by establishing a Baltic Squadron and/or joint coastal defense system.
13. Enhance air defense by establishing joint command and control (C2).
14. Analyze and assess an adversary with the premise of B3 being a sub-target of NATO in the adversary's plans.
15. Enhance Joint Exercises and shared capabilities accomplishing economies of scale, using Whole of Government Approach.
16. Consider amending either the B3 constitutions to make them more flexible and efficient to react in cases of an active armed conflict in order for the Baltic States to act through concerted actions and operations, or concluding international agreements to be further ratified by the national parliaments. It is for top-ranking military officers to examine the current *status quo* of opinions with regard to common operational and C2 issues between the Baltic States in case of integration of B3 forces, stationing of foreign military forces, transfer of authority and operational planning, as well as the responsibility of the state in commanding a common armed forces organ.
17. Empower the new Divisional HQ to lead on development of multinational combat issues for the three states. This should include cross-border combat, use of National Guard and reserves, reinforcements and all associated issues.
18. Work with NATO and allies to create an immediate reserve of brigade size for the three states
19. Work with NATO and regional allies to create a common air-defense strategy. Identify if eFP can be used to deploy air-defense units instead of more infantry. Create a more robust BALTNET air-defense control system.
20. Work with NATO and allies to create a common maritime strategy with a standing operations center for the Baltic Sea Region. Create a regional risk management plan (RMP).

21. Create a regional strategic course for senior officers and politicians at BDCOL to teach and discuss intra-regional interoperability.

2. SOCIETAL SECURITY AND RESILIENCE

2.1. Expert Assessment

Olevs Nikers, Otto Tabuns, Alina Clay, Ēriks Kristiāns Selga, Rasa Zdanevičiūtė, Vytautas Keršanskas, Laima Zlatkutė, Ivo Juurvee

Within international institutions such as the European Union and the North Atlantic Treaty Organization (NATO), "societal resilience" has become a new catchphrase, emphasizing a holistic, all-of-society approach to, among other things, responding to modern, hybrid-related security threats. Integrating a society-based strategy in traditional defense and military discussions and decisions is a particularly notable development, and a positive one at that. Furthermore, as the world is becoming more globalized and thereby more complex, societal resilience alludes to appropriately responding and adapting to the myriad of sociopolitical issues that arise. In the context of the Baltic States, societal resilience is critical to the fundamental survival and sovereignty of these geographically small countries—their joint population being just 6.2 million—juxtaposed against their opportunistic eastern neighbor.

On the one hand, this concept is nascent and therefore still in the early stages of evolution. On the other hand, efforts toward bolstering societal security and resilience are underway and being adopted in a number of sectors, especially since the 2014 Russian intervention into eastern Ukraine. That is, increased attention has been given to societal security and resilience in such sectors as defense, the economy,

politics, infrastructure and civil society. Efforts advancing intra-regional cooperation have included identifying and mapping regional risks and establishing methodologies to analyze risk threats and capabilities. Specifically, in-country examples include military trainings and curriculum innovations for youth in Latvian schools; the reintroduction of conscription in Estonia and Lithuania; the national total defense strategy implemented once again in Latvia; and attention in all three Baltic countries in varying degrees toward bolstering media literacy and critical thinking in the education sector.

Unfortunately, lingering fragmentation of capacity-building and initiatives toward societal security and resilience in the Baltic States contributes to their collective vulnerability and unpreparedness for increasingly complex and unexpected hybrid threats and attacks.

Intra-regional (Estonia, Latvia, Lithuania) cooperation takes different formats depending on the subject.

Broader intra-regional cooperation exists in the field of culture—notably, activities that promote European culture and culture of the Baltic States, national and European values, languages, protection of Baltic heritage and history, enhancement of patriotism, etc.—and ends up indirectly enhancing societal resilience. Yet, levels of Baltic State cooperation are significantly more varied in the area of media policy.

When it comes to intra-regional cooperation on culture, the three countries have an active and successfully operating format of the Baltic Cultural Committee of Senior Officials, which meets annually at the ministerial level. Cultural cooperation guidelines are provided by the Program of Cultural Cooperation, signed between all three ministries of culture, a current program in operation from 2015 to 2018. Trilateral initiatives and the program agreement currently include: exchange of information between the ministries on legislative initiatives, acts and policy documents, Kremerata Baltica, Baltic

Museology Summer School, cooperation on the 100th anniversary program, cooperation in the field of film and audio-visual production, the Festival of Contemporary Baltic Drama, the Baltic Dance Platform, the Baltic Architects' Unions Association (BAUA), cooperation on preservation and promotion of properties inscribed on the UNESCO lists (Song and Dance Celebration Tradition, the Baltic Way), cooperation within the formats of international organizations and European Union, etc. This cooperation is implemented within the programs of the ministries and cultural support foundations of all three countries.

Furthermore, the Baltic Culture Fund has been established within the framework of the Baltic Assembly. Other successful formats include the Baltic Heritage Network (Martynas Mažvydas National Library of Lithuania is an active participant) and Baltic Heritage Group meetings (Department of Cultural Heritage under the Ministry of Culture participates there).

Intra-regional cooperation in the media policy area is more prevalent between Lithuanian and Latvian ministries, as they share a similar approach towards the media sector (both in Lithuania and in Latvia there is a tendency towards regulation of the media sector, while Estonia leans toward deregulation).

Cooperation between the Lithuanian and Latvian ministries is usually informal; officials exchange relevant information (e.g., about the same media service provider that targets Lithuanian and Latvian minorities) and discuss common goals and strategies (for example, in the format of the review of the Audiovisual Media Services Directive, both ministries advocated for the inclusion of an "extra urgent case procedure," media transparency rules and stronger rules pertaining to cooperation between regulators). Existing institutional cooperation is considered normal, but there is space for improvement. The main obstacle to closer regional cooperation is at times excessive

concentration on national issues, which leads to disregard of common regional interests of strategic importance.

In the field of societal security and resilience a perfect example of cooperation is the collection of Centers of Excellence (CoE) established in Baltic Capitals and Helsinki: NATO Cooperative Cyber Defense CoE, NATO Energy Security CoE, NATO Strategic Communication CoE and the European Center of Excellence for Countering Hybrid Threats. Although these organizations are focused on wider-scale international cooperation, they are also useful umbrellas for supporting intra-regional cooperation. A good example of how things should work is the NB8 (eight Nordic-Baltic countries: Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, Sweden) launched by NATO StratCom Coe in Riga, which regularly brings together practitioners and academics from these eight countries in order to exchange information and best practices in the field of strategic communication. It also demonstrates that intra-regional cooperation does not have to be limited to just the B3 but can include additional partners.

Some previous scholars have pointed to the Nordic model as an ideal one for other countries to embrace. Indeed, emulating the Nordics is especially relevant for the Baltic countries due to geographical proximity and some shared cultural traditions and history. And generally speaking (there is of course cross-country variance), the Nordic region's embodiment of societal resilience reflects an empowered and active civil society. Yet, while the Nordic model presents a goal for the Baltics to strive to attain, much work remains. For example, non-government institutions are plagued by little financial support and resources in the Baltic States, which, in turn, hampers the long-lasting impact and community capacity-building needed to advance intra-regional cooperation and societal resilience.

Despite the exposure and recurrence of these concepts on the international institutional stage—regularly analyzed and discussed in

a number of publications and conferences both at NATO and the EU—societal resilience is not addressed as often in high-level national security and defense discourses across the Baltic States, nor has it yet entered the social consciousness of the Baltic populations. The latter assessment could be easily made for a number of Western societies, as many of them struggle today to address hybrid threats and attacks in their political and media spaces; in sum, the Baltic States are not alone in this regard.

Due to the newness of societal resilience as a working term in this region, some of the issues and challenges we see may be partially remedied with time and governmental attention, although the institutional weakness of non-governmental organizations (NGO), discussed in more detail below, may continue to present a serious challenge. In this case, there must exist a deeper understanding, and, more importantly, a capacity and willingness for action and financial support, within the highest levels of decision-making authority to empower non-government institutions, as they are the critical actors in achieving the formula for societal resilience.

Relevant to total defense capacity-building, the Baltic States should work together to achieve strategic communications. This strategy could partially be carried out by non-governmental stakeholders, like community civil society groups, businesses, and schools, if provided with sufficient resources and easy-to-understand instructions. Furthermore, the Baltic States can benefit from being influenced by and adhering to NATO security culture, attitudes and norms, in the framework of societal resilience.[3] NATO has increasingly cast attention and funding toward advancing societal security, and this topic was notably discussed at the 2016 NATO Summit in Warsaw.

Sharing best practices and lessons learned regarding media literacy training and education should be developed, especially in the most vulnerable communities of each Baltic State (i.e., near the eastern borders). Currently, no such intra-regional efforts exist. One positive

step is that Latvia will be rolling out official media literacy curricula accessible to all education instructors across the country, thanks to the efforts of a notable education NGO, the Education Development Center, in collaboration with the Ministry of Culture, in the summer of 2018. If this kind of effort is implemented on an intra-regional level, critical thinking would be advanced, as would the intellectual security of individuals, particularly among students.

Multi-stakeholder involvement and project management must be integrated into the intra-regional framework of societal resilience. Active community stakeholders—from policy centers to think tanks, from academic institutions to NGOs—in all three Baltic States should be both more cooperative and vigilant in identifying and applying for various international grants and programs that help to bolster societal resilience. For example, the United States' Global Engagement Center has recently released a funding opportunity entitled the "Information Access Fund" that calls for local stakeholders to submit program applications that commit to fighting disinformation and promoting societal resilience. EU-level grants are also a possibility, such as Jean Monnet Projects. And international entities, including Konrad Adenauer Stiftung, the National Endowment for Democracy, the Foreign Policy Research Institute, the Swedish Foundation for Humanities and Social Sciences, and embassies scattered across the Baltics additionally offer grants that can be used to promote societal resilience and civic education.

Elaborating on the aspect of institutional cooperation, NGOs across the Baltics are perceived to be—and historically have been—institutionally weak, plagued by constrained finances and resources to design and implement community-based projects and initiatives. Moreover, they often lead individual efforts, and therefore projects instituted in one Baltic country are not spread nor extended to another. This phenomenon mirrors the intra-agency efforts as well, which is fragmented and could be stronger in cross-communication and cooperation. Together, these are critical weaknesses for within-

country and intra-regional efforts toward societal resilience. It is often the case that civil society groups foster the strongest, most durable linkages and trust among local citizens of all ages, and civil societies in the Baltics are no exception. The potency of NGOs' reach and impact in the Baltics is thereby severely constrained by the insufficient funding they receive from the respective Ministries.

The increasing role of social media within the information space and digital market economy, combined with growing hybrid threats, demonstrate the need to include a wider definition of security in drafting policy options. This is especially true for the Baltic States, which are routinely a testing ground for Russian political instruments designed to gain influence over power and resources as well as to divide the Baltics from their Western. The policy implications should consider the interactions between national decision-makers and domestic social groups, addressing societal security as a fundamental aspect in dealing with the resilience and cohesiveness of a society of each Baltic State.

The Baltic governments need to create a broader public discussion on security, defense matters and intra-regional security in order to capitalize on the widespread general public interest in these subjects domestically. Baltic countries also have to build up a joint approach to dealing with financial, economic and energy threats, including cyber-attacks on strategic infrastructure.

A report by the Washington-based Center for European Policy Analysis (CEPA) found Russian strategy to be highly adaptive on a country-by-country basis, with disinformation targets ranging from specific individuals to the political health of the state.[45] The European

[45] Edward Lucas and Peter Pomeranzev, "Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe," *Center for European Policy Analysis*, August 2, 2016, available https://www.cepa.org/winning-the-information-war.

Union's East StratCom Task Force[46] has also highlighted Russia's use of different tools in different areas. NATO's STRATCOM accentuates this trend.[47] Campaigns directly targeting Russian-speaking minorities in the Baltic States purposely fill Central Europe with "alternative" websites and flood them with comment trolls. Vulnerabilities are carefully sought out to create fitting narratives for the target audience.

Thus, intra-regional cooperation faces a significant obstacle beyond the awareness and tracking of disinformation campaigns, which, in itself cannot extract the full benefit from transnational cooperation while there are different extents of resources and strategies allocated to following the threat. Concurrently, high-level political cooperation in the matter is strong. The idea of Russian disinformation is common knowledge across the three neighboring states, and efforts to increase this public awareness originate from the top. The presidents of the Baltic States—Latvia's Raimonds Vejonis, Lithuania's Dalia Grybauskaite, and Estonia's Kersti Kaljulaid—have all taken strong public stances against malicious disinformation campaigns by affirming their existence and leading various response efforts.

The combined initiatives of Baltic leaders, the public sector, and the private sector, which consistently echo charges of the Russian disinformation threat, aid in forming awareness of the problem. As a result, Baltic populations are more critical when analyzing the media and less susceptible to modern information warfare tactics. Most importantly, the nudging within different levels of society has raised awareness without panic against Russia or other possible perpetrators. Information warfare is considered similar to hacking—a matter of daily life that must be dealt with.

---

[46] EU East Center for Strategic Communication, accessed July 19, 2019, available https://euvsdisinfo.eu/.
[47] NATO StratCom Center of Excellence, accessed July 19, 2019, available https://www.stratcomcoe.org/.

Nevertheless, the most active area for cooperation is strategic communication (StratCom). StratCom representatives from the Baltic ministries of defense hold annual or biannual meetings to exchange information and coordinate positions and messages before major events, exercises, etc. Military StratCom representatives also cooperate on a number of initiatives. For the past two years they have been engaged in a pilot project developing a virtual platform that enables sharing information about adversarial influence operations (directed against Baltic States, NATO, eFP, etc.), whereby producing a timeline that simultaneously shows what is happening in each country. At the same time meetings and workshops for sharing best practices and lessons learned, as well as briefings for visiting officials on information security are continuously organized. Finally, information operations specialists from the Baltics are also engaged in cooperation together with their Polish, US and Canadian counterparts.

Resilience is also closely related with the Host Nation Support (HNS) mechanism, whereby civilian and military assistance is rendered to deployed allied forces. To ensure preparedness to provide HNS, the Baltic States hold annual exercises (Baltic Host) to enhance coordination and interoperability both among the Baltics and allies, as well as between military and civilian institutions.

The Baltic States together with the US have also been involved in an initiative focused on developing an approach to resistance as a means of national defense. This initiative has two major features. First, it is directed toward developing an approach that encompasses whole-of-government and whole-of-society activities. Second, the initiative addresses national resilience as an ability of a nation to withstand aggression and regain sovereignty.

Two main (interconnected) aspects may prevent more prominent cooperation on societal security and resilience among the Baltic States. First of all, since the purpose of an adversarial hybrid strategy

is to find vulnerabilities of an individual country and exploit them, the execution of this strategy will be different for every given country. Therefore, although the challenges that the Baltic States face may be of the same general nature or emanate from the same source, they will be different in the nuances of their scope, manifestation, etc., depending on the conditions of each country. These differences are key to how particular issues are or should be addressed, meaning that the solutions employed by the states must be tailored to their specific situations. Second, the view shared among NATO and EU member states is that resilience is, first and foremost, a national responsibility. Therefore, states are more focused on identifying and addressing national issues pertaining to resilience.

2.2. Taking a Hybrid Governance Approach Against Hybrid Warfare: Lessons From National Cyber Security Incident Response Teams

Ēriks Kristiāns Selga

Introduction

In 2014, the Russian occupation of Ukraine with the use of a modernized doctrine of hybrid warfare awoke the hibernating concerns about Russian military aggression that might be directed at the Baltic States and their allies. The West hurried to secure the Baltic region from the most immediate, conventional military threats; and the result of the cooperation has been hailed a success.[48] But cooperation on defending against the other facet of hybrid warfare—"nonviolent subversion"—continues to pose a challenge,[49] particularly, in attempts to multilaterally build societal resilience and security among the Baltic States. The following study charts several of the most important practical difficulties in fighting against information disorder, draws comparisons with the challenges faced by the markedly similar national cybersecurity incident response teams (NCSIRTS),[50] and outlines recommendations to guide Baltic and

[48]Justinas Mickus, "Baltic Security Situation: A Short Overview Santrumpa ..." EESC. 2016. Accessed August 18, 2018. http://www.eesc.lt/uploads/Baltic-Security-Overview-EESC.pdf.

[49]Radin, and Andrew. "The Potential for Russian Hybrid Warfare in the Baltics." RAND Corporation. February 23, 2017. Accessed August 18, 2018. https://www.rand.org/pubs/research_reports/RR1577.html.

[50]When referring to NCSIRTs I also include national cybersecurity response teams

Western policymakers in structuring a foundation for approaches to societal security.

Challenges to Building Baltic Societal Security and Resilience

The difficulty in building systematic cooperation measures against the soft elements of hybrid warfare is underpinned by the high level of subsidiarity, unpredictability and virality of their proliferation. Disinformation campaigns, for instance, are highly reactive to localized events, often of only contextual significance. Language barriers can isolate such campaigns to only one nation. The campaigns also traverse a variety of mediums, ranging from traditional television and radio media, to digital news outlets, digital social media, to targeted religious, non-profit, and academic institutions. Their messages exploit different strata of society, and can be aimed at various age groups, ideological orientations or other differentiators. The content can be localized, but denounce an extraterritorial instance, or focus on inciting against another domestic entity. Disinformation strains with local success are immediately amplified through an omnipresent echo chamber of different communication channels, translated into other languages, adapted for different localities, and reverberated.

Disinformation campaigns are also difficult to reign in, once identified. Ones that spill over into different countries then have to be individually rebutted by the country of origin. Such falsities further have to be retracted internally, depending on what segments of society were permeated. This is a particularly demanding task because how individualized and rapid the delivery of messages can be. Furthermore, any attempts to confront disinformation necessitate substantial evidence and investigation before being challenged and removed by authorities, by which time the campaign has potentially lost relevance. Authorities acting against disinformation with higher

(CERT).

executive freedom risk being challenged for overstepping Western values, like freedom of media or speech. Each challenge can further be mixed into the cycle of disinformation, to sustain the information fog.

The disinformation tool is also difficult to measure when it comes to consequences. It is unclear to what extent disinformation impacts its target audience, be it on an individual or a group.[51] Moreover, no clear understanding exists regarding how disinformation affects society over extended periods of time or whether halting a certain message is reflected in the recipient audience.[52] Concurrently, it is difficult to understand the impact of a viral campaign in the short term, beyond the political destabilization caused by confusion alone.[53] The gaps in the aforementioned measurements significantly reduce the ability to prepare against the threat, even in budgeting—if the potential damage caused by disinformation is unclear, proportional resources for their mitigation cannot be calculated.

Anti-Hybrid Cooperation Frameworks in the Baltic States

The nature of disinformation campaigns challenge contemporary bureaucratic and centralized international cooperation efforts, and new systems of cooperation must be considered, reflecting the particularities of disinformation. The BSSP working groups recommended various intergovernmental strategies that should be undertaken. Institutions responsible for long-term integration and social resiliency building should share best practices, as should short-term incident responders. Particular attention was devoted to the

[51]Joshua Tucker, Andrew Guess, Pablo Barbera, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature." *SSRN Electronic Journal*, 2018. doi:10.2139/ssrn.3144139.

[52]Id. at 4.

[53]Ibid.

shape of the institutional cooperation. Proposals included using existing organizations, like the Baltic Assembly, as a starting point. However, the novel challenges posed by modern disinformation call for novel operational set-ups. Inspiration could be found in the collaboration systems of NCSIRTs. Trans-border challenges faced in the realm of disinformation parallel those of cybersecurity. In both cases, the threats can have a localized impact, traverse borders through the digital medium, and may generally only be remedied by subsidiary entities. Both benefit from intelligence and best practice sharing, and isolation is detrimental.

Generally, the primary role of an NCSIRT is to be a country's contact point for information sharing and coordination in the area of cybersecurity threats, both aimed and wanton.[54] NCSIRTs differ greatly in organizational setup, authority, authorization, function and funding structures among states.[55] Great schisms exist between the maturities of different NCSIRTs, denoting different resources, experience, and capabilities.[56] A prevented or successfully defeated cyberattack may go unnoticed in a different jurisdiction. Thus, NCSIRTs often have to share intelligence or best practices as well as give warnings and expediently react to received information. If a "cyber-fire" starts in any part of the globally enveloping "cyber-forest," it risks spreading to other states directly, or indirectly via political or economic shock.

In the EU, the so-called NIS Directive, which sets baseline cooperation

---

[54] Joseph Nye. "The Regime Complex for Managing Global Cyber Activities". GLOBAL COMMISSION ON INTERNET GOVERNANCE, No. 1. 2015.

[55] Michael Miora, et al. "Computer Security Incident Response Teams." *Computer Security Handbook*, 2015. doi:10.1002/9781118820650.ch56.

[56] John Haller et al., "Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability." 2010. doi:10.21236/ada536721.

rules for NCSIRTs, came into force only three years ago. It requires that states designate a CSIRT, a competent authority, single point of contact, and forms a cooperation group that must, to some extent, work with other national entities.[57] The approach is minimalistic, mainly setting in stone the current paradigms of self-regulation. NCSIRTs, for example, can exist as non-governmental organizations, integrated governmental organizations, or independent governmental institutions, while being bound to different government constituents.[58] The NIS Directive successfully avoids over-formalization and allows for organic trust-based growth, which underpins much of international NCSIRT cooperation. As transnational organizational resiliency building would be a new effort for the Baltic States, and would require cooperation among various levels private and public entities, similar groundwork may ease the beginning stages of cooperation efforts.

Recommendations for Setting up Trans-National Baltic Cooperation

The structure of cooperation between NCSIRTs as set by the EU's NIS Directive offers a starting point for Baltic policymakers. BSSP working groups highlighted the necessity of building resiliency through both short-term and long-term measures, with concurrent collaboration taking place at various levels of vertical hierarchies. A competent authority should be selected in all three countries that would liaison among each other, decide and disseminate pan-Baltic strategies to their stakeholders. A few points of contacts could be created in each of the Baltic States, with equivalent mandates. One, for example, could concern short-term crisis response teams—disinformation fire-fighter teams. These could involve hotlines between relevant leaders. Another could concern long-term measures aimed at developing

[57] Ibid.

[58] Ibid.

long-term societal resilience and security. This point of contact could regularly exchange working best practices. Minimum cooperation could be set as a requirement between the three states to secure intelligence exchange between the relevant authorities.

Policymakers should also focus on the strengths allotted by cooperation among the states, which is a strong understanding of the cultural nuances of their respective populaces and information spaces. This knowledge should be collected, aggregated and used to study regional tendencies. Data should be amassed to understand the underlying operations of disinformation sources. Disinformation may underpin broader paradigm shifts in underlying political communication, and the Baltic States should invest in understanding the modalities of their respective communication flows among institutional, media, private and public actors.[59]

Leaders should also consider raising their voices in favor of requiring more cooperation between governments and technology firms, which are rapidly becoming more successful at automating sources of disinformation.[60] Any initiatives should be cross-referenced against allied efforts, especially NATO and the European Union. Among other efforts, the North Atlantic Alliance has actively been bolstering cooperation through its excellence centers, while the EU has recently formed a Hybrid Fusion Cell.

---

[59] Lance W. Bennett and Steven Livingston. "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions." *European Journal of Communication*33, no. 2 (2018): 122-39. doi:10.1177/0267323118760317.

[60] Tom Wheeler, "Using "public Interest Algorithms" to Tackle the Problems ..." Accessed August 18, 2018. https://www.brookings.edu/blog/techtank/2017/11/01/using-public-interest-algorithms-to-tackle-the-problems-created-by-social-media-algorithms/. And Tacchini, Eugenio, Gabriele Ballarin, Marco L. Della Vedova, Stefano Moret and Luca de Alfaro. "Some Like it Hoax: Automated Fake News Detection in Social Networks." *CoRR*abs/1704.07506 (2017):

Lastly, when discussing fledgling intergovernmental networks, consideration must also be given to the form of governance. Classic vertical hierarchies of international organizations are not able to provide the reaction time and holistic interoperability of the NCSIRT networks. Leaders should beware of creating purely vertical hierarchal power structures and recognize where allowing high levels of subsidiarity may bring the best results. US scholar and former Director of Policy Planning at the State Department, Anne-Marie Slaughter's, findings on power securement may be a helpful guide: when parties do not have direct control over the stakeholders in an effort, individual state power should be secured by adding value and finding mutual benefit, not isolating responsibilities.[61]

[61] Anne-Marie Slaughter, Filling Power Vacuums in the New Global Legal Order, Boston College Law Review 919, Boston College International And Comparative Law Review (Boston: 2013).

2.3. Defeating Disinformation Threats

Dalia Bankauskaitė, Vytautas Keršanskas

Introduction

Russia, to a smaller or larger extent, has deliberately challenged the Baltic States on both the domestic and international levels since the breakup of the Soviet Union. After Russia waged unannounced war against Ukraine and occupied and annexed Crimea in 2014, the Western security community conceptualized these Kremlin tactics as "hybrid warfare." And while the search for most accurate phrasing to describe this *modus operandi* is still in progress in the West, the Baltics look at the issue from a much less theoretical and more practical point of view—it is a reality for them and a constant strategic challenge, which occasionally features new elements but whose general content does not change.

A report on hybrid warfare published by the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) suggest Russia possess the following range of hybrid tools that it utilizes against foreign countries:

- Propaganda;
- Fake news;
- Strategic leaks;
- Funding organizations;
- Political parties;
- Organized protest movements;
- Cyber tools for espionage, attack and/or manipulation;
- Economic leverage;
- Proxies and unacknowledged war;

- Paramilitary organizations.[62]

However, the experience of the Baltic States proves that even this extensive list is not definitive. In the last decade and, especially, with the increased tensions between the West and Russia, related to Russia's invasion of Ukraine, the Baltic States have also been targeted by other measures that would perfectly fit the notion of hybrid attacks:

- Sabotage of strategic infrastructure and energy;
- Border violation by intelligence and (officially unconfirmed) military troops;
- Large-scale offensive military drills;
- Threats of military attack; among others.

Such multidimensional threats require not only a comprehensive analytical approach by security experts, academics, policymakers and implementors, but also a developed national as well as multinational approach to practically counter these challenges. Because discussing all types of hybrid-style influence operations would take too much space, in this paper we selected several of the most notable cases of Russian hybrid activities in the Baltic States. Analysis of these cases will present their presumed goals and target audiences. Later, the actual response by the targeted states' governments will be discussed. Finally, some food for thought for possible countermeasures will be suggested.

The paper also aims to present a pilot overview of the cooperation of the three Baltic States as well as indicate the opportunities, need, and potential for the further development, harmonization or synchronization of the national security effort in the context of closer regional cooperation.

---

[62] G. F. Treverton, *et al*, *Addressing Hybrid Threats*, Swedish Defence University, (Stockholm: 2018), 4

Cases of Russian 'Hybrid' Influence Operations

CASE NO. 1. CYBERATTACKS AGAINST ESTONIA (MAY 2007) AND LITHUANIA (2014/2015)

The main goals of the cyberattacks Russia waged in the Baltic States in 2007 and 2014/2015 were to influence local decision-making processes and interfere with routine information flows as well as to cripple democratic values and beliefs and thus weaken Baltic societies. Furthermore, Moscow sought to collect important information. Finally, it tried to foster anxiety and distrust of society at the security level of the allied states. Political and social unrest benefits the attacker, which routinely attempts to pursue the strategy of "divide and rule." In these cases, several target audiences could be named: governmental institutions, media and society.

Actual Reaction by the Baltic States and NATO

- In response to Russia's cyberattacks on Estonia, NATO conducted an internal assessment of the Alliance's cybersecurity and infrastructure defenses. The assessment resulted in a report issued to the allied defense ministers in October 2007. It further developed into the creation of a cyber-defense policy and the creation of the NATO Center of Excellence for Cyber Defense in May 2008, which is now providing important expertise to the entire Transatlantic community.

- Due to the cyber-attacks, the non-binding, analytical Tallinn Manual on the International Law Applicable to Cyber Warfare was developed. This report outlined international laws considered applicable to the cyber realm. The manual includes a total of 95 "black-letter rules" addressing cyber conflicts. The Tallinn Manual has worked to provide a global

norm in cyber space by applying existing international law to cyber warfare. The manual suggests that states do not have sovereignty over the Internet, but over components of the Internet in their territory.[63]

- In response to the growing number of cyber-attacks, Lithuania created its National Cyber Security Center in 2015—a governmental organization that takes care of state information systems as well as security of their infrastructure and investigates cyber incidents. The service is subordinated to the Lithuanian Ministry of National Defense.

Except within the scope of EU or NATO formats—like the Permanent Structured Cooperation Cyber Rapid Response Teams (PESCO CRRT) project initiated by Lithuania in 2018—the counter measures implemented by the Baltic States were all at the national level.

Possible Reactions

- The lack of understanding of the significance of the threat is visible among the political elites. For example, one could assume dangers and chaos of a cyberattack on transport grid systems (traffic lights, etc.) during rush hour. However, due to the lack of understanding of such a threat, the issue of cybersecurity is a major concern in the political agenda of most states. Therefore, informing politicians and governmental officials is necessary and could be done by research institutions working on cybersecurity. Special emphasis should be put on sharing experience between countries.

- National cybersecurity strategies have become an essential

[63] Stephen Hezog, "Revisiting the Estonian Cyber Attacks: Digital threats and Multinational Responses". Journal of Strategic Security, 4 (2), (Tampa: 2011), 49–60.

backbone for preparedness to tackle cyber issues that may affect governmental institutions, important media channels as well as general societal security. Drafting this document is considered one of the key commitments to prepare and respond to attacks against domestic digital networks. According to the 2017Global Cybersecurity Index, Estonia is the highest-ranking country in Europe in terms of both its organizational structure to respond quickly to attacks as well as legislation requiring a minimal level of operation available without access to the Internet.[64] Lithuania only recently presented the Strategy, which, as of mid-2018, still needed to be approved by the parliament.

- Certain cyber-related issues could be considered matters of national security necessitating greater attention from the authorities. These could include the cyber-supply chain, evaluating supply-chain operations, practices and security, or usage of software produced in other countries (for instance Kaspersky Anti-virus software and its possible security gaps to authorities in NATO countries).

- Authorities should continue working on policies that encourage adoption of multi-factor authentication (MFA) solutions, preventing password-based attacks and ensure better protection of critical data and systems.[65]

- Governments should further encourage adoption of advanced technologies into the governmental sector as well as

[64]"Global Cybersecurity Index 2017", International Telecommunication Union, (Geneva: 2017). Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf p. 37.

[65]M. Chertoff, J. Grant, 8 Ways Governments Can Improve Their Cybersecurity. Accessed December 22, 2017, https://hbr.org/2017/04/8-ways-governments-can-improve-their-cybersecurity.

among the general population and businesses, such as Blockchain, etc. For instance, it can help to track sources of insecurity in supply chains related to Internet-of-things devices.[66] Public-private partnerships can become an important measure to ensure effective protection in cyber space. Authorities could work together with business to enhance the Blockchain ecosystem and improve security and privacy as a result.[67]

- Additional information campaigns are also needed for broader society, as irresponsible and precarious use of the Internet may lead not only to personal insecurity: infected devices can be used in general cyberattacks against public institutions. Informational campaigns on "cyber hygiene" are necessary for both younger and elder users of the Internet. An essential element to this approach would also be the monitoring of public social networks, where individual devices and users could experience cyberattacks after visiting forums and websites that frequently transmit hate and discriminatory messages openly and attract visitors through pirated content.

- A clear need exists to strengthen counter-cyber threat capabilities to make Internet-based networks less vulnerable. For this, experienced IT security experts should be engaged together with institutions and analytical centers to address the

[66]N. Kshetri, Can Blockchain Strengthen the Internet of Things? *IT Professional*, *19*(4), 72. Accessed December 22, 2017, https://doi.org/10.1109/MITP.2017.3051335.

[67] R. Materese, Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure. Accessed December 22, 2017, https://www.nist.gov/speech-testimony/strengthening-public-private-partnerships-reduce-cyber-risks-our-nations-critical.

issue in a proper way both in a political and technological fashion. In the case of Lithuania, there is already a relatively highly developed IT infrastructure and large numbers of global IT actors (CSC, for example)[68] working in the country. Part of the latter have experience in cybersecurity and infrastructure development efforts in Western countries, providing a valuable base for contextualizing this experience in Lithuania.

- A quick reacting cyber incident research and analysis group should be ready to immediately disclose perpetrators of such acts and then publicly identify them.

CASE NO. 2. BREACH OF BORDER, INTELLIGENCE OPERATIONS: KIDNAPPING AND SENTENCING OF ESTONIAN INTELLIGENCE OFFICER (SEPTEMBER 2014–AUGUST 2015)

This operation had two main goals: First, revenge and to intimidate the KAPO (Estonian intelligence service), which had successfully caught numerous Russian spies in Estonia in previous years. Second, the Estonian officer might have been kidnapped to be exchanged for Russian spies in Estonian custody. The main target audiences of this hybrid influence operation were the Estonian government, security structures, and the public, as well as NATO allies.

Actual Reactions by Estonia

- "The abduction of officer Eston Kohver from the territory of the Republic of Estonia by the Russian Federal Security

[68] CSC Wins $30 Million U.S. Air Force Cybersecurity Contract, *Business Wire,* January 18, 2011. Accessed on December 22, 2017, https://www.businesswire.com/news/home/20110118005423/en/CSC-Wins-30-Million-U.S.-Air-Force.

Service (FSB) on September 5, 2014, and his unlawful detainment in Russia thereafter constitute a blatant breach of international law," the Estonian foreign minister at the time, Marina Kaljurand, said in a statement.

- The case provoked condemnation from the international community and its main actors. The European Union's top foreign policy official, Federica Mogherini, said that Russia's actions were "a clear violation of international law." The United Kingdom's minister for Europe, David Lidington, said he was "deeply concerned" by the sentencing. "I have repeatedly raised my concerns about the handling of Mr. Kohver's case and called for his release during my meetings with the Russian ambassador to London," he said in a statement released by the Foreign Office. In Washington, US State Department spokesperson John Kirby denounced Russia's actions, saying they showed disregard for the rule of law.

- Since Kohver's capture, Estonia has ramped up defenses along its 290 km border with Russia, allocating more than €2 million for clearing and buying land and setting up a special border task force.

- Eston Kohver, sentenced in August 2015 to 15 years imprisonment in Russia, was exchanged for a former Estonian security official who, at that moment, was serving a 16-year sentence for spying for Kremlin. This swap was made possible at the highest political level prior to Putin's visit to the UN.

Possible Reactions That Could Be Taken

- Already in August 2015, there were discussions about fencing

along the border with the Russian Federation to enhance security and protect the Schengen zone, costing around €73 million. According to the Estonian Ministry of Interior, it would have permanent technical surveillance. The fence could also help to prevent such incidents as Officer Kovher's abduction and would stop Russian counterintelligence from executing similar operations violating the Estonian border.

- Before building the fence, surveillance (remote monitoring) along the border and particularly around key facilities should be enhanced and paired with the most advanced technologies available. The most vulnerable areas along the border could also be coupled with some type of rapid-response forces.

- Capabilities to ensure both intelligence and counter-intelligence efficiency is crucial in criminal intelligence, as well. Russia has often used local criminal networks and oligarchic connections to gain influence and stir unrest in Ukraine, for example.

CASE NO. 3. INTERRUPTIONS OF STRATEGIC INFRASTRUCTURE: INTERRUPTION OF NORDBALT SUBMARINE POWER CABLE WORKS (MARCH–APRIL 2015)

In March–April of 2015, the Russian navy, the Military-Maritime Fleet (*Voyenno-Morskoy Flot*—VMF) disrupted NordBalt power cable infrastructure being laid between Sweden and Lithuania. According to the Lithuanian Ministry of Foreign Affairs, a ship from the Russian Baltic Fleet entered the exclusive economic zone of Lithuania on April 30, during a regular military drill, and unlawfully ordered the Swedish-Swiss construction ship *Alcedo* to change course. Similar incidents took place on March 19, April 10 and April 24 as well. Such cables lie on the Baltic seabed unburied and unhidden; therefore, there is always a special ship present that informs other vessels not to encroach on the infrastructure to avoid harming the power cable with

fishing equipment or anchors. However, the ship was ordered to diverge from the cable route by Russian military ships.[69]

The dispute was swiftly resolved, but it nonetheless demonstrated how international waters can be manipulated by adversaries. The ultimate goal of the Russian side was to undermine the underwater powerline project, which is designed to increase the diversification of energy sources for Lithuania. The target audience for this operation was both the Lithuanian government and society.

Actual Reactions

Hours after the incident at the NordBalt cable construction site, the Russian ambassador to Lithuania was summoned to the Lithuanian foreign ministry. Lithuania expressed protest to the Russian ambassador concerning the Russian navy's violation of the United Nations Convention on the Law of the Sea (UNCLOS) as well as Lithuanian economic interests. According to Lithuanian Foreign Minister Linas Antanas Linkevičius, military ships in a maritime economic zone of another state have the right to sail, but this should not interfere with other ships' routes.[70]

- Rokas Masiulis, the lithuanian minister of energy, noted that the incident ultimately had no impact on the NordBalt project's progress, but he nevertheless stressed the seriousness

[69] Russia Accused of Disrupting New Energy Link between Sweden and Lithuania', *EU News & Policy Debates, across Languages*, 4 May 2015a accessed December 2, 2018, http://www.euractiv.com/sections/global-europe/russia-accused-disrupting-new-energy-link-between-sweden-and-lithuania-314279.

[70] Lithuania accuses Russia of disrupting work on Baltic power cable, *Financial Times,* May 2 2015, accessed December 22, 2017, https://www.ft.com/content/b63B33ea-f0b9-11e4-ace4-00144feab7de

of the incident.[71]

- Lithuanian Foreign Minister Linkevičius declared that safe shipping in the Baltic Sea is not only an interest of Lithuania, but also of the Western countries, so NATO, the EU and Lithuania's other allies should more strongly react to maritime violations by the Russian navy.[72]

Possible Reactions That Could Be Taken

- It is important to understand the meaning of Russian provocations and their goals and act decisively when encountering illegal Russian military activity in the Baltic Sea. First, this means that, in the future, Lithuania should consider deploying Lithuanian naval elements near the construction sites of important maritime infrastructure links. The Russian VMF may be more deterred from colliding with the navy of a NATO country than with civilian ships because it could result in more serious consequences for Russia.
- Another important step would be to persuade Western NATO allies about the seriousness of the maritime security situation in the Baltics and to promote their stronger reaction to repeated Russian violations. Countries like the United States and the United Kingdom could take additional measures to deter Russia from violating international law off the coasts of the Baltic States. Meanwhile, countries like Germany, whose economic interests are strongly related to Baltic Sea security and Russian markets, are likely to have greater leverage in negotiating with Russia for increased regional security.
- Last but not least, Lithuania's non-NATO partners, Sweden and Finland, play an important role in Baltic Sea security

[71] Ibid.

[72] Ibid.

structures. In a long-term perspective, it is vital for Baltic State and NATO interests that those two countries, which currently have more or neutral foreign policies, eventually shift their official discourse and rhetoric to a more explicit pro-Western geopolitical and military orientation that would include clear elements of a deterrence strategy against Russia.

Disinformation as the Major Challenge

The societies of the Baltic States are extensively exposed to the Kremlin's disinformation and subversion activities designed to create a favorable environment for Russian policies and politics. The three Baltic States reside on the frontiers of NATO and the EU, and they are the only former Soviet republics to have become full members of these Euro-Atlantic organizations. At the same time, however, these countries have large minorities of Russian-speaking people; and although public nostalgia for Soviet times has significantly decreased over the last two decades, a level of it persists. The Baltic States are viewed by the Kremlin as one area where it might be possible to subvert Transatlantic as well as EU unity. Any weakness of the Baltic States would serve the Kremlin's propaganda and disinformation campaign as proof at home and internationally that the EU and NATO are failing organizations.

The pro-Kremlin narratives are similar (e.g., "Lithuania, Latvia and Estonia are failing states"; "the Baltic States are puppets/proxies of the US"; "the Balts are Russophobic"), and pro-Kremlin media outlets make continuous efforts to reach vulnerable target groups in each Baltic State to take advantage of the weaknesses of their domestic economies, social issues, contested histories as well as weak inter-state cooperation.

CASE NO. 4. DISINFORMATION: SPREAD OF BROCHURES CONTAINING DISINFORMATION ABOUT THE LITHUANIAN ECONOMY

In December 2016, the inhabitants of several districts in Vilnius received information brochures written in the Russian language. These brochures called on people of Russian nationality to participate in a program supporting resettlement of ethnic Russians from Lithuania to Russia. The program is apparently open to persons who once held Soviet citizenships or know the Russian language. The brochures mentioned that the nearest Russian territory where resettlement could take place is Kaliningrad. The hand-outs also list addresses and web pages at which those willing to resettle could apply.[73] Finally, the leaflets incorrectly state that living costs (including the prices of apartments, gasoline, daily consumer goods and other expenses) in Kaliningrad are three times cheaper than in Lithuania, while the average salary is similar.

The main goal of this brochure seems to have been to spread disinformation about the socioeconomic conditions in Lithuania and Russia in order to influence part of Lithuanian society (mostly ethnic Russians) to be less loyal to the state and to strengthen their dissatisfaction with living standards of the country. The Russian-speaking minority was the main audience of this action. No clear counter-actions were taken except publicizing the incident in the media and warning that this biased provocation should not be taken seriously.

[73] Ugnius Antanavičius, "Russia lies to inhabitants of Vilnius that living costs in Kaliningrad are three times cheaper than in Lithuania", *15minLT*, accessed December 5, 2018, http://www.15min.lt/verslas/naujiena/finansai/rusija-vilnieciams-meluoja-kad-kaliningrade-zmones-gyvena-triskart-geriau-negu-lietuvoje-662-725702.

Possible Reactions That Should Be Taken

Russian-speaking minorities are continuously the target of Moscow's propaganda, which claims to defend their rights. Thus, more attention must be given to national minorities in the Baltic States:

- It is important to monitor the dynamic of Russia's propaganda on national minorities in the Baltic States, paying attention to content, scope and tools of propaganda, as well as identifying the level of harm for local societies;
- Additional efforts must be devoted to dialogue between the state and local ethnic communities, providing more opportunities for those ethnic community leaders to discuss their economic and cultural situation. This approach should facilitate legal proposals designed to ensure appropriate defense of their rights as well as provide more information in ethnic languages about the economic and social cultural trends in Baltic and neighboring countries;
- Local opinion leaders and experts must be widely included in the local public sphere (in ethnic languages as well) to fight against Russia's disinformation and propaganda, providing real facts for the aforementioned or similar situations.

CASE NO. 5. RUSSIA ESTABLISHING A STRONG PRESENCE IN LOCAL INFORMATION ENVIRONMENTS

Moscow's main goals in moving into local information spaces in the Baltic States is the formation of positive opinions on Russia, exacerbating dissatisfaction with local governments, shaping and mispresenting historical facts, as well as exploiting the vulnerabilities of the Balts' political systems, economy and society to its own advantage. The main target audiences are, therefore, the societies of the three Baltic States (and in particular, their Russian-speaking communities).

Actual Reactions Taken by Baltic States to Date

- Lithuania and Latvia introduced temporary bans on Russian media outlets that breached preexisting media laws.[74]
- In 2017, the Lithuanian parliament adopted a law restricting Russian media production content on Lithuanian TV. According to the new law, 90 percent of Lithuania TV content must be produced inside the EU and broadcast in one more of the official languages of the EU. Although this law restricts direct Russian influence on Lithuania media, it still permits various other pro-Russian media companies registered in EU countries to broadcast their content without limitations.
- In June 2018, the Lithuanian parliament adopted new amendments[75] to the Public Information Law, according to which TV channels in Lithuania must translate TV programs into Lithuania if these programs are produced in Russian or other non–EU languages and broadcast for longer than one hour and a half. The amendments are aimed at Russian TV productions.

Possible Reactions Baltic States Could Take

- Reactions to Russian measures in the information sphere are often problematic due to their potential political and legal repercussions as well as domestic statutory hurdles. Therefore countries should focus on prevention to decrease the effects of such potential measures.

---

[74] "Russia questions on Latvia´s ban on Rossiya RTR channel", *The Baltic Times*, 8 April 2016, accessed 15 October 2016, http://www.baltictimes.com/russia_questions_latvia_s_ban_on_rossiya_rtr_channel/.

[75] "Amendments to the Public Information Law," Parliament of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a205c6237b8e11e89188e16a6495e98c.

- It is vitally important to restrict the financing of pro-Russian "fake news" media outlets and to establish legal norms among local media representatives that discourage journalists from working for Russian media channels. Restricting the functioning of potentially dangerous Russian media sources is a realistic option if all measures taken are fully in accord with the legal regulations of the state.
- Another important measure is raising public awareness about the threats and overall functioning of information warfare. One of the common solutions is to establish Russian-language channels that can reach the local Russian-speaking population, thus providing an alternative to the broadcasts coming from Moscow. One of the best examples is Estonia's *ETV+* project.[76] Additionally, trainings need to be organized both for owners and staff of the key media outlets in the given country; through these people, it is possible to significantly decrease the effects of Russia's information influence. Much can be learned from the experience of the Baltic countries, particularly regarding the online domain, where voluntary groups, so-called "elves," were set up to virtually fight against Russian coordinated trolling.[77]
- The best tool to defend against hybrid warfare is good governance, speaking in the broadest sense. To sustain democratic political structures and well-functioning public administrations, it is necessary to respect the values of transparency, media freedom, human rights, the rule of law, and to guarantee proper rights to ethnic, national, religious and other minorities. All these need to be in place to improve domestic democratic legitimacy and support the government,

[76] Homepage, ETV Plus, accessed 2 December, 2016, http://etvpluss.err.ee/.

[77] Michael Weiss, "The Baltic Elves Taking on Pro-Russian trolls," *The Daily Beast*, 21 March 2016, accessed 15 October 2016, http://www.thedailybeast.com/articles/2016/03/20/the-baltic-elves-taking-on-pro-russian-trolls.html.

which is the basis for the stability of the state. Special focus requires measures to fight against corruption at all state and societal levels, paying special attention to the members of the political elite, state administration and, of course, personnel and leadership of the armed forces.

Examples of Smart Defense: Environmental Monitoring in Space and Time as Well as Inter-Institutional Crisis Management

Lithuania daily monitors the national information space in time and space. The authorities collect and follow available indicators and symptoms while establishing potential correlations. It is a complex, comprehensive, multifaceted exercise carried out by several governmental institutions. The main task of this activity (function) is to access indications of hostile activities, and to act proactively.

The following three examples demonstrate that such an approach proves that the Baltics are not defenseless against the Kremlin's asymmetrical disinformation campaigns, as sometimes may appear.

RUSSIAN DISINFORMATION ON GERMAN 'RAPE' OF LITHUANIAN GIRL

In February 2017, Lithuania became the target of an information operation and cyberattack from an unknown source. Weeks after the Seimas (parliament) ratified the Defense Cooperation Agreement[78] with the United States, the speaker of the Seimas received an e-mail stating that a girl from an orphanage "was surrounded and raped by a crowd of drunken German-speaking uniformed German soldiers" on her way home from school. The letter claimed the alleged incident occurred in the region where NATO's Enhanced Forward Presence battalion, led by Germany, had been deployed.

[78] The US-Lithuanian Defense Cooperation Agreement details the status of US troops, their dependents and contractors based in Lithuania.

This story resembles the infamous "Lisa case" of January 2016, in which Muslim immigrants in Germany were falsely reported to have sexually assaulted a Russian girl. That story first appeared on an obscure German website but was immediately spun by Russian media outlets like Perviy Kanal, a state-run TV channel. By spreading that fake story, the Kremlin likely sought to inflame German public opinion about the threats posed by immigrants and create a backlash to Chancellor Angela Merkel's permissive immigration policies.

Actual Reactions by the Lithuanian Authorities

- The Prosecutor's Office established that the story was fake, that the letter was signed under a false name, and that it was sent from an undisclosed server located in a non-EU member state.
- The timing of the letter and its content suggests it was released by Russia, with the aim of discrediting Lithuania and its NATO allies, encouraging public disapproval of government decisions and sowing distrust among Lithuanians about the deployment of NATO soldiers to Lithuania.
- The national institutions acted in a coordinated way: the Parliament Speaker's office immediately informed the national security agencies; in parallel to the investigation process, the media and the public were regularly informed about the fake information (the case that never happened). The German government also was informed.

HACKING OF TV3.LT

On January 18, 2018, a cyberattack targeted *TV3.lt*, the website of a major Lithuanian TV channel: the hackers inserted false information about Defense Minister Raimundas Karoblis. According to the planted story, Karoblis admitted to being gay and was accused of sexual harassment by a well-known radio journalist and some diplomats. In contrast to previous cyberattacks on the country, this

story was written in grammatical Lithuanian. The cyberattack took place two days after Lithuania released the Magnitsky List, which names 49 Russian citizens banned from entering Lithuania for violating human rights.

The fake story was notably disseminated via an e-mail containing an attachment with a virus. Any official addressee who opened it—there were only a few who did—would have had their computers infected. So the aim could have been to gain access to a decision-maker's computer and phone data. The hackers played on the natural inquisitiveness of human nature: inventing an absurd story makes the attachment more tempting to open.

The cyberattack could have been meant to test the resilience of Lithuanian information systems, the speed and scope of their reaction, and how quickly the false message might spread and be received. News websites are attractive targets for cyberattacks because they are themselves information disseminators. Moreover, such sites are a key source of information for citizens in case of emergency—a serious potential threat if these news websites suddenly start to carry lies, false information or disinformation.

Some analysts claimed the *TV3.lt* attack may have been an extension of Russia's Zapad 2017 military exercises, held the previous September. Indeed, the Kremlin repeatedly shows that cyberattacks are integrated into its conventional offensive strategy. And during these last Zapad drills, Russian radio-electronic combat forces disabled much of Latvia's mobile network and as well as GPS signals in Norwegian airspace.

Actual Reactions by the Lithuanian Authorities

- It is obvious that this false story was meant to be spotted immediately. *TV3.lt* removed the fake article within five minutes; but e-mails from the website's account with the

false story attached were sent to a number of prominent Lithuanians—politicians, ministers, foreign diplomatic missions, and other news sites.
- The initial IP address led to St. Petersburg, Russia; and the National Cyber Security Center of Lithuania started an investigation.
- Lithuanian government institutions prevented the cyberattack: the attachment was made public, and government institutions cooperated with media to explain the case to the public in detail.

Lithuania's information environment is constantly exposed to Russian cyberattacks, big and small. According to Russian military doctrine, information confrontation is an essential aspect of military operations.

FALSE STORY ABOUT VIOLENCE AGAINST RUSSIAN CONSCRIPTS IN ESTONIAN ARMED FORCES

The Estonian Defense Forces (EDF) prevented a *Sputnik* disinformation attack in March 2018 by informing Estonian media about a possibly false story before it was written.

On March 13, Estonian media reported on an incident within the EDF: a conscript had shot himself in the shoulder to, in his words, "get a cool scar." According to the investigation, as reported by the media, the conscript—who had served as a driver at the Kuperjanov Infantry Battalion (a unit of the Estonian Land Forces)—stole a cartridge for his AK4 rifle and, when no one was near, pulled the trigger. According to the medical report, the conscript lost a lot of blood, but no critical organs were injured and he was recovering under medical supervision. Military police discovered no evidence that the shooting was caused by anything other than what the soldier claimed: the conscript was well trained, his relationships with his comrades were good, and he had earlier told his friends that he wanted a bullet scar.

And yet, two days later, the local Estonian branch of the Kremlin-financed media channel *Sputnik News* geared up to publish a disinformation story that would have suggested the Estonian draftee was a Russian speaker and had been shot by his ethnic-Estonian comrades as he tried to escape their abuse. Moreover, the story would have claimed that, as a non-Estonian speaker, he was being denied medical treatment by the authorities.

Actual Reactions by the Estonian Authorities

- On March 15, Estonian *Sputnik* sent an inquiry to the EDF asking it to confirm the channel's supposed information that the conscript was a Russian speaker, that he was shot during an escape attempt sparked by tensions on base between Estonians and Russians, and that military doctors deny medical care to conscripts who do not speak Estonian. Instead of answering *Sputnik* directly, the EDF sent the channel's inquiry to the Estonian media to publicize *Sputnik's* attempt to inflame conflict between ethnic Estonians and Russians and to neutralize any disinformation that *Sputnik* might try to spread. The neutralization was successful: *Sputnik* never wrote the story. The Kremlin-financed channel did answer with an article claiming that by giving out *Sputnik's* questions to journalists, the Estonian Defense Forces were themselves spreading disinformation. In Russia, *Sputnik's* article on how the EDF went on the counterattack by giving *Sputnik's* questions to Estonian media reached *RIA Novosti*, the state-operated domestic Russian-language news agency. But because of the EDF's proactive release of *Sputnik's* inquiry, Estonians were already informed about the facts, and the article did not cause any significant public reaction.
- If disinformation is like a virus, it should be treated as such, warranting diagnosis, cure, education and the development of

a vaccine. In the three Baltic States, CEPA's 4D approach—detect, debunk, defend, and disarm[79]—has proven successful. Local monitors, local voluntary activists, and local media have successfully used three of the four: detecting disinformation by diagnosing it, curing by debunking it, and defending people by educating them. By neutralizing *Sputnik's* disinformation, the Estonian Defense Forces tried the fourth defense, disarming the disinformation. It worked—at least with regard to Estonian society.

Institutional Structures for Common Actions Against Disinformation

Mechanisms for fostering the Baltic States' regional cooperation were established in the 1990s: at the inter-parliamentary level with the Baltic Assembly, and at the inter-governmental level with the Baltic Council of Ministers. They function successfully and provide a framework (agenda) for more tangible Baltic cooperation.

In addition, Baltic cooperation takes place within other regional and international structures, including the Nordic-Baltic Eight (NB8), Baltic-Polish relations, the Three Seas Initiative framework and, of course, with NATO and the EU.

The Baltic States' latest institutional engagement in dealing with targeted Russian information operations against their societies took place at a joint conference of the Baltic Assembly and the Baltic Council of Ministers on May 2016. Notably, the Baltic States adopted a resolution addressing the current issue of strategic communications,[80] stating their full support to the NATO Strategic

[79] Lucas and Pomeranzev, "Winning the Information War," 2016.

[80] "Joint Statement of the 22nd Baltic Council," Ministry of Foreign Affairs of the Republic of Lithuania, https://urm.lt/uploads/default/documents/uzienio_politika/Baltijos_taryba/bendras-pareiskimas20161028.pdf.

Communications Center of Excellence in Riga and the EU East Strategic Communications Team in Brussels. The Baltic States also confirmed their readiness to undertake joint activities promoting quality media in Baltics as well as cooperation in media literacy development and support for the Baltic Center for Media Excellence in Riga.

During its annual sessions, the Baltic Assembly regularly mentions the issue of strategic communications, disinformation and societal resilience. The Baltic Assembly resolutions of 2014[81] and 2017[82] pointed to the importance of Baltic cooperation in strategic communications activities; in 2018, the Baltic Assembly Security and Defense Committee named strategic communications among its priority activities.[83] These resolutions are of a declarative character and, so far, have never instructed or empowered their national government to take concreate measures regarding joint activities. On the other hand, the Baltic States can sincerely boast of extensive experience in confronting (impeding) hostile soft power activities at their national level.

The topic of Information Warfare is approached by the Baltic States within the Nordic-Baltic cooperation format. On May 6, 2015, the

[81]Baltic Assembly resolution of 2014, Baltic Assembly resolution of 2017, https://docs.google.com/document/d/1BY-4fJMLKPBS8jAyIlh4EbejP_0Tq5vPlEHyOVAvcts/edit?ts=5b5870c1.

[82] "Centre participates in the conference of Baltic Assembly and Baltic Council of Ministers", NATO Stratcom COE, accessed on December 3, 2018, https://stratcomcoe.org/centre-participates-conference-baltic-assembly-and-baltic-council-ministers.

[83] "Legal Affairs and Security Committee", Baltic Assembly, accessed on December 3, 2018, http://www.baltasam.org/en/structure/comitees/24-structure/committees-of-the-baltic-assembly/1292-legal-affairs-and-security-committee.

Nordic and Baltic (NB8) ministers of foreign affairs discussed the Russian media's ongoing broad campaign of biased coverage, including regarding the crisis in Ukraine. The NB8 meeting aimed at identifying common approaches.[84] The initiative was followed by several meeting. Finally, in 2017, the Nordic Council finalized its program to support media content and strengthen minority-language media production in the Baltic States; the program included concrete technical aid to media producers, media information sharing, training of young journalists, direct financial aid to *ETV+* (Estonian TV in Russian) and to several Latvian radio stations in Russian, and grants for journalists.[85]

In July 2018, the Baltic States established the Baltic Cultural Fund[86] to finance cultural cooperation programs in Lithuania, Latvia and Estonia, as well as organized common international cultural events. The Fund will sponsor professional projects in the areas of architecture, visual arts, design, literature, music, theater, libraries, museums and archives. The Fund should be viewed as a practical measure in building up the identity of the region and strengthening societal resilience to subversion.

---

[84] "NB8 foreign ministers' statement on strategic communication", Nordic Council of Ministers, accessed on December 3, 2018, https://www.norden.lv/en/news/06.05.2015.nb8-foreign-ministers-statement-on-strategic-communication/.

[85] "Support for increased quality of media content […]", Nordic Council of Ministers, accessed on December 3, 2018, https://www.norden.lv/en/mobility-programmes/support-for-increased-quality-of-media-content-and-strengthening-of-minority-language-media-production-in-estonia-latvia-and-lithuania.

[86] "Lithuania, Latvia and Estonia are establishing joint cultural fund of the Baltic States", Ministry of Culture of the Republic of Lithuania, accessed on December 2, 2018, https://lrkm.lrv.lt/en/news/lithuania-latvia-and-estonia-are-establishing-joint-cultural-fund-of-the-baltic-states.

To sum up, there is a clear understanding among the Baltics' parliamentary and governmental institutions about the need for more concrete cooperation or coordination of activities in the strategic communication field, as well as when it comes to information and experience sharing. With the active participation of third parties, such as the Nordic Council, such cooperation can more easily be converted into concrete measures and activities.

2.4. Disaster Risk Reduction and Urban Resilience

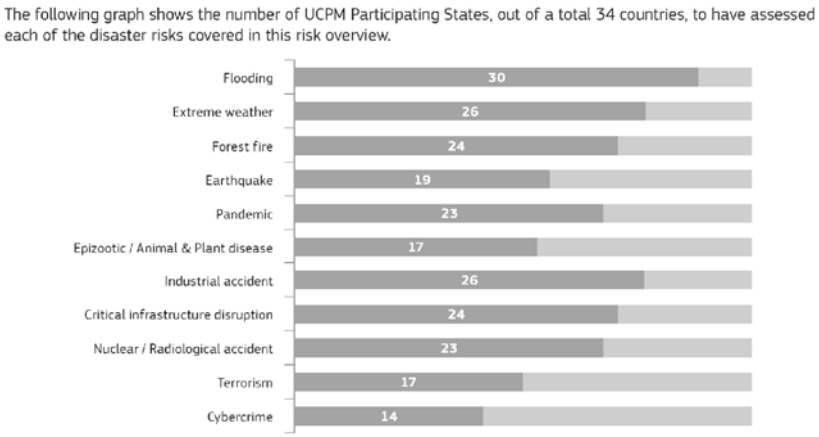
Edmunds Āķītis

Introduction

Risk Assessment is becoming more and more important in EU policymaking (civil protection, cohesion funding, solidarity clause). This is closely related to the United Nations' Sendai Framework for Disaster Risk Reduction.[87] Risk assessments help to inform decision-makers on how to prioritize and allocate investments in prevention, preparedness and reconstruction measures. Within Europe, 34 countries (28 EU member states and 6 other countries) have established the EU Civil Protection Mechanism.[88]

[87] "Sendai framework," United Nations Office for Disaster Risk Reduction, accessed on December 3, 2018, https://www.unisdr.org/we/coordinate/sendai-framework.

[88] "Civil Protection", European Commission, accessed on December 3, 2018, http://ec.europa.eu/echo/what/civil-protection/mechanism_en.



Graph 1: Number of UCPM Participating States having assessed each risk covered by the Overview of Risks

A regional approach to strengthen and address disaster risk and man-made risk management is one way ahead. At the policy level, the Council of the Baltic Sea States[89] is an overall political forum for regional cooperation. Since 2002, the Civil Protection Network (CPN) convenes annually at the level of Directors General to exchange views on ongoing activities and to coordinate joint measures in the field of civil protection, critical infrastructure protection and other emergency preparedness issues in the Baltic Sea Region.

Next in line are the capability assessments vital for identifying the resources and capacities needed to prevent and respond to a crisis. EU member state authorities are proceeding with these activities and commitments; however, there is a substantial lack of common understanding of Disaster Risk Reduction by the general publics in Europe. Arguably, the situation is even worse when it comes to urban resilience—"a new kid in town"—as well as urbanization processes, migration and other factors not presently recognized as potential hazards or risks.

[89] Council of the Baltic Sea States, http://www.cbss.org/.

The three Baltic States have been addressing this issue of capability assessments in a differentiated manner. Estonia does not have a common approach at all. Capability assessment is partially covered by the vital services (vital societal functions) risk assessment, partially by the emergency risk assessment, and in part by a summary of Estonian national emergency risk assessments (risk-reducing measures). Each of the above-mentioned risk analyses are made according to the Emergency Act and are linked to the national risk assessment.

Latvia has neither a common approach for capability assessment nor a so-called methodology. Instead, the National Security Law prescribes that institutions, basically all ministries and institutions, be responsible for forecasting, in a timely manner, as well as preventing internal and external threats to the state. The newly adopted Civil Protection and Disaster Management Law prescribes clear disaster management coordination tasks to ministries and local municipalities, according to their respective competencies, compelling them to organize and carry out disaster risk assessment; and based on the outcome of risk assessment, these government bodies must plan measures for all of the disaster management cycle.

Lithuania does not have an approach for capability assessment; however, all ministries, public authorities, institutions, municipalities, and some essential entities have to group and analyze their managed resources (or plan to invoke additional resources) while compiling and updating their emergency management plans. A methodology for emergency management plans has been compiled for ministries, public authorities, institutions, municipalities and other government entities.[90]

Common terminology and an understanding of (disaster) risk

[90] Report on National Capability and Risk Assessments and related challenges in the Baltic Sea Region.

management related issues in the three Baltic States seems to be quite apart. It is worth exploring what kind of risk assessments are in place, what capabilities exist to address them, and how and to whom they are communicated in relation to children, young people, disabled people and the elderly. This is closely related to city resilience or urban resilience. Furthermore, it remains unclear in the Baltic States how natural and man-made risks affect these vulnerabilities, what are the cascading effects and cross border impacts, as well as how societies deal with the vulnerabilities before, during and after the disaster.

The need to reinforce the regional dimension of risks and subsequent risk management capabilities is expected to become increasingly relevant within the European Union Civil Protection Mechanism framework.

Disasters can happen irrespective of national borders. At the regional level, natural and man-made events can take the form of:

- Small-scale events that affect border regions—regional entities within and across countries may be vulnerable to certain risks and face a combination of obstacles, vulnerabilities to their natural border environments; and various legal/administrative issues.
- Large-scale events with impacts across different countries, which may overwhelm capacities at the national level.

Initiatives addressing disaster risk management on a supra-national scale exist, but these remain limited to a number of EU macro-regional strategies (Danube, Baltic Sea, Alpine, Adriatic-Ionian) or hazard-specific cooperative initiatives (e.g. Nordic Forum for Risk Analysis). Moreover, existing regional initiatives on risk management are not reflected in the risk assessment, risk management planning, or response planning processes undertaken at the national level.

The recent communication from the European Commission,

"Strengthening EU Disaster Management: rescEU—Solidarity With Responsibility" (COM[2017] 773 final) calls on "Member States and [the] Commission to promote more systematic collection and dissemination of loss data, to enhance the collection of loss data and make use of loss data for optimized prevention and climate adaptation planning." This is, thus, another option for addressing the regional dimension—that is, through analyzing loss data to understand the preparedness issues and capability shortcomings.

Further integration of disaster risk response in EU policies could involve: environmental impact assessments, nuclear safety, water management, cross-border health, green infrastructure, agriculture, forestry, construction, industry, security, critical infrastructure as well as off-shore safety. But attention and respective preparations should be done at all levels, including national, city, local, etc.

The Commission and the High Representative of the Union for Foreign Affairs and Security Policy Federica Mogherini (who is dual-hatted as the Commission's Vice President) adopted in April 2016 a Joint Framework on Countering Hybrid Threats.[91] The Joint Framework proposes 22 operational actions aimed at raising awareness, building resilience, better responding to crises and stepping up cooperation between the EU and NATO. However, if not properly addressed in a timely manner, the response will be costly and might entail not only the damaged reputation or disruption of vital services, but also fatalities.

Political decisions are translated into actions and one concrete action stemming from DG ECHO is the risk assessment report compiled based on member state risk assessments.[92] The excerpt from the EU

[91] Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats: a European Union response, JOIN(2016) 18 final, 6.4.2016.

[92] Overview of natural and man-made disaster risks the European Union may face.

member risk assessments related to cyberattacks, suggests that there is no cross-border risk with no cascading risks. And yet, Lithuania is the only Baltic State that actively considers international cooperation in this case. This is one example of the level of existing—or rather non-existing—international cooperation. A crucial part of risk management is risk awareness—how and how well are societies informed as well as how sufficiently prepared are they to address these risks and withstand the shocks.

The traditional approach to protect citizens is through the prism of a civil protection system. Additional research should be performed at the local, regional, national and inter-regional (cross-border) level with a focus on social resilience, city resilience, refugee influx, risk awareness, and disaster loss. That all would lead to new potential cooperative initiatives related to urban resilience. The term itself—"urban resilience"—is not particularly well known or accepted yet in the Baltics. Again, the civil protection prism prevails if something happens.

Improving resilience means strengthening the capacity of both local and national actors to identify and deal with risks, vulnerabilities and their underlying causes. But resilience is inclusive and requires participatory societies. Strong evidence shows the link between inclusive and participatory societies, with accountable, transparent and democratic institutions.

Conversely, shortcomings in governance, democracy, human rights, the rule of law, gender equality and corruption or shrinking space for public participation and civil society, pose a fundamental challenge to the effectiveness of any society's development efforts. The quality of governance and public administration determines the performance of a country in all public policy domains, shaping economic prosperity, social and territorial cohesion, as well as sustainable growth.

In conclusion, resilient societies are underpinned by sustainable and

balanced socioeconomic development that anticipates and addresses socioeconomic inequalities, vulnerabilities, and their root causes. This understanding is at the heart of the EU's approach to state and societal resilience.

2.5. Expert Recommendations

1. Create incentives for editors and journalists in the Baltic States' media outlets to present at least basic information about political news, societal trends and cultural events in the other two Baltic states: e.g., build a network of Baltic media representatives that they could refer to (and trust) whenever fact-checking is needed;
2. Urge editors and journalists to contact and communicate with not just local experts or experts from the US, Germany, France and Poland, but also other Baltic states—to grasp the atmosphere in neighboring countries with regards to the most pressing issues of the day;
3. Begin a series of conferences (each year in another country) to tackle the most pressing issues in the field of the Baltic States' societal resilience and security; one of the binding themes should be the vulnerability of Russian-speaking minorities in the respective countries along with the best ways to strengthen these communities and the mistakes made in reaching out to them (by presenting them as inherent "*vatniks*," etc.);
4. Encourage Lithuania's, Latvia's and Estonia's (B3) Public Broadcasters to create TV shows or films about common B3 history or the current geopolitical situation;
5. Promote student exchanges among all three Baltic countries;
6. Invite think tanks in all three Baltic countries to think of joint initiatives and projects for tackling disinformation, propaganda and hybrid threats;
7. Integrate Media and Information Literacy methodology, e.g. classes/curriculum that have been developed in Estonian, Latvian, Lithuanian on their history, culture or art into the educational programs of each Baltic State;

8. Form a "fact platform" providing reliable/factual and updated information on each Baltic State, and which is available for people (e.g. media people, students, etc.) looking for such information;
9. Promote knowledge of societal resilience in local communities and to ethnic minorities in an intra-regional context.
10. Develop common media channels of information for bolstering intra-regional cooperation and resilient media sectors;
11. Prioritize civil protection and related measures to establish city resilience among both government and non-governmental interlocutors;
12. Institutionally share best practices and lessons learned in order to support each of the recommendations mentioned;
13. Establish a financial instrument to help the region carry out far-reaching and long-term societal resilience measures as well as the effective narratives accompanying them.

3. ECONOMIC SECURITY

3.1. Expert Assessment

Olevs Nikers, Otto Tabuns, Giedrius Česnakas, Arunas Molis, Jako Reinaste, Gunārs Valdmanis, Romas Švedas

Cooperation among the three Baltic States—Estonia, Latvia and Lithuania (B3)—in the energy sector may be considered positive, even though reaching this point has not been easy. And from a wider European Union or Central Eastern Europe perspective, the outcome of this cooperation may even merit being called exceptional. *Inter alia*, the B3 countries have:

- Developed and signed the EU Baltic Energy Market Interconnection Plan (BEMIP) and have regularly monitored its implementation;
- Completed or continue to develop power and natural gas interconnections with the support of EU financial grants;
- Established (liberalized and integrated) electricity and gas markets;
- Eliminated (especially in Lithuania) Gazprom's vertically integrated monopoly and energy dependencies on Russia.

That said, a number of energy security challenges persist, the first being the synchronization of the Baltic States' power systems with that of Continental Europe—an issue that is further hampered by risks connected to security challenges stemming from Russia's Baltic exclave of Kaliningrad. A further challenge stems from ensuring fair competition in the gas sector: artificially low prices from one supplier could threaten to eliminate Norwegian, US or other gas suppliers or

economically harm local liquefied natural gas (LNG) terminals and undermine the development of further LNG projects, infrastructure etc. In addition, there is the contentious issue of electricity imports from the Astravets nuclear power plant (NPP), in Belarus, which the Lithuanian government has claimed is being developed in violation of international practice and standards. Finally, there are the issues of improving public consultation methods, in particular regarding new energy projects and the education of society on energy-related topics: energy saving and efficiency, the benefits of renewable energy, the "prosumer" movement, etc. Good interinstitutional Baltic cooperation is of crucial importance in order to manage risks and to prevent the most popular Russian tactics of "divide and rule."

Baltic intra-regional cooperation in energy security is, first of all, limited by the lack of understanding of regionalism among the B3 states, which usually assess their energy security and energy projects individually. This creates duplication and expansion of excessive energy infrastructure in neighboring states, preventing the most efficient or rational use of financial resources and thus increasing expenses related to the maintenance of this infrastructure.

Regional cooperation is also limited by the domination of the self-help principle and the lack of trust among the states. Because of that, the Baltic States experienced problems when a regional LNG terminal concept was being developed. Lithuania and Estonia were suspicious that an LNG terminal in Latvia might become an instrument of Gazprom, which controlled Latvias Gaze and a regional underground storage facility. Thus, infrastructure that could have serviced the whole B3 region was not accepted by the neighboring countries. Instead, in 2014, Lithuania implemented an LNG terminal project at Klaipėda (a floating LNG regasification unit) on its own, with the political and financial support of the European Commission. The capacity of this LNG terminal nearly satisfies the total annual natural gas needs of the B3 and could theoretically serve as a regional LNG terminal. However, Latvia and Estonia failed to accept Klaipėda as a

regional project and have continued to pursue competing individual LNG terminal projects. Estonia and Finland plan to develop Balticconnector, a bi-directional natural gas pipeline. A single LNG terminal would be able to service both countries; however, they each also have plans for individual LNG terminals.

The dominance of small gains and short-term interests has frequently hampered international cooperation. The same is true for cooperation in the B3 energy sector. Despite their agreement on the strategic importance of particular energy security projects, they have regularly sought to increase their bargaining power or pursued funding for other projects. The last country to agree on a particular multilateral project frequently has the greatest opportunities to receive more benefits. Therefore, such international projects, despite their strategic significance, become hostages to small-gain policies, which prolongs their implementation and extends the period of energy insecurity for all the actors involved. Such a situation was perfectly exemplified by the NordBalt submarine power cable project, developed between Sweden and the Baltic States. The project was initiated in the early 2000s by Lithuania and Sweden; but in order to receive EU funding, it had to become regionalized, with the participation of Estonia and Latvia. Each of the participating B3 countries assumed that the NordBalt cable should terminate in its territory. Negotiations on the project prolonged and were successfully dealt with only when the EU increased the financial package and Latvia could finance the construction of additional electricity lines to the termination point in Lithuania.

Overcoming problems in regional cooperation is frequently a great challenge; it takes time and intensive negotiations. Closer economic and political cooperation is time-consuming and difficult to implement with larger energy security projects. The NordBalt example illustrates the importance of the involvement of strong international actors that have the power and resources to exert influence and thus compel closer cooperation.

As such an influential international actor, the European Union has had at least three types of positive impact on the energy security of the Baltic States.

First, the EU improved the negotiation position for all of its smallest member states but also forced them to move toward the market principle based in the energy sector by compelling changes to their regulations. Thus, the EU Third Energy Package allowed the Baltic States to decrease the role of Gazprom in their domestic energy markets, which would hardly have been possible otherwise.

Second, political and financial support from Brussels facilitated the implementation of various strategic regional projects. Notably, the above-mentioned Baltic Energy Market Interconnection Plan, introduced in 2009, allowed the B3 countries to receive financial support for the development of interconnections inside the region (reinforce gas and electricity connections) and infrastructure links outside it (LitPol Link electricity interconnection; NordBalt electricity interconnection; Estlink 1 and 2 electricity interconnections).

Third, the European Union also played a significant role as a mediator between the B3 states when they failed to reach an agreement, as in the NordBalt case. At the same time, the EU can press the countries to move forward on projects that create connections they have failed to implement themselves at the regional level.

Most of the outlined issues continue to be valid today. For example, the Baltic States have had trouble agreeing on electricity interconnection and synchronization with Continental Europe—either with Poland or Finland. Lithuania and Estonia have notably been advocating different approaches: Vilnius has called for synchronizing the B3 electricity grid via a connection with Poland, Tallinn continues to insist on a second power line between Lithuania and Poland. Similarly, the LNG terminal in Klaipėda could become a

regional project that saves money on investments in the regional natural gas sector; but Estonia plans to construct its own LNG terminal as well.

Coordination of the external energy policies of the B3 countries remains limited, as the case of the Astravets NPP exemplifies. Latvia has, to date, not clearly stated its position on the possible import of electricity from this Belarusian nuclear plant, despite Lithuania's unyielding assertion that the facility threatens its core national security interests.[93]

As repeatedly alluded to above, perhaps the most important unresolved strategic energy issue for the Baltic States is the current status of their Soviet-legacy electricity grid. Despite membership in the EU since 2004, the region's electricity system still operates synchronously with the Integrated Power System/Unified Power System (IPS/UPS) coordinated by the Electric Power Council of the Commonwealth of Independent States, headquartered in Moscow. In other words, the three Baltic States may buy and sell electricity in the Nordic countries or Poland, but the daily management of their electricity systems is dependent on Moscow's centralized control over the frequency. Furthermore, provisions in the BRELL Agreement[94] oblige the Baltic transmission system operators (TSO) to coordinate the development of national electricity networks they are responsible for with Belarusian and Russian authorities. Dramatically worsening

[93] Giedrius Česnakas, The 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 South Caucasus, IOS Press, 2017. pp. 1–7. doi: 10.3233/978-1-61499-777-1-1.

[94] In 2001, Belarus, Russia, Estonia, Latvia and Lithuania (BRELL) signed the Agreement on the Parallel Operation of the Power Systems. The signatories established a so-called BRELL loop, synchronizing their high-voltage power-transmission networks under a single system.

relations with Russia increase the Baltic States' worries that such dependency may result in contrived supply disruptions.
The Baltic States have attempted to overcome this Soviet legacy in the electricity sector as early as 2007, when the B3 prime ministers declared de-synchronizing from the IPS/UPS and synchronizing with the European Continental Network (ECN) a strategic priority. They have made some progress in this regard. In particular, the Baltics have worked on surmounting their infrastructural isolation from the rest of the EU and succeeded in pushing the European Commission as well as most countries in the Baltic Sea Region (including Germany, Sweden, Finland and Poland) to openly acknowledge that electrical grid synchronization contributes to a functional internal EU energy market. The generic aim of synchronization was included in the list of EU Projects of Common Interest (PCI) and recognized as a feasible project from both a technical and a legal point of view. However, since then, Moscow has successfully prevented de-synchronization of the Baltic States' electricity systems.

In the natural gas sector, the historical development of the Baltic countries was rather like that of the power sector—the gas system in Baltic countries was developed as part of the interconnected and coordinated natural gas network of the Soviet Union. However, due to both physical and economic aspects, cooperation between the gas system operators in the B3 countries was less intensive than in the power sector. Latvia, with its natural gas underground storage, has historically acted as the sole source of supply for Estonia during heating seasons and as an emergency supplier for Lithuania; but such operation was mostly coordinated by the foreign supplier of this natural gas, Gazprom. With the continued decrease in natural gas consumption in the Baltic countries and the liberalization of the markets and change of ownership of gas system operators, the overall intensity of energy security cooperation has, in fact, decreased. Nevertheless, there is potential for further increase in technical cooperation thanks to the growing regional natural gas trade.

Currently, the main mechanism for providing operational security of energy infrastructure is the coordination between the transmission system operators. And the existing exchange of information between B3 TSOs allows them to quickly identify and mitigate or prevent most operational security disturbances and challenges as they occur. In contrast, however, the exchange of information between operators and power suppliers is sometimes slow regarding operational decisions—with a resulting longer-term potential effect on security.

One example of the above problem is the exchange of information regarding available power production capacities. At present, the exchange domain for such information in the electricity sector is the Nord Pool Spot power exchange, which does not always provide the necessary data to evaluate the overall security implications of any particular decision. In some cases, the choice by one of the Baltic countries to discontinue the operation of significant (approximately 1,000 megawatts) but aging power-production capacities was communicated to neighbor countries via the Nord Pool Spot information exchange platform only several weeks before the implementation of the decision—and without prior consultations or regional security studies.

On June 17, 2009, eight Baltic countries (Finland, Sweden, Estonia, Latvia, Lithuania, Poland, Germany, Denmark) and the European Commission signed a Memorandum of Understanding on BEMIP (Baltic Energy Market Interconnection Plan), including an action plan on improving cross-border interconnections and functioning of the market. The BEMIP cooperation framework targets the development of a functional and integrated internal energy market and elimination of "energy islands," combined with the development of necessary electricity and gas infrastructure and interconnections in the Baltic Sea region. In BEMIP's first phase, the focus was on developing a single harmonized electricity market in the Baltic Sea Region by establishing interconnections between Baltic and Nordic countries and then connections to the Central European electricity

market. In a longer-term perspective, energy security in the electricity sector can be increased by connecting the Baltic countries to the EU's synchronous grid.

Development of a regional gas market has also become increasingly important in the BEMIP framework, with an agreement reached in 2013 on an action plan for building gas infrastructure and diversifying gas supply in the Eastern Baltic region. A discussion on updating BEMIP was initiated in the autumn of 2014; after that, energy security came into sharper focus in connection with ensuring the security of gas supplies and establishing a regional gas market.

Also in 2014, the Baltic Council of Ministers' (BCM) Committee of Senior Officials on Energy was established to ensure better communication among the B3 at the senior level. This body's main topics of discussion are the same as under BEMIP (synchronization, electricity trade between third countries, development of regional gas market and infrastructure).

BEMIP and especially BCM cooperation frameworks are a positive example of regional cooperation that has helped the Balts move toward meeting these targets. Nevertheless, it is clear that lack of political can cause delay or freeze the process. In the context of energy and infrastructure security, the B3 countries are mainly on the same page. But at the end of the day, investments in energy infrastructure usually (initially at least) increase network tariffs for energy consumers and influence the welfare of the industry and the economy overall.

Today, both higher- and lower-level B3 officials gather regularly to discuss energy issues. In parallel, there are working groups for electricity and gas transmission system operators, energy experts and regulators. Cooperation is constructive, and the participants are committed. Agendas continue to be followed. And if needed, it is

relatively easy to ask for constructive support or confirmation from higher level authorities (government or minister).

Overall, the experts brought together by the BSSP agreed that a number of challenges hinder full Baltic cooperation in bolstering economic security, particularly with regard to energy. These challenges span a number of different sectors, including political, public and private; and in moving forward, the Baltic States must express a serious commitment to come together, transcend their respective political interests and priorities, and address these multifaceted obstacles. The following topics were most commonly discussed during the BSSP workshops addressing economic resilience: energy security, public-private partnerships, strategic communication, infrastructure vulnerabilities, hybrid threats, and risk assessment and protections.

Attention was given to the need for the Baltic States to develop and share knowledge about preventative solutions, alerts, and practices to combat and resolve both physical infrastructure and hybrid attacks. If a vulnerability in critical infrastructure is exploited, it could completely destabilize an entire society. Because Russia, in particular, is increasingly innovative and unconventional in its aggressive campaigns vis-à-vis the Baltic States, intra-regional cooperation in enhancing and protecting current critical infrastructure is necessary. The role of strategic communication in this regard becomes relevant, as it can play an especially important part in anticipating and helping to resolve infrastructure attacks and vulnerabilities. Responses to hypothetical and current hybrid threats must be better communicated and synchronized across the Baltic States' governments and societies. For years, the Baltic States have progressed in efficiently responding to technical attacks from Russia. However, there is no comprehensive strategic approach in the region to disabling hybrid attacks, such as cyber or information breaches. Based on this existing cooperation at the technical level, though, intra-regional actions could establish similar procedures and information exchange on prevention of

accidents related to such cases as national disasters and physical or cyber-attacks on infrastructure.

Furthermore, active steps can be taken in an intra-regional context to buttress infrastructure resilience, such as synchronizing the power grids. It is also important to consider that infrastructure and broader economic and energy matters do not stand alone in the Baltic region—that is, they are deeply enmeshed in sociopolitical, security and geopolitical issues. Therefore, addressing such multifaceted problems in turn underpin Baltic economic growth and infrastructure.

Energy and security are intricately interconnected in the Baltic region, and significant portions of each Baltic State's economy and energy infrastructure are still vulnerable to Russia's influence and dominance. Currently, each Baltic government takes its own stance toward conceptualizing economic security, which poses an issue for intra-regional cooperation and long-term economic dependence from Russia. Solutions toward remedying this multifaceted issue must integrate a range of ministries and governmental actors, as well as non-governmental and private interlocutors. Furthermore, some BSSP experts agreed that the Baltic States should establish a systematic approach to analyzing and monitoring energy sector-related risks on a regular basis. Once again, the role of strategic communication resonates deeply with energy security in the Baltic States and is a critical factor in ensuring that energy projects are carried out fully and efficiently.

The BSSP experts unanimously agreed that when it comes to bolstering infrastructure across the Baltic States, there is a need for greater public-private cooperation. Currently, private cooperation is decent but insufficient by itself, and heightened public-private cooperation on infrastructure matters would, in turn, enhance overall security in this critical field. One idea provided in the discussion was to push institutions like the current NATO Excellence Centers located across the Baltic States to bring together and open communication

channels between public and private interlocutors. Moreover, as these Excellence Centers already publish on developments in the energy and economic realms, these findings could be made more accessible to the general publics. Such communication and cooperation between public and private actors should be especially considered and applied to "gray zone" times—that is, ambiguous periods that exist between definite peace and war. Private companies on their own should also work toward improving coordination on critical risk assessment and protections in an inter-regional context. Lastly, public consultation and media forums connecting the two sides—private and public—can play a proactive role in helping to improve public-private communication and cooperation.

B3 cooperation in energy security is, first of all, limited by the lack of understanding of regionalism among the states, which generally assess their energy security and energy security projects individually. This creates duplication of projects and expansion of excessive energy infrastructure in neighboring states, not leading to the most efficient or rational use of financial resources, including in maintenance costs.

Measures intended to bolster B3 economic security have been primarily undertaken at the national level due to the absence of a mutually agreed upon long-term vision for long-lasting economic prosperity and resilience. Each Baltic State focuses on its national interests and responses as well as assesses risk threats differently, rather than following a regional or European agenda. Without a sense of unity and determination to advance regional cooperation in this arena, any projects developed and implemented in an intra-regional context are thereby likely to be stunted or limited in impact and longevity. The post-Brexit reality vis-à-vis the European Union means that, in the future, there will be constrained financial resources for the Baltic States to attempt to lobby for and receive. Because of this looming even more competitive landscape, it is all the more imperative that the Baltic States commit now to developing a cohesive vision, a set of common tangible goals, and joint policy

recommendations in the realm of economic security that they can then express to international institutions like the EU.

The necessity for a unified B3 strategy in economic and energy field are especially underscored in relation to such strategic issues as the synchronization of the power grid, as well as a common position regarding the Astravets NPP.

Even a preliminary analysis points to several important areas where closer cooperation between the Baltic countries and coordination with strategic international partners could contribute significantly to the overall resilience of the B3 energy infrastructure:

First, based on existing cooperation at the technical level, the B3 energy transmission system operators should consider establishing similar procedures and information exchanges related to accident prevention involving natural disasters, physical attacks or infrastructure cyberattacks.

Second, with the increased importance of digital information networks for transmission system operation, existing communication routes and means and solutions for their improvement should be reviewed to improve the ability of operators to securely communicate in emergency events or overcome communication disruptions.

Third, in the light of existing trends, current mechanisms for direct technical assistance to energy system operators in emergency situations should be reassessed. It must be noted, that, for example, in power distribution networks, the overall level of automation and digitalization of network equipment allows the distribution system operators (DSO) to significantly decrease the number of personnel and motorized supply units for daily operation purposes. The Latvian DSO Sadales Tīkls has already acknowledged that the number of employees, including technical personnel, will be reduced by approximately 800 during next few years—in line with worldwide

trends in the industry. This, however, means, that additional analysis must be carried out to estimate the potential impact on the overall ability of the DSOs to mitigate disruptions to the power supply caused by larger natural disasters or directed attacks on infrastructure. Sharing of available technical and human resources and respective coordination and assistance at the regional level should be evaluated as one of the solutions to maintain or improve the existing resilience of Baltic DSOs and TSOs without compromising their efforts to improve overall operational and economic efficiency.

3.2. Energy Security

Tadas Jakštas

Introduction

The last several decades have seen many positive developments in improving energy security in the Baltic region. Progress has been made on building new infrastructure in the electricity and natural gas sectors to enable market integration and efficient market functioning. Overall cooperation at the political and technical levels has been growing, with regional energy security issues regularly discussed at various inter-governmental forums. In addition, power grid operations in the three Baltic countries—Latvia, Lithuania and Estonia (B3)—remain well coordinated, with regional transmission system operators (TSO) providing technical means and procedures to withstand technical malfunctions and security-related disturbances.

Some challenges remain, however—most notably the Baltic States' continued electricity grid synchronization with the Integrated Power System/United Power System (IPS/UPS), on the basis of the BRELL Agreement with Russia and Belarus. This situation means that the grid frequency and frequency containment reserves (FCR) in the Baltic States are both currently maintained from Moscow. Several other areas also need improvement, such as data analysis and information sharing, as well as policy coordination, common training and exercises, and a lack of understanding of regionalism that undermine regional energy developments.

Cooperation at the Political Level

At the political level, B3 cooperation on energy issues is strong. There

are many regional forums which discuss energy cooperation among the Baltic countries themselves as well as with the Nordic countries (Iceland, Denmark, Norway, Sweden and Finland) and Poland. For example, the Baltic Assembly, a forum for B3 inter-parliamentary cooperation, attempts to find common ground on many regional energy issues, including the diversification of sources of supply and routes of transit of imported energy, and the security of supplies (Baltic Assembly, 2018). In addition, The Baltic Council of Ministers (BCM), a forum for inter-governmental cooperation, discusses among other things the development of integrated and well-functioning regional gas and electricity market policies, the implementation of regional energy projects as well as nuclear safety and environmental requirements.

Cooperation between the Nordic and Baltic countries has been growing steadily since relations were formalized in the early 1990s. Through various initiatives such as the Baltic Energy Market Interconnection Plan (BEMIP), the Nordic-Baltic Eight (NB8, consisting of five Nordic countries and three Baltic countries), the Nordic Council of Ministers' cooperation with the Baltic countries, Baltic integration in the Nord Pool exchange market, and other initiatives, the link between the Nordic and Baltic countries has been growing over the years. For instance, BEMIP, introduced in 2009, aims to achieve an open and integrated regional electricity and gas market between EU countries in the Baltic Sea Region, ending energy isolation (EC, 2018). The initiative's members are the European Commission and Denmark, Germany, Estonia, Latvia, Lithuania, Poland, Finland, and Sweden; additionally, Norway participates as an observer. Much progress has been made under BEMIP and other such initiatives toward integrating the B3 energy markets with Europe. BEMIP allowed the Baltic States to receive financial support for the development of interconnections inside the region (reinforcing gas and electricity connections) and infrastructure outside it (e.g., the LitPol Link electricity interconnection, NordBalt electricity interconnection, and the Estlink 1 and 2 electricity interconnections).

Another regional format for Nordic-Baltic cooperation is NB8, including Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden, where the members discuss regional security issues such as energy security, the implementation of the EU 2030 climate and energy framework, the completion of essential regional energy infrastructure projects, cyber threats against the energy infrastructure, etc. (MFA Lithuania, 2018).

Despite a number of various political channels through which to discuss energy security issues, Baltic intra-regional cooperation in energy security has often been hindered by the domination of self-interests and the lack of understanding of regionalism among the states. This contributes to a duplication of projects and expansion of excessive energy infrastructure in neighboring countries, leading to inefficient or irrational use of financial resources. Infrastructure that could service the whole region is not accepted by neighboring countries as such. For example, the Baltic States showed disagreements during the development of a regional liquefied natural gas (LNG) terminal. Instead, Lithuania implemented an LNG terminal project in Klaipėda (floating LNG regasification unit) on its own, with political and financial support from the European Commission. The capacity of the LNG terminal in Klaipėda would still nearly satisfy the annual natural gas needs of the B3 and could, thus, serve as a regional LNG terminal. However, Latvia's and Estonia's governments refused to accept the Klaipėda LNG terminal as regional and have continued to pursue competing individual LNG terminal projects (Česnakas, 2017). Moreover, regional energy projects, despite their strategic significance, often become hostages of short-gain policies, which prolong their implementation and extend the period of energy insecurity for all countries involved. For instance, the issue of Baltic electricity grid synchronization has been blocked for several years due to disagreements between Lithuania and Estonia.

Intra-regional cooperation is also hindered by different political interests and priorities. The sense of extreme urgency that prevails in

Lithuania over the issue of synchronization does not exist in the other two Baltic States. In addition, relatively little attention is being paid to the Baltic synchronization debate in the countries belonging to the Nordic synchronous area. Moreover, the coordination of external energy policy among the B3 remains limited, as in case of the Belarusian Astravets Nuclear Power Plant (NPP), which Vilnius considers a national security threat, unlike the other two Baltic capitals.

Cooperation at the Technical Level

The Baltic States' power system (Baltic system) was historically developed to be, and operates currently as, synchronous with the IPS/UPS system. The networks of Estonia, Latvia and Lithuania are operated on the basis of the transmission system operators' BRELL Agreement. This ensures a constant coordination of activities among the TSOs in the Baltic States.

On the technical side, cooperation is built on several levels. The main mechanism of providing operational security of the energy infrastructure is the operative coordination between the transmission system operators: the existing exchange of information between TSOs allows them to quickly identify and mitigate or prevent most operational security disturbances and challenges as they occur. However, the exchange of information between operators and power suppliers is sometimes slow regarding operational decisions with a longer-term potential effect on security.

One example is the exchange of information regarding available power-production capacities. Currently, the domain for such information sharing is the Nord Pool Spot power exchange, but this system does not always provide the necessary data to evaluate the overall security implications of a given decision. For example, there were cases when a decision by one of the Baltic countries to

discontinue operation of significantly large but aging power-production capacities (approximately 1,000 megawatts) was communicated to neighbor countries via the Nord Pool Spot information exchange platform several only weeks before the implementation of the decision—and without prior consultations or regional security studies.

Cooperation among Baltic TSOs is also facilitated within the wider European ENTSO-E format. On February 18, 2015, European TSOs entered into the Multilateral Agreement on Participation in Regional Security Coordination Initiatives (MLA RSCI) (Baltic RSC, 2018). Baltic TSOs (Elering, AST, Litgrid), taking into account the provisions of MLA RSCI as well as experience already gained in different aspects of cooperation, then concluded further mutual agreements. In October 2016, the B3 TSOs notably signed the Baltic Regional Security Coordinator Agreement (Baltic RSC, 2018), designed to set up the framework for regional security coordination among these companies. Coordination within the Baltic RSC falls within the following main areas: an improved individual grid model/common grid model for delivery, coordinated security analyses, coordinated capacity calculations, short- and medium-term adequacy, outage planning coordination, as well as management functions of the Baltic RSC (Baltic RSC, 2018).

In the natural gas sector, closer cooperation on security issues has been mostly restricted by two factors. The first has been the existing cost of adding more regional security measures. But the second constraint has been the lack of a common B3 understanding about the amount of security measures needed to prevent accidents or possible attacks by third parties. As such, the B3 governments have not carried out common assessments of the role of such critical infrastructure as the Inčukalns natural gas underground storage facility in Latvia. But such an assessment will be necessary in advance of further discussions on the creation of a single Baltic and Finnish natural gas market area.

That said, since the unbundling of the gas market in Latvia, cooperation among the Baltic transmission system operators in the gas sector has begun to intensify. For example, in January 2017, the Baltic States' natural gas TSOs AB Amber Grid (Lithuania), AS Conexus Baltic Grid (Latvia) and Elering AS (Estonia) signed a Cooperation Agreement on the Implementation of the Implicit Capacity Allocation Model. The introduction of this model marks a concrete step toward the integration of the national gas markets of the Baltic States (Amber Grid, 2018).

Critical Energy Infrastructure Protection

The security of critical infrastructure in the Baltic States faces a number of challenges. Some of the most critical energy infrastructure nodes do not meet all physical security requirements. Moreover, there is a lack of intra-regional physical security exercises among TSOs in the Baltic States. Additionally, there is a lack of regional exercises to test for blackout scenarios. The existing intra-regional cooperation in critical energy infrastructure protection (CEIP) is not sufficient in the context of growing security challenges in the region. The intra-regional cooperation in energy security first of all is limited by a lack of awareness and understanding of the interconnectedness of threats in the region.

Economic cooperation in the Baltic region takes place mainly through maritime links, and there is a maritime dimension to almost every commercial activity in the B3, including when it comes to energy supplies (Ojala, 2016). Baltic Sea routes are used for exports as well as oil and gas supply diversification. In addition, the security of energy supplies could be disrupted by so-called "gray zone" (or "hybrid") operations, including military activities, in the maritime domain. Indeed, the Baltic Sea hosts some of the B3 countries' most important energy infrastructure (NordBalt, Estlink cables, LNG terminals).

Current B3 cooperation on maritime security situational awareness and exchange of information is limited. The level and scope of cooperation within the framework of the Sea Surveillance Co-Operation Baltic Sea (SUCBAS) program is not adequate, especially in the context of growing kinetic/non-kinetic threats in the region (e.g., aggressive exercises, dangerous overflights and maritime intimidation of vessels, as well as increasing submarine activity).

3.3. Financial Security

Didzis Kļaviņš

The Baltic States have experienced harsh financial and economic turbulence over the past ten years. The 2008 financial crisis was sudden and severely hit the Baltic economies. Described as the "Baltic Tigers" before the global economic downturn of 2008, Estonia, Latvia and Lithuania (B3) had to overcome the crisis by adopting tough fiscal austerity policies. While economic growth profoundly accelerated in all three Baltic States in the last five years, and economic development currently looks quite stable and positive, it is important to identify all possible risks and threats that may negatively affect future financial and economic security. The aim of this study is to look at financial and economic security in Estonia, Latvia and Lithuania, paying increased attention to major possible risks and disadvantages. As the theme is diverse and complex, the following will address three main questions: What are the most important challenges in Estonia, Latvia and Lithuania concerning financial security? What is the current state of intra-regional cooperation on financial security issues? And what are the main issues and gaps for intra-regional cooperation on financial security matters in the Baltic States?

The concept of security has been revised multiple times, and financial and economic security is associated with something different for everyone, owing to a broad spectrum of perceptions and contexts. According to the European Central Bank, financial security is related to a financial system's capability to withstand shocks without impairing the transformation of savings to investment opportunities.[95] Whereas, another definition may draw attention to

[95] European Central Bank. Progress towards a Framework for Financial Stability Assessment, available at

the absence of crises in the financial system and a diverse financial sector. It has also been defined as the efficient performance of the financial system in the event of crises and profound structural change. While financial security more often tends to characterize individual money management, economic security refers to the broader effect of monetary support. This study will consider the interrelatedness between financial security and economic stability, and that symbiotic relationship will be looked at in the context of the Baltic States.

Since the global financial crisis, Estonia, Latvia and Lithuania have strengthened the legal and institutional foundations of financial stability at the national, regional and international levels. Lithuania, for instance, enacted a Law on Financial Sustainability in 2009; and few years later (2015), it adopted a Strategy of Macro prudential Policy. In order to deal with the specific challenges of the financial system, the Bank of Lithuania was granted an explicit mandate to conduct macro-prudential policy. As a result, a newly introduced broad and flexible macroprudential policy toolkit now provides the Bank of Lithuania with the appropriate instruments needed to deal with the specific challenges of the financial system.[96] Similar improvements can been observed in Estonia and Latvia, too.

The current status of Baltic inter-regional cooperation on financial stability issues seems to be well integrated into the overall financial system of the European Union and the framework of the joint cooperation of financial institutions in northern Europe. In 2011, the Nordic-Baltic Macroprudential Forum (NBMF) was established in order to discuss risks to financial stability in the Nordic-Baltic

https://www.ecb.europa.eu/press/key/date/2007/html/sp070628.en.html (accessed August 10, 2018).

[96] Ministry of Finance of the Republic of Lithuania, information provided to the author, August 28, 2018.

countries and the implementation of macroprudential measures.[97] Lately, several memorandums of understandings (MoU) have been signed addressing financial stability issues in the Baltic and Nordic countries—the MoU on cooperation among Nordic-Baltic central banks regarding banks with cross-border establishments (2016),[98] the MoU on supervision of significant branches between the national supervisory authorities and the ECB (2017)[99] and the MoU on cooperation and coordination on cross-border financial stability between relevant ministries, central banks, financial supervisory authorities, and resolution authorities of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden (2018).[100]

---

[97] David Farelius. "Macroprudential Policy in the Nordic-Baltic Area." Seacen.org. https://www.seacen.org/publications/RePEc/702003-100385-PDF.pdf (accessed August 15, 2018).

[98] Memorandum of Understanding on Cooperation regarding Banks with Cross-Border Establishments between the Central Banks of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden, December 15, 2016, https://www.lb.lt/uploads/documents/files/news/2016-12-15_mou_-_publication_version.pdf.pdf.

[99] Accession to Memorandum of Understanding between Finansinspektionen (Sweeden), Finanstilsynet (Norway), Finanstilsynet (Denmark), Finanssivalvonta (Finland) and the European Central Bank on prudential supervision of significant branches in Sweden, Norway, Denmark and Finland, http://www.fktk.lv/en/commission/collaboration/memorandum-of-understanding/6409-accession-to-memorandum-of-understanding-between-finansinspektionen-sweeden-finanstilsynet-norway-finanstilsynet-denmark-finanssivalvonta-finland-and-the-european-central-bank-on-prudential-supervision-of-significant-branches-in-sweden-norway-denmark-and-finland.html.

[100] Memorandum of Understanding on Cooperation and Coordination on cross-border financial stability between relevant Ministries, Central Banks, Financial Supervisory Authorities and Resolution Authorities of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden, January 31, 2018, https://www.lb.lt/uploads/documents/files/Ziniasklaida/Naujienos/NBSG%20MoU_FINAL_31%20January%202018.pdf.

Due to the interlinked banking system, as the Bank of Lithuania describes, cooperation on financial stability issues (such as macroprudential policy, liquidity issues of cross-border banking groups, and crisis management) is quite close in the Nordic-Baltic region.[101] Having said that, it is unclear to what extent intra-regional cooperation takes place in practice between the relevant entities in the B3; the perception is that most such matters are settled at the national level. However, as mentioned by Andrejs Jakobsons, an economist and faculty member at the Riga Business School, when it comes to cooperation in the area of bank supervision, it is well-known that there are several institutions involved—as some of the banks are directly supervised by ECB.[102] While the framework for cooperation based on MoUs express a clear intention among relevant institutions to cooperate in the region and countries organize discussion forums, however, these agreements are not legally binding. Moreover, the current crisis management framework is rather new, established after the 2008 financial crisis.[103]

The issue of non-resident deposits is one of the biggest challenges facing financial and economic security in Latvia. According to Scope Rating, "non-resident deposits (mostly from Russia and other CIS [Commonwealth of Independent States] countries) amounting to 41% of total deposits are prone to flight in times of market volatility and are concentrated in banks servicing foreign clients, adding to financial risks."[104] While the total share of deposits from non-residents

[101] The Bank of Lithuania, information provided to the author, July 26, 2018.

[102] Andrejs Jakobsons (Economist, Faculty member at Riga Business School), interview with the author, July 18, 2018.

[103]The Bank of Lithuania, information provided to the author, July 26, 2018.

[104] Scope Rating, "Republic of Latvia: Rating Report," Scoperatings.com, https://www.scoperatings.com/ScopeRatingsApi/api/downloadanalysis?id=9911aa25-8524-4798-8774-0121683d6765 (accessed August 5, 2018).

has declined during the last three years, the current share remains significant.[105]Morten Hansen, the head of the Economics Department at SSE Riga, also states that non-resident banking is the main challenge in Latvia. "I have long thought of it as a comparative advantage for Latvia […] but it has been shameful to see how often it has ended up in money-laundering cases and other dubious kinds of business," Hansen summarized.[106] No doubt the recent AML scandals related to Latvia (the ABLV case) and Estonia (allegations of money laundering at Danske Bank in Estonia) prove that intra-regional cooperation is essential.[107] As aptly pointed out by economists Liudas Zdanavičius and Taurimas Valys, this situation in Latvia and Estonia also damages Lithuania's reputation even though the latter has more transparent financial market control and better rankings as well as support from the ECB.[108] Describing inter-institutional cooperation on financial security issues as weak, Valys acknowledged it should be more intensive, especially after the recent AML scandals in Latvia and Estonia.[109] If AML remains a national issue, Hansen rightly sees that as an institutional weakness.[110] Overall, it is important for all three

[105] The Economist Intelligence Unit. Latvian banking sector in the spotlight. Eiu.com http://country.eiu.com/article.aspx?articleid=1996467783&Country=Latvia&topic=Economy (accessed August 5, 2018).

[106] Morten Hansen (Head of Economics Department at Stockholm School of Economics in Riga), interview with the author, July 23, 2018.

[107] Andrejs Jakobsons (Economist, Faculty member at Riga Business School), interview with the author, July 18, 2018.

[108] Liudas Zdanavičius (Lecturer and Researcher at the Military Academy of Lithuania, interview with the author, September 5, 2018); Taurimas Valys (Associate Professor at Vilnius University Business School), interview with the author, July 30, 2018.

[109] Ibid.

[110] Morten Hansen (Head of Economics Department at Stockholm School of

Baltic countries to consider money laundering as a top priority to ensure the transparency of their domestic financial systems.

According to the MONEYVAL Committee's fifth-round mutual evaluation report on Latvia, "Latvia has taken steps to improve its AML/CFT legal framework."[111] But in acknowledging Latvia as a regional financial center with a majority of its commercial banks focusing on servicing foreign customers, the MONEYVAL report recommends that Latvian authorities "step up efforts to engage with key partners to address cooperation issues."[112]

Furthermore, as Jakobsons points out, there are also other areas that may create threats to Latvia's financial security under certain conditions. First, as the European Deposit Insurance Scheme (EDIS) is still under construction, problems in the Latvian banking sector may have broader implications (for example, negative impact on the Latvian budget if the Latvian deposit insurance system runs out of resources). Second, there are usually concerns that the state budget of Latvia may face some political pressure in an election year. So far, this has not materialized, partly thanks to continued growth. Besides, the Fiscal Discipline Law also provides mechanisms to prevent a deterioration of the situation. Third, adverse changes in the international financial markets may raise interest rates on Latvian debt, creating problems with refinancing.[113] However, with the

---

Economics in Riga), interview with the author, July 23, 2018.

[111] Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). "Anti-money laundering and counter-terrorist financing measures: Latvia." https://rm.coe.int/moneyval-2018-8-5th-round-mer-latvia/16808ce61b (accessed September 14, 2018).

[112] Ibid.

[113] Andrejs Jakobsons (Economist, Faculty member at Riga Business School), interview with the author, July 18, 2018.

government debt below 40 percent of GDP, this should not be a major concern under usual circumstances.[114]

Although Estonia, Latvia and Lithuania are able to offer many advantages to foreign investors (for example, an advantageous geographical location, low corporate income tax rates, educated and multilingual workforces, etc.), it is important (from an economic and security standpoint) for all three countries, and especially Latvia, to attract large-scale investment projects from the West. According to the Coordinated Direct Investment Survey (CDIS), a worldwide statistical data collection project launched by the International Monetary Fund (IMF), the top five sources of foreign direct investment (FDI) in Latvia are Sweden, Cyprus, the Russian Federation, the Netherlands and Estonia (see **Table 1**). It is widely believed that Cyprus, Switzerland, Luxembourg and Malta serve as transit countries for Russian capital.[115] Assuming that many Russian investors hide behind offshore companies, this likely makes Russia the largest foreign investor after Sweden.

Considering Russia's unpredictable behavior since the Russian-Georgian War (2008) and Russia's annexation of Crimea (2014), as well as the specifics of Russia's current foreign policy challenges, President Vladimir Putin's regime has economic instruments to exert pressure on Latvia. According to the Polish economic security specialist Adam Klus, "the Kremlin could punish Riga by forbidding Russians from making further direct investments in Latvia and, in more extreme circumstances, pressure current investors to liquidate their existing investments. Such measures would likely be ineffective if not counter-productive."[116] Having said that, it is important to note

[114] Ibid.

[115] Liudas Zdanavičius (Lecturer and Researcher at the Military Academy of Lithuania, interview with the author, September 5, 2018).

[116] Victoria Panova, "Foreign Economic Policy of the Russian Federation: The

that "the share of Russian investments constitutes an important, but not critical factor in Latvia's economic development."[117]

Taurimas Valys, an associate professor at Vilnius University Business School also believes that the current Kremlin regime is always trying to test the sustainability of various most important sectors, including financial sector (others are energy, media, infrastructure, cultural, etc.). As Valys noted, ignoring this might cause serious damage in the short and long term because it is one of the most sensitive areas, which may bias social and political issues without a strong risk management implementations process.[118] While Latvia and the other two Baltic States rely primarily on Western FDI (see **Tables 1–3**), it is important to strengthen Western companies' capital in the Baltic States.

The factors limiting future growth in Latvia—the lack of adequate labor and productive investment—are becoming more urgent. The growing shortage of qualified specialists can slow down growth potential as well as increase the pressure on labor costs.[119] According to an August 2018 survey conducted by the Latvian Chamber of Commerce and Industry (LTRK), the majority (67 percent) of business representatives are worried about shortages in the labor force.[120] In addition, high-value-added investments are still relatively

---

Constraints and Opportunities of the Baltic Dimension," in *The Economic Presence of Russia and Belarus in the Baltic States: Risks and Opportunities*, ed. Andris Sprūds (Riga: Mantojums, 2012): 61.

[117]Ibid.

[118] Taurimas Valys (Associate Professor at Vilnius University Business School), interview with the author, July 30, 2018.

[119] Ministry of Finance of the Republic of Latvia, information provided to the author, August 9, 2018.

[120] "67 Percent of Business Representatives in Latvia are Worried About Shortage of Laborforce," *Baltic Course*, August 3, 2018, http://www.baltic-

small.[121] While countries do compete with each other, the governments of the Baltic States should attracts more high-value-added investment and invest more in infrastructure that unites the Baltic region. Rail Baltica is one joint project likely to serve as a litmus test for the Baltic union concept. Until now, external threats and challenges, not joint initiatives and diverse projects, have been the strongest motivators for closer cooperation among the B3.[122] But Rail Baltica has the potential to bring significant socio-economic gains or all three countries.

The main risks and challenges to Lithuania's financial system include the following: the potential effect of imbalances in the Nordic countries and a snapback in risk premiums on the risk appetite of banks operating in Lithuania; the rapid growth of credit and real estate markets in Lithuania; as well as cybersecurity threats to financial institutions. According to the Bank of Lithuania, which semi-annually conducts a survey on risks to the Lithuanian financial system, domestic market participants view cyberattacks is the key risk for a year and half now.[123]As there is a high presence of Nordic banks not only in the Lithuanian banking sector but also in Latvia and Estonia, and given that household indebtedness in Sweden and Norway is high and continues to grow, falling housing prices could lead to bank losses

course.com/eng/analytics/?doc=142055.

[121] Ministry of Finance of the Republic of Latvia, information provided to the author, August 9, 2018.

[122] Didzis Klavins, "The Baltic Sea Region Stream in Latvia's Foreign Affairs," *The Centenary of Latvia's Foreign Affairs: Ideas and Personalities*, eds. Diāna Potjomkina, Andris Sprūds and Valters Ščerbinskis (Riga: Latvian Institute of International Affairs, 2016): 208.

[123] These surveys collect the opinions of market participants regarding their perceptions of risk. The Bank of Lithuania, information provided to the author, July 26, 2018.

and an overall economic slowdown. However, as the Bank of Lithuania has informed, the potential impact of this risk on banks operating in Lithuania is mitigated by the active implementation of macroprudential policy measures in the Nordic countries and the decreased indebtedness of Lithuanian banks to parent banks.[124]

Table 1: Inward Direct Investment Positions in Latvia (Top 10 Counterpart Economies, 2016)

Investment Source	Inward Direct Investment Positions (US Dollars, Millions)
World (total investment)	**14,185**
Sweden	2,229
Russian Federation	1,387
Cyprus	1,331
Netherlands	1,244
Estonia	1,027
Lithuania	763
Norway	741
Germany	642
Denmark	629
Luxembourg	625

Source: Coordinated Direct Investment Survey (CDIS), Data extracted from IMF Data Warehouse on 8/14/2018

[124] The Bank of Lithuania, information provided to the author, July 26, 2018.; Ministry of Finance of the Republic of Lithuania, information provided to the author, August 28, 2018.

Table 2: Inward Direct Investment Positions in Estonia (Top 10 Counterpart Economies, 2016)

Investment Source	Inward Direct Investment Positions (US Dollars, Millions)
World (total investment)	**19,368**
Sweden	4,907
Finland	4,449
Netherlands	1,791
Lithuania	751
Russian Federation	723
Cyprus	664
Latvia	650
Luxembourg	576
Denmark	508
Norway	486

Source: Coordinated Direct Investment Survey (CDIS), Data extracted from IMF Data Warehouse on 8/14/2018

Table 3: Inward Direct Investment Positions in Lithuania (Top 10 Counterpart Economies, 2016)

Investment Source	Inward Direct Investment Positions (US Dollars, Millions)
World (total investment)	**14,679**
Sweden	2,740
Netherlands	1,933
Germany	1,096
Poland	1,029
Cyprus	972
Norway	948
Estonia	779
Denmark	631
Finland	621
Malta	515

Source: Coordinated Direct Investment Survey (CDIS), Data extracted from IMF Data Warehouse on 8/14/2018

Interviews

1. Andrejs Jakobsons (Economist, Faculty member at Riga Business School), interview with the author, July 18, 2018.
2. Dainis Gašpuitis (Expert on Macroeconomics at SEB banka), interview with the author, August 1, 2018.
3. Ministry of Finance of the Republic of Latvia, information provided to the author, August 9, 2018.
4. Morten Hansen (Head of Economics Department at Stockholm School of Economics in Riga), interview with the author, July 23, 2018.
5. Taurimas Valys (Associate Professor at Vilnius University Business School), interview with the author, July 30, 2018.
6. The Bank of Lithuania, information provided to the author, July 26, 2018.
7. Ministry of Finance of the Republic of Lithuania, information provided to the author, August 28, 2018.
8. Liudas Zdanavičius (Lecturer and Researcher at the Military Academy of Lithuania, interview with the author, September 5, 2018).
9. Märten Ross (Deputy Secretary-General for Financial Policy and External Relations at the Ministry of Finance of the Republic of Estonia) interview with the author, September 10, 2018.
10. The Association of Latvian Commercial Banks, interview with the author, September 11, 2018.

3.4. Transportation and Infrastructure Security

Aivar Jaeski

Introduction

The three Baltic States—Estonia, Latvia and Lithuania (B3)—have often been lumped into a single security region since their liberation from Soviet occupation in 1991. To be sure, they share a common recent history and face largely the same security threats from their large eastern neighbor. But at the same time, they frequently exercise wholly independent and differing policies (including in defense, economic, foreign and environmental spheres) designed to preserve their national identities. Arguably, when the B3 states work together, they are security providers to the region; while membership in the North Atlantic Alliance makes each of them a security consumer. The transportation sector—which consists of several industries, including air freight and logistics, airlines, marine transport, road and rail, as well as physical transit infrastructure—plays a key role in relative levels of security both nationally and regionally. The following study will seek to identify the main threats to Baltic regional security from the perspective of the transportation sector and intra-regional cooperation in this area (see **Annex I**)

Current Status of Railroads Among Baltic States and Their Neighbors

The Baltic region has historically been a crossroads between East and West in terms of trade and passenger flows. Railway development in the 20th century was driven largely by military requirements. The passenger use of railways, while historically significant, is currently

outperformed by other means of transport; as a result, rail infrastructure and the level of service has seen limited development in the B3 countries.

The rail transit system in Estonia consists of about 1,452 kilometers of railway lines. This infrastructure is regulated and surveyed by the Estonian Technical Surveillance Authority. The Estonian railway network is owned by the state-owned company AS Eesti Raudtee and the private company Edelaraudtee Infrastruktuuri AS. These railway network infrastructure operators provide all network services for railway operators running freight and passenger services. With the help of European Union funds, Estonia has managed to replace all of its domestic passenger trains, in 2013–2014, with new Swiss-made Stadler trains. Even earlier and without EU support, in 2004, the country managed upgrade its freight trains with US-origin GE C36-7 type trains.

State-owned Latvian Railways has more than 12,400 employees and controls 1,933.8 kilometers of the country's 1,520-millimeter-width Russian-gauge railway lines as well as 33.4 kilometers of Latvia's 750 mm narrow-gauge railway lines. Latvian Railways carries all freight cargo in the country, and freight trains operate over the whole current passenger network, including a number of lines currently closed to passenger services. Latvia has renovated its existing Russian-origin trains but has not succeeded in purchasing any new train types to date.

Lithuanian Railways owns a main network consisting of 1,749 km of 1,520 mm broad-gauge railway, of which 122 km are electrified. A 179 km section of 750 mm narrow gauge network, listed as an object of cultural heritage, was split off into a separate company—Aukštaitijos Siaurasis Geležinkelis—in 2001. In 2006, Lithuanian Railways transported 6.2 million passengers and 50 million tons of freight. Oil is the main freight item carried. Lithuania has managed to modernize its train fleet; however, the number of different train types in its possession makes ongoing maintenance quite challenging.

As at the end of 2014, Finland had 5,944 km of railways in use, of which 3,256 km were electrified. This includes 5,342 km of single-track railways. Nearly €200 million a year is spent on track maintenance. The width of the Finnish rail network is 1,524 mm, which differs from the standard rail width (1435 mm) in use in most of the rest of continental Europe (although not the Baltic States or Russia). The speed limit for passenger trains traversing Finnish territory is 220 km per hour, and 120 km per hour for freight trains. Maintenance and construction of the railway network itself is the responsibility of the Finnish Rail Administration, which is a part of the Finnish Transport Agency. The Finnish business community as well as the Ministry of Transportation have shown interest in linking Finland to the Baltic States' railway networks. And a plan to build a connecting railway tunnel between Tallinn and Helsinki has increased Finnish interest in Rail Baltica (see below).

The Polish railways network consists of around 18,510 kilometers of track as of 2015, of which the vast majority is electrified. The nationally owned PKP Group operates the majority of rail services. In addition to PKP-owned companies, there are a number of private cargo operators as well as a number of independent passenger operators, owned predominantly by *voivodeship* (top-level administrative divisions in the country) governments. The vast majority of the network was built before World War II by various rail companies, and a minor component was built from 1946 onwards by the Communist authorities. Due to the average age of the network and lack of maintenance, many sections are limited to speeds below 160 km/h. Since Poland's entry into the European Union in 2004, major financing has been made available by European financing institutions to improve both the Polish rail network and the rolling stock fleet. Up to June 2014, the European Investment Bank had provided loans totaling €1.9 billion for rail modernization projects in Poland. An additional €578 million had been provided through December 2013 to modernize 70 percent of PKP Intercity rolling stock. The €665 million purchase of 20 Alstom Pendolino high-speed trains, delivered

in 2014, was financed in part by €342 million from the European Investment Bank. Still, Poland is heavily engaged in improving its own transportation network; therefore, it does not devote much attentions to its neighbors' projects.

The Russian rail network is ranked as the second longest globally, behind the total length of rail lines in the United States. Train transport in Russia has been described as one of the country's economic challenges in the 19th, 20th as well as the 21st centuries. State-owned Russian Railways accounts for 2.5 percent of Russia's GDP and employs 800,000 people. In 2007, about 1.3 billion passengers and 1.3 billion tons of freight went via Russian Railways. In 2007, the company owned 19,700 goods and passenger locomotives, 24,200 passenger cars (carriages) and 526,900 freight cars (goods wagons). A further 270,000 freight cars in Russia are privately owned. Russian Railways is a fully state-owned, vertically integrated company that manages both the infrastructure and operating freight and passenger train services. In 2012, it became one of the three largest transport companies in the world. Due to European and US sanctions on Russia since 2014, rail cargo transit from Russia to the Baltic States decreased dramatically—to the point where a cost/benefits analysis for the Rail Baltica project produced by the company the Ernst & Young (EY) has evaluated that the potential for Russian freight transit will be absolutely minor.

Belarusian Railway is a national state-owned rail company that operates all of the rail transport network in Belarus. As of 2005, Belarusian Railway employs 112,173 people. The train network consists of 5,512 km of rail lines with a Russian gauge of 1,520 mm; 874 km are electrified. The national network has no high-speed lines. Oil transit from Belarus is main source of income for Lithuanian Railways.

Rail Baltica Project

Rail Baltica is an international railway project that will connect the Baltics with Central and Western Europe. Rail Baltica is one of the B3 region's largest investments in years for a project designed to improve the travel opportunities for Baltic people. The rail project also aims to develop regional business, trade and tourism. The railway route will ensure speeds of up to 240 km/h and provide an opportunity to travel comfortably and quickly from Estonia to Latvia and Lithuania and onward to Central Europe and beyond.

Rail Baltica is a greenfield (i.e., new) rail transport infrastructure project with a strategic-level goal of integrating the Baltic States into the European rail network. The project includes five European Union partner countries—Poland, Lithuania, Latvia, Estonia and, indirectly, also Finland. It will connect Helsinki, Tallinn, Pärnu, Riga, Panevežys, Kaunas, Vilnius and Warsaw. Rail Baltica will feature fast, conventional, double-track electrified and ERTMS-equipped lines with a maximum design speed of 249 km/h (the maximum operational speed will be 234 km/h). Crucially, the new railway line will use the standard European 1,435 mm gauge, thus conforming to all requirements of the Technical Specifications for Interoperability (TSIs).

Rail Baltica, scheduled to be completed by 2026, will be fully electrified, thus avoiding localized emissions from locomotives. And only the newest technologies and materials will be utilized in the railway's construction. The line is planned to avoid Natura 2000 protected areas as much as possible and be built without significant impact on other environmentally sensitive protected areas. Wherever necessary, noise protection barriers will be installed. Special animal passages will be built across the embankment.

The project has presently reached the design phase and procurements

for Detailed Technical Design have been announced. According to a European Court of Auditors assessment of high-speed cross-border railway projects in Western Europe, the average planning period for such projects is 16 years. Thus, considering the fact that Rail Baltica has moved from planning to the design stage in only eight years, the project is arguably progressing remarkably smoothly.

The European Commission has committed to supporting the project by co-financing 85 percent of the costs; the rest should come from national budgets. The total estimated construction cost of the project is approximately €5.8 billion, according to the cost/benefit analysis prepared by EY. So far, the three Baltic States and the project coordinator, RB Rail AS, have received three grants for the construction of the Rail Baltica railway, having signed grant agreements totaling €824 million.

Thanks to its strategic value, the Rail Baltica project will bring greater economic security to the region. Today, Estonia, Latvia and Lithuania use old Russian-gauge 1,520 mm track lines, which provide easy access from the east. Yet, Russia is trying hard to avoid B3 railways for its export transit, building bypasses and using other transit corridors. After Russia annexed Crimea in early 2014, the West applied economic sanctions against some Russian transit sectors. As a result, Lithuanian Railways remains the only B3 player still earning some profit from transiting Russian oil being exported via Belarus.

Transporting goods by train from Western Europe to the Baltic countries is complicated because the rest of Europe uses the 1,435 mm gauge railway. To deliver products from Germany to Riga, these have to be reloaded from one train to another at the Polish-Lithuanian border, which takes time and increases costs. Therefore, it is fair to say that the B3 are, economically speaking, still more dependent on the eastern railway market then the European common market. This comes with rather profound security challenges: the Baltics can be economically manipulated by, for example, Moscow suddenly

refusing to deliver spare parts for Russian-origin technologies or seeking alternative transportation corridors for its western-bound exports. Rail Baltica, however, promises to address this economic-security vulnerability by bringing the Baltics closer to the EU single market.

The construction of Rail Baltica will deliver €5 billion worth of investment into region, thus helping to boost not only the construction sector but also scores of related businesses. Benefits will accrue to all key stakeholder groups: travelers (travel time and cost savings), freight shippers (travel time and cost savings), railway companies (operating profit), inhabitants around major regional roads and airports (reduced local noise, air pollution), and the general public (climate change mitigation, tourism, cultural/educational exchange).

Lastly, there is an important hard-security dimension to Rail Baltica, as well. Here it is useful to recognize the historically important role armored trains played in the Estonian and Latvian wars of independence during the early 20th century.

A military role for railways continues to exist even today, particularly when it comes to supplying forces and moving large pieces of military equipment. Trains have some great logistical advantages over trucks, ships and airplanes, which boil down to speed and cost. First, rail moves faster than cargo vessels, which top out at around 35km/h. Second, the transport of tanks or other heavy armored vehicles by airplane or truck over long distances becomes extremely expensive. Rail Baltica will, thus, have an important role in improving the Alliance's military supply chain from Western and Central Europe to the Baltics.

What do the B3 and wider Europe stand to lose if Rail Baltica is canceled? For one thing, shorter travel times, new businesses, decreased environmental pollution, EU investments into the Baltic

economies, new jobs, greater cultural exchange, more opportunities to study in neighbor countries, and so on. But just as importantly, not following through on completing Rail Baltica will mean a missed opportunity to more strongly link the B3 with the rest of Europe.

Military Logistics and Civil Defense Considerations

In the Baltic States, as in much of the rest of Europe, military criteria rarely trump civilian concerns when it comes to transportation and other related security domains. After the collapse of the Soviet Union, preexisting civil defense considerations were frequently ignored; and when it came to newly built infrastructure and systems, there was no authority in the Baltic countries able to competently assess military requirements in infrastructure and other engineering projects. This same tendency could be observed all over post–Cold War Europe, with the largest shortfalls arguably present in the EU's railway freight transportation sector. Notably, maximum axle load on European railways is two times lower than in the US, thus limiting the use of train cars for transporting heavy military equipment. To finally try to address this weakness, the EU recently launched a Military Mobility action plan.

It would be easy to say that the Baltics simply need to follow the rules agreed at the NATO and EU levels. But the problem is execution. Mainly, it is the member state's individual responsibility to fall in line with the agreed-upon standards. And when resources are limited, priorities regarding implementation can quickly diverge.

Conclusions

Baltic regional security relies heavily on NATO from a military perspective and on the EU when it comes to economic security concerns. But at the same time, Estonia, Latvia and Lithuania are actively in the process of strengthening and modernizing their national security apparatuses. Unfortunately, due to limited

resources, they continue to face challenges in this endeavor. Those challenges certainly include the high price of procuring advanced military equipment. But they also comprise the costs related to the construction of strategic (including trans-border) infrastructure and, importantly, the question of how to apply the same standards across the region in the continued absence of concrete agreements to this effect. The third shortfall relates to the fact that even when NATO and the EU establish minimum requirements, these tend to ignore specific regional differences, while giving extensive freedom of action to member states to implement those standards as they see fit, with little oversight from Brussels.

Returning specifically to the focus of this study, the above-mentioned issues and gaps in intra-regional transportation and infrastructure security cooperation should be addressed by, *inter alia*:

1. The B3 countries agreeing on common regional policies, standards and procedures that are in line or supplementary to NATO and EU regulations;

2. Implementing joint procurement among the three Baltic States. To date, there have been no success stories to showcase in this field;

3. Establishing joint enterprises and institutions akin to NATO Centers of Excellence to address the transit sector. Rail Baltica is already a positive example of a joint project that is galvanizing the regional railway business sector, boosting investment, as well as, importantly, leading to sharing knowledge, experts, standards, new technologies, manpower and money.

The implementation of cross-border projects is often hampered by national interests, especially from an economic point of view. Thus, when foreign investments from international organizations like the

EU are secured to fund strategic infrastructure, those international organizations should be given more of a leading role to implement these projects.

Intra-regional B3 cooperation regarding transportation and infrastructure security will bring with it closer relations with other NATO allies, as well as common understanding and fiscal savings. Regionally oriented joint organizations and activities, like regional commands, joint enterprises and joint procurement can certainly bring positive implications. But all that requires, first of all, vision, will and investments. Therefore dedicated, continued and successful implementation of existing agreements like the EU Military Mobility action plan as well as economically important projects like Rail Baltica must keep moving forward.

3.5. Expert Recommendations

Energy Security

1. Initiate the development of a unified Baltic Security Strategy in the economic and energy fields as well as a common position toward various regional energy projects. Within the context of the Baltic Security Strategy, identify the key factors that allow a state to maintain energy security, including the increasing share in renewable energy sources, interconnections, and support for renewables/carbon-based fuel switching.
2. Foster regional investments in the energy domain (e.g., in the renewable sector) to better coordinate policies at the strategic level.
3. Step up technical efforts to implement the synchronization process by putting forward concrete solutions to synchronize the Baltic States' electricity system with the continental European Network even before the target date of 2025. Since Kaliningrad has made substantial progress in recent years in improving its electricity infrastructure to ensure self-sufficiency in electricity supplies by 2020, the Baltic States' transmission system operators (TSO) should assess the ability of the Baltic power system to work synchronously in a crisis situation as soon as possible.
4. In order to develop close cooperation at the technical level, increase the regional TSOs' situational awareness and ensure they intensify information sharing.
5. Based on existing cooperation at the technical level, establish similar procedures and information exchange by all energy transmission system operators regarding incident and accident prevention, related to such causes as natural disasters, physical attacks or cyber-attacks on infrastructure.

6. In order to mitigate threats to sea lanes of communication and ensure the security and safety of energy infrastructure in the maritime domain, make sure the national authorities in the Baltic States work together with the Nordic countries to address some of the following important challenges:
    a. Establish common coordination mechanisms to link maritime surveillance systems in the Baltic Sea Region in order to maintain 24-hour situational awareness in the entire Baltic Sea.
    b. Improve coordination and information sharing between national agencies, such as coast guards. In addition, national emergency response mechanisms should be integrated into regional response plans together with improvements in information sharing.
    c. Facilitate intra-regional cooperation to counter Russian threats and the legal challenges they present by creating a common intra-regional International Maritime Law Center that could study, address, and respond to hybrid threats in the maritime domain.
7. Increase the NATO Shipping Center's (NSC) engagement and cooperation with the civilian maritime community in the Baltic Sea Region.
8. Increase crisis preparedness by developing and testing contingency mitigation plans for partial/full closure of maritime areas of the Baltic Sea that could also affect energy supplies. Such plans should reflect the mitigation measures, including alternative land and sea lanes of communication. The necessary infrastructure and arrangements for fuel supply/re-supply and distribution operations should be tested in joint regional civilian-military exercises.
9. Improve regional maritime training focusing on the most effective counter measures against the intentional/unintentional loss of Global Navigation Satellite System (GNSS) signals.

10. Develop a comprehensive response strategy to mitigate threats to critical energy infrastructure (CEI). Toward this end, the national authorities in regional countries should:
    a. Include the protection of critical energy infrastructure into regional civilian-military exercise scenarios for national and multinational training purposes.
    b. Coordinate actions to protect cross-border connections through regular security checks and analysis, including regional cross-border exercises that would involve energy infrastructure.
    c. Increase cooperation between regional TSOs in organizing common physical-security and cybersecurity training and exercises. For example, it is important to regularly organize regional physical-security exercises for protection of cross-border energy infrastructure between all relevant agencies of neighboring countries.
    d. Test and verify procedures for fuel/oil-supply disruptions by organizing regional live fuel-supply exercises, including civilian and military sectors.
    e. Develop intra-regional cooperation and share best practices in raising cybersecurity awareness among the personnel in energy sector.
    f. Foster attractiveness to investors by way of a common market in energy and infrastructure, including the coordination of taxes, tariffs, and regulations. This would also include promoting free operation between the three countries for TSOs.
    g. Practice greater transparency. Countries should state their interests and priorities (what they cannot afford to lose) up front when coordinating common market activities in a format such as Chatham House Rules. Furthermore, current channels for communication need to be improved, rather than trying to create new channels. This recommendation goes for private companies and individual government agencies as well. Results of

exercises and studies need to be made available. Likewise, banks need to be more transparent with the structure of investments.

h. Coordinate information sharing between governments, private sector businesses, and government agencies. Here again, the current channels for communication should be improved, rather than creating new channels. Furthermore, government and civilian channels need enhancement, including, but not limited to, greater cooperation between civilians and navies/coast guards for disaster preparedness.

i. Improve intra- and inter-regional situational awareness, including regular cross-border checks and analyses, as well as cross-border exercises involving energy and fuel supply infrastructure. An inter-regional maritime law center should be established to study, address and respond to hybrid warfare challenges. Finally, close cooperation with neutral allies Finland and Sweden needs to be improved to link maritime surveillance systems in the Baltic Sea region.

j. Develop comprehensive response strategies at the regional, inter-regional, and inter-agency levels to challenges posed by gray zone operations, cyberattacks, and other security risks. Information sharing is integral to the effectiveness of this recommendation. Likewise, contingency exercises should intensify to enhance preparedness, especially in cybersecurity.

k. Maintain EU frameworks for funding. The EU provides a safeguard for securing funding and promoting common objectives. Likewise, in securing sources of funding, the Baltic States must make sure that the motives of the investors are known and clear. Risk management measures must be taken in sectors where third parties are highly involved, such as transport and logistics.

l. Take a systematic approach to energy and infrastructure security. Diversify supplies, fuel portfolios, and supply routes in order to work toward regional self-sufficiency in a free-market format. Integrate the network of critical infrastructures to enhance military mobility, including networked industries.
m. Improve public awareness of how the energy market works and about the interconnectedness of threats.

Financial Security

1. Promote the fact that, in the Baltic States, the overall financial and economic situation is stable (public debt is moderate by international standards, and the state budget has not experienced any major shocks recently; external trade and financial flows are much more balanced than a decade ago).
2. Attract more high-value-added foreign direct investment (FDI) in order to sustain and foster economic growth.
3. Establish intra-regional (Estonia, Latvia, Lithuania) cooperation mechanisms on financial security issues. This is crucial to the effectiveness of anti-money laundering operations and countering the financing of terrorism in each country.
4. Diversify risks by taking preventive measures to ensure economic stability and regularly identify all possible threats. Risk assessment in combination with inter-institutional trainings could help the Baltic States to be better prepared for unforeseen financial and economic fluctuations.
5. Consult regularly with financial and economic experts representing leading think tanks or research institutions, as well as synchronize the approaches and methodologies of relevant ministries, Central Banks and Financial Supervisory Authorities to assess financial risks and identify challenges.

6. Crucially, ensure that Baltic political elites do not lose focus on economic security issues. These, in combination with societal security, are among the most substantial factors determining and strengthening the feeling of belonging of ethnic groups to a particular society and state.

Transport and Infrastructure Security

1. Develop, agree and implement common regional military criteria for transportation and infrastructure areas in the Baltics.
2. Seek political agreement regarding long-standing policies for transportation and infrastructure area developments in the Baltics.
3. Develop a regional action plan on how to improve resilience against new threats in the Baltics.
4. Support the Rail Baltica project with political statements and the encouragement of Baltic political leaders.
5. Invest in the Rail Baltica project by sharing knowledge, experts, standards, new technologies, manpower and money.
6. Improve existing railway networks and simplify cross-border procedures.
7. Establish common regional policies, standards and procedures that Estonia, Latvia and Lithuania all agree on and that are in line with or supplementary to NATO and EU regulations.

4. CYBERSECURITY

4.1. Expert Assessment

Olevs Nikers, Otto Tabuns, Piret Pernik, Edgars Poga

Numerous international organizations—the North Atlantic Treaty Organization (NATO), the European Union, the United Nations, the Organization for Security and Cooperation in Europe (OSCE), the Organization for Economic Cooperation and Development (OECD), the Council of Europe, etc.—that have already put forward their own cybersecurity initiatives. And so, it is fair to ask what added value could come from developing greater Baltic intra-regional cybersecurity cooperation, either within or outside of these preexisting formats.

At the political level, Estonian, Latvian and Lithuanian (B3) cooperation in the cybersecurity domain is quite intense. Cybersecurity issues are regularly discussed in different official formats, including the Baltic Council of Ministers as well as the Baltic Assembly. The same can be said about talks between the Baltic and Nordic countries. Importantly, these issues are often discussed within the broader topic of regional resilience against hybrid threats.

That said, in the area of cybersecurity, the Baltic States could benefit from more institutionalized and regular cooperation in the following areas:

1. Exchange of experiences and lessons learned in improving basic cyber-hygiene skills across at the central, regional and local levels of administration (municipal governmental authorities). Lessons learned should be shared regarding national initiatives to improve cybersecurity awareness in

society because cybersecurity threats and vulnerabilities are quite similar across the B3.

2. In the telecommunications, financial, energy and transport sectors, there are B3 joint ventures that operate in all three countries, and there are interdependencies related to cross-border vital services and infrastructure. A need exists to map these interdependencies and vulnerabilities, as well as coordinate various state-level prevention and resilience approaches and measures. Cybersecurity baseline requirements for vital services are not harmonized across the Baltic States. Added value could come from developing joint approaches in some sectors or sub-segments, but this needs further research. Based on expert interviews with B3 government officials and critical infrastructure owners and operators, researchers should look into specific areas and measures to support cross-border resilience of critical information infrastructure. Once a final agreement on the synchronization of the B3 electricity networks with continental Europe is achieved, there will be further need to cooperate on enhancing the cybersecurity aspects of regional and European electricity networks.
3. Research is needed on further ways to foster B3 crisis-response cooperation in the even to of a large-scale cyber incident that affects more than one country. One example could be to establish cooperation between the Cyber Defense Units of the Estonian, Latvian and Lithuanian national guards with regard to penetration testing (pentesting) of critical infrastructure and incident response.
4. Despite the existence of national initiatives to curb disinformation in social media, there is little B3 cooperation in this field. Possibilities to exchange best practices and to develop common approaches should be explored.
5. Lithuania has proposed to develop a Rapid Reaction Team (RRT) within the EU's Permanent Structured Cooperation (PESCO) format; but Latvia and Estonia have not joined the

project. It should be analyzed if a Baltic regional RRT would add value.

6. More institutionalized and regular coordination of national positions is needed regarding the application of international law, development of norms of responsible state behavior and confidence-building measures (CBM) ahead of multilateral meetings of the UN, the OSCE and the Council of Europe. A designated Point of Contact in each country could facilitate this process.
7. Education, training, and exercises should be developed with an eye toward a strong cybersecurity curriculum at the Baltic Defense College.
8. Regional defense academies, universities and think tanks should consider jointly applying for funding to undertake cybersecurity research projects. An EU initiative already exists to create a European Cybersecurity Research and Competence Centre and network that would, among other objectives, fund new research. B3 educational institutions should consider proposing joint research projects to this body.

Ahead of its Baltic neighbors, Estonia already takes part in several bi- and multilateral cybersecurity and defense cooperation formats. Since B3 have different capacities and levels of cyber security maturity it might not be feasible to include all of them in all of the same formats—especially since the basis for such cooperation is, first of all, national interest, existing resources (human, technical, financial) and relative capacity.

Additional interviews with subject-matter experts in all three countries are needed to determine where deeper cooperation is needed to improve the Baltics' levels of cybersecurity. A preliminary assessment by the Tallinn-based International Center for Defense and Security (ICDS) found that current cooperation and information exchange between B3 state authorities on cybersecurity issues is

optimal, effective and efficient. And yet, this cooperation could be greatly improved at the operational level. Potential approaches include:

1. Closer cooperation between national Computer Emergency Response/Readiness Teams (CERT) regarding the exchange of information on threat assessments and best practices.
2. More intense cooperation between B3 CERT on pentesting of critical infrastructure and incident response, including building a cyber toolbox for rapid reactions teams.
3. Exchange of information between cyber security institutions on cyber awareness, cyber hygiene projects, exchange of national best practices should be intensified.
4. Better cooperation and coordination on cybersecurity exercises.
5. A coordinated approach among the Baltic States on mapping/assessing the interdependencies existing between essential services, including communications, energy, and transportation. This should involve exchange of information, discussions on methodologies, common assessment tools, etc.
6. Cooperation through the framework of NATO Centers of Excellence (COE). The NATO Energy Security (ENSEC) COE, for example, should be better utilized to work on certain cross-sectoral issues.

4.2. Addressing Cooperation Challenges

Edgars Poga

Introduction

The following analysis looks at five aspects of cybersecurity activities that would be more efficient if executed together by all three Baltic States—Estonia, Latvia and Lithuania (B3). These are national measures to promote education in regard to cybersecurity, the coordination of various cybersecurity efforts between the three countries, deepening the understanding in society of cyber threats to the electoral process, cybersecurity as a key to modern energy resilience, as well as the reform of legal frameworks to enable a wholesome cybersecurity effort by the Baltic States.

Development of Cybersecurity Capacity Through Education in Both Public and Private Sectors

Cybersecurity is still a relatively modern topic, dating back only to the 1980s[125]; but in regard to the B3 states, it became a national priority even more recently, motivated by the cyberattacks against Estonia in 2007.[126] Yet, despite its novelty, so to speak, cybersecurity is an immensely complicated subject that—as noted by professionals of the B3 national Cyber Emergency Response Teams (CERT) and academics in the field—requires attention to training and education in both the private and public sectors. Indeed, this point is made in all

[125] Vin McLellan, "CASE OF THE PURLOINED PASSWORD," *The New York Times*, July 26, 1981, https://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html.

[126] A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Cyber Conflict Studies Association, 2013).

of the B3 cybersecurity strategies.[127] A recent survey carried out by the international professional association focused on information technology (IT) governance, ISACA, cybersecurity "[d]emand is greatest for skilled technical resources at the individual-contributor level, rather than the management or executive level."[128]

The demand for cybersecurity professionals and general capacity building can be approached from the perspective of two levels of educational incentives. First, the education of new cybersecurity professionals can be provided, for example, through the programs of Vidzeme University of Applied Sciences,[129] the Riga Graduate School of Law[130] and the cyber-defense unit of the National Guard[131] in Latvia; the Vilnius University[132] in Lithuania; and Tallinn University of

[127] National Cyber Security Organisation: Lithuania - https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf; National Cyber Security Organisation: Estonia - https://ccdcoe.org/multimedia/national-cybersecurity-organisation-estonia.html; Cyber Security Strategy Of Latvia 2014–2018 - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

[128] "State of Cybersecurity 2018: Workforce Development," ISACA, http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF?regnum=455415.

[129] "Cyber Engineering Master's Degree," Vidzemes Augstskola, http://va.lv/en/study-here/masters-degree/cybersecurity-engineering.

[130] "The Law and Technology Masters Programme," Riga Graduate School of Law, https://www.rgsl.edu.lv/programmes/law-and-technology.

[131] "Cyberdefence unit of the National Guard of Latvia," National Guard of Republic of Latvia, http://www.zs.mil.lv/lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx.

[132] "Information Systems and Cyber Security Undergraduate studies," Vilnius University, https://www.vu.lt/en/studies/undergraduate-studies/56-studies/studies/3829-infor-system-cyber-security.

Technology[133] in Estonia. In other words, each of the B3 states is moving forward with the overall building of educated professionals in the field of cybersecurity. While this may be effective for each individual state's domestic goals, there is clearly a possibility here for better information exchange among them at the academic level, which could be realized through the development of a joint Baltic Cybersecurity program on the basis of Baltic university cooperation. This idea has, in fact, already been articulated in the current Latvian Cybersecurity strategy: "Create a common Baltic university study program to combine regional educational resources for preparing strong and qualified experts."[134] Second, the development of a common educational program specifically targeting policymakers and other professionals could help resolve the problem of institutional policies being adopted that are incoherent with cyber defense and expanding the capacity of CERTs and national cyber-defense structures. This will allow B3 domestic authorities to shift more of their focus to regional/international cybersecurity threats.

Taken together, the aforementioned approaches facilitate the establishment of a single point of contact—a step that will be more deeply analyzed within the next sub-section (**Dedicated B3 Point of Contact on Cybersecurity Matters**). Moreover, as established, the lack of general capacity to reach the aims of effective cybersecurity cooperation between the B3 states provides for the necessity to remove the burden from the national CERTs and national cyber-defense structures. The said goal is accomplished by educating both cybersecurity professionals and policymakers. This, then, can provide the national institutions with the required amount of professionals

---

[133] "Cyber Security Masters Programme," Tallinn University of Technology, https://ttu.ee/cyber-security/.

[134] "Cyber security strategy of Latvia 2014–2018," Ministry of Defense of the Republic of Latvia, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss.

educated both in the technical field of cybersecurity and cyber politics when tackling the harmonization of policies, strategies or law. It will provide the possibility of creating a permanent position of cyber affairs official in charge of national cybersecurity. Hence, the educational system that prepares both dedicated experts in the field of cybersecurity and educated policymakers effectively would expand the reaction speed to threats at the regional level while still contributing to the aims set forth by the North Atlantic Treaty Organization (NATO) to develop a "partnership with industry and academia from all Allies to keep pace with technological advances through innovation."[135]

Solely identifying the seriousness of cybersecurity is not enough to ensure growth of capabilities and capacities in this field. The requirement is to educate new experts using a bottom–up approach and intra-regional sharing of expertise. The policies, which move toward the establishment of a common educational atmosphere, have to be built upon a basis of understanding the crucial interdependencies between the B3. Thus, it will evade the possible overlap with projects established by NATO, the European Union, the Organization for Security and Cooperation in Europe (OSCE), the Organization for Economic Cooperation and Development (OECD) and other organizations in which the B3 states are active participants. That said, the common educational atmosphere can be further advanced by having its policies and aims coordinated with the above-mentioned organizations via a dedicated point of contact.

Dedicated B3 Point of Contact on Cybersecurity Matters

The Locked Shields 2018 exercise took place on April 23–27 of that year, at the NATO CCD COE, in Tallinn.[136] But at the same time,

[135] Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, NATO, 12 July 2018.
[136] "*The Largest International Live-Fire Cyber Defence Exercise in the World to be*

Lithuania hosted the multinational Amber Mist exercise, thus proving the necessity for more efficient coordination of exercises, operations and different cyberspace-related activities not only between the B3 governments but also with international organizations active in the Baltic region.

The main obstacle to closer B3 cooperation is the excessive concentration on national issues, leading to frequent disregard for common regional interests of strategic importance. Therefore, it is crucial that the Baltic States establish a joint single point of contact to avert such problems in coordination as the previously mentioned example of overlapping Locked Shields and Amber Mist exercises in 2018. Namely, coordination is needed in exercises, operations and different incentives. Guided by the examples of BALTBAT, BALTRON and BALTNET,[137] the Baltic States already have significant experience of developing cooperation in different operational domains. The creation of a single point of contact in cyberspace has to be highlighted even more after the NATO Warsaw Summit, in 2016, which declared cyberspace as an operational domain.[138]

A single point of contact can be achieved in many institutional forms, but one of the most recently developed initiatives is the position of a "cyber affairs official." Two poignant examples are the new NATO Communications and Information (NCI) Agency's chief of

---

Launched Next Week," The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/largest-international-live-fire-cyber-defence-exercise-world-be-launched-next-week.html.

[137] "Baltic Defense Cooperation," Ministry of Foreign Affairs of the Republic of Latvia, http://www.mfa.gov.lv/data/file/e/Books/Latvia%20in%20Facts/Bdc.PDF.

[138] "Warsaw Summit Key Decisions", North Atlantic Treaty Organization. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf.

cybersecurity[139] as well as Australia's dedicated cyber affairs official.[140]

Even though the Tallinn-based International Center for Defense and Security (ICDS) recently evaluated the degree of cybersecurity cooperation between the B3 state governments as very good,[141] with cyber issues persistently appearing as a regular agenda item at all levels of trilateral meetings, this cooperation could nonetheless be improved by developing a "cyber affairs official" position. With representation and coordination work delegated to a joint Baltic cyber affairs official, the national-level cybersecurity institutions such as CERTs could devote all of their attention to building up technical expertise. Moreover, with coordination help from the Baltic cyber affairs official, dedicated cybersecurity departments of the Baltics' various state institutions could simultaneously develop new legal and policy initiatives urged by both state and international organizations.

A bottom-up approach is needed to achieve the above recommendations because, first, a sufficiently large pool of experts has to be created with active communication between them and the state. This will enable an academic basis upon which the position of a Cyber affairs official can then be developed. Indeed, this point is made clearly in a 2018 report by the Latvian Institute of International Affairs (LIIA), entitled "Security in the Baltic Sea Region: Realities and

---

[139] "Cyber Security", NATO Communications and Information Agency. https://www.ncia.nato.int/Our-Work/Pages/Cyber-Security.aspx.

[140] "Australian Ambassador for Cyber Affairs.", Australian Government Department of Foreign Affairs and Trade, https://dfat.gov.au/about-us/our-people/homs/Pages/ambassador-for-cyber-affairs.aspx.

[141] Hayretdin Bahşi, Anna Bulakh, Nolan Theisen, Tomas Jermalavičius, Artūras Petkus, and Emmet Tuohy. *The Geopolitics of Power Grids – Political and Security Aspects of Baltic Electricity Synchronization*, (Tallinn: International Centre for Defence and Security, 2018), https://uploads.icds.ee/ICDS_Report_The_Geopolitics_of_Power_Grids_Tuohy_Jermalavicius_Bulakh_March_2018.pdf.

Prospects."[142]

The single B3 point of contact, whether in the form of a cyber affairs official or a chief representative, will provide the Baltic national ministries with a structured approach to policy and exercise planning. Furthermore, the existing operations within the framework of the NATO COEs will be utilized in a more standard manner and developed more fully with the help of cybersecurity assessment reports.

Enhancing Societal Security Through More Secure Elections

Russia notoriously succeeded in interfering in the 2016 US presidential elections, despite widespread understanding that extra precautions are advisable when it comes to protecting elections—both due to the need to maintain societal security as well as trust in government officials, information, and communications systems (ICT). In contrast, positive lessons in how to successfully counter Russian electoral interference can be drawn from the French elections of 2017.[143]

Thus, by having effective communication between national CERTs and cybersecurity professionals, it is possible for the B3 to, first, deal with malicious occurrences ahead of time. Second, by ensuring the digital aspects of electoral systems are actively monitored, tested and in, case of any findings, patched, the B3 can guarantee their elections

---

[142] Andris Sprūds, Māris Andžāns. *Security in the Baltic Sea Region: Realities and Prospects,* The Rīga Conference Papers 2017. Accessed on December 5, 2018, http://liia.lv/en/publications/security-in-the-Baltic-sea-region-realities-and-prospects-the-Riga-conference-papers-2017-643?get_file=1.

[143] Jean-Baptiste Jeangène Vilmer, "Successfully Countering Russian Electoral Interference 15 Lessons Learned from the Macron Leaks," *Center for Security and International Studies*, (June 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180621_Vilmer_Countering_russiam_electoral_influence.pdf?qFOz5qjpEuTzu5cvUa.UgOj0Dg3FklQP.

based on the rule of law as well as societal security. Finally, by educating individuals participating in elections (either as candidates or voters) of proper election-related cyber hygiene, public awareness and trust in democratic elections can actually be further heightened.

Resilience of the Energy Sector Through Greater Public-Private Cooperation

When it comes to boosting B3 energy sector resiliency in the cyber sphere, recommendations can be divided into three examples of cooperation:

1. Cooperation within the already-existing framework of energy security;
2. Incentives at the EU level; and
3. Existing regional frameworks such as the Nordic-Baltic (NB8—Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway and Sweden) and Nordic Defense Cooperation (NORDEFCO).

First, transmission system operators (TSO) are currently the primary mechanisms of operation security with regard to energy security cooperation. The current version of information exchange among TSOs provides for quick identification and mitigation of security disturbances and challenges in the online environment, thus, creating both a problem and an opportunity. The problem lies in the fact that the current structure is prone to cyber threats. But on the other hand, the TSOs are adaptive and capable of efficiently transmitting information. Therefore, building up more flexible communication by giving national CERTs access to these TSO mechanisms can be expected to strengthen the cross-sectorial interdependencies of the B3 within the already-existing framework.

Second, the current state of cooperation is mostly within the frameworks of leading international organizations (NATO, EU,

OSCE, OECD); whereas, at intra-regional level, cooperation between national CERTs is limited mainly to such exercises/events as Locked Shields[144] and Crossed Swords.[145] Therefore, it is necessary to put emphasis on B3 information-sharing within the scope of the European Union Agency for Cybersecurity (ENISA), to which they all belong. This EU body, importantly, helps to proactively facilitate long-term operational relationships between experienced and newly founded CERTs with the involvement of multiple pertinent stakeholders. Such mechanisms provide for successful intra-regional cooperation while still incorporating the benefits of broader collaboration with outside actors for intra-regional capability development initiatives.

Third, it is important to advance the contributions of NORDEFCO and the NB8 due to the geopolitical closeness of the Nordic countries to the B3. According to the aforementioned ICDS energy geopolitics assessment study, "Nordic countries rank higher than the Continental area members in the Global Cybersecurity Index; this is also due to the prevailing culture of public-private, whole-of-society, and whole-of-government collaboration."[146] On the basis of this assessment study, a number of specific achievements of NORDEFCO and the NB8 can be recommended for improving the intra-regional cyber cooperation of the B3 states.

For example, within the memorandum of understanding of

[144] "The Largest International Live-Fire Cyber Defence Exercise in the World to be Launched Next Week," The NATO Cooperative Cyber Defence Centre of Excellence. Accessed on December 1, 2018, https://ccdcoe.org/largest-international-live-fire-cyber-defence-exercise-world-be-launched-next-week.html.

[145] "Crossed Swords Exercise," The NATO Cooperative Cyber Defence Centre of Excellence. Accessed on December 1, 2018, https://ccdcoe.org/crossed-swords-exercise.html.

[146] Hayretdin Bahşi, [..] op. cit.

NORDEFCO, the stated aim is "To strengthen the Participants' national defense, explore common synergies and facilitate efficient common solutions."[147] In such voluntary cooperation, there is more added value and less negative consequences of being tied to the other two states. The opt-out position fosters communication. This factor has to be emphasized due to previously mentioned problems of focusing too intensely on national goals and, thus, sacrificing strategic flexibility not only when it comes to procurement but also in regard to joint projects and exercises.

As indicated, for efficient cooperation, there is a necessity to have added value when enhancing the aimed robustness of regional security. The current examples have to be put into perspective in association with recommendations. Concerning the existing frameworks and organization, it has to be emphasized that although organizations are focused on international cooperation on a broader scale, they are also umbrellas for intra-regional cooperation.

Legal and Technical Structures for Crisis Management

In order to achieve common ground for crisis management, the three Baltic States must first develop common legal norms as the basis for action in times of peace and emergency. First, the necessary preconditions and steps for active communication of activities within the cyber domain need to be highlighted. Second, the legal norms to enforce cooperation and set up a common legal framework and necessary assessments for effective deterrence should be examined.

A logical cooperation framework and legal basis requires uniformity and active communication of activities carried out at the intra-

[147] Memorandum of Understanding between the Ministry of Defence of the Kingdom of Denmark and the Ministry of Defence of the Republic of Finland and the Ministry for Foreign Affairs of Iceland and the Ministry of Defence of the Kingdom of Norway and the Government of the Kingdom of Sweden on Nordic Defence Cooperation (NORDEFCO), (Helsinki, 4 November, 2009).

regional level. The recommendations aim to establish active coordination of regional legal procedures in the domain of cybersecurity while recognizing the necessity to provide actively tested end-to-end communication. Furthermore, the development of legal norms allows both the private and public sectors to have adaptive measures put in place on the basis of communication, therefore, setting up a legal framework during peacetime and crisis enhancing deterrence by denial.[148]

[148] Jeff Kossef, Jeff. "Developing Collaborative and Cohesive Cybersecurity Legal Principles." NATO CCD COE Publications, Tallinn. Accessed November 4, 2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2015%20Developing%20Collaborative%20and%20Cohesive%20Cybersecurity%20Legal%20Principles.pdf.

4.3. Expert Recommendations

1. Consider working on a common annual Baltics Cyber Security Threat Assessment report. That would allow more intense cooperation in terms of the exchange of information on the main threats, best practices, and pentesting.
2. Consider the creation of a regional task force for assessing service interdependence, which would include exchange of information, discussions on methodologies, common assessment tools, etc.
3. Develop more intensive cooperation on cyber security awareness and training as well as exercise initiatives. Different initiatives on cyber security hygiene exist in the public sectors across the Baltic States. This could also be a good topic to exchange information and share best practices on what works and what does not.
4. Coordinate exercise activities more effectively. It is suboptimal for two important cyber security exercises to happen at the same time. For example, Locked Shields 2018 occurred at the same time as the main planning conference of the Lithuanian-led multinational Amber Mist Exercise.
5. Establish cooperation through the framework of NATO COEs on cross-sectoral issues. For instance, the NATO ENSEC COE is running a project assessing cyber security risks and vulnerabilities of CEPS. However, CCD COE is not involved.
6. Achieve cooperation on cross-sectoral issues via the framework of NATO COEs, combined with regional cyber-security forums such as Lithuania's PESCO project, as a mechanism for creating a standard approach to cybersecurity issues.
7. Create a Baltic University curriculum to train a dedicated regional cadre of cyber professionals.

8. Develop a joint education platform that consists of both technical and policy academics to educate the current stakeholders in the B3.
9. Improve cyber defense training for military personnel by creating a common cyber command study curriculum for army commanders in BALTDEFCOL.
10. Emphasize the necessity for cyber crisis management structures to be clearly understood by state officials by presenting and establishing the regional security aspect in such exercises as Cyber Europe, organized by ENISA.
11. Address the gender inequalities within the field of cybersecurity by considering implementing diversity programs that can bring both competition and variety to the public and private sectors.
12. Utilize non-governmental actors such as think thanks, businesses and universities with clear aims at the intra-regional level of cooperation. This is necessary to contribute to regional security and aims established by NATO.
13. Establish a point of contact that could help coordinate and develop B3 cross-border communication autonomously from the national parties.
14. Utilize said point of contact to coordinate exercises and operations, not only within the B3 region but also with international organizations. The position can help prevent a situation of redundantly overlapping major cybersecurity exercises in the future. Moreover, established cyber domain technicalities vary in their form: for example, the three Baltic COEs separately tackle CCD, STRATCOM and ENSEC. Thus, a single point of contact would be necessary to achieve the goal of a structured approach in this sector.
15. Harmonize cyber security baseline requirements for vital services across the Baltic States.
16. Develop a common annual Baltic Cybersecurity Threat Assessment Report to increase contact and information

exchange as well as provide an assessment of cybersecurity professionals in the vital services fields.

17. Develop a proper forum to expand common understanding of intra-regional norms regarding cyberspace.
18. Ensure public sector officials actively participate in an academically oriented atmosphere, thus enhancing their understanding of the importance of cybersecurity and different threat vectors that can be used to pose a cyber threat during elections.
19. Actively document the communication of parties during elections across all domains, thus protecting them from the possibility of malicious threats to interfaces and leaks of confidential information.
20. Correspond with the private sector via end-to-end communication to conduct pentesting activities and continue monitoring election processes ahead of time, thus preparing and securing information systems before the election process has begun.
21. Have both private and public sectors communicate actively and utilize end-to-end communication with CERT professionals.
22. Educate society ahead of time, exposing the problem and possible consequences of a cyberattack, in order for any such potential incident to have less impact on public trust as to the legitimacy of elections.
23. Regarding the energy sector, continually focus on enhancing the security around TSO transmission. The aim can be achieved on the basis of CERTs having access to the communications between TSOs, thus giving the national emergency response team the capability to firstly, carry out gap filling and secondly, to direct online access to the energy sector in case of emergencies.
24. Develop the tradition of information and experience sharing by contributing to a joint end-to-end information platform capable of sharing best practices and opinions, thus fostering

CERT cooperation, best exemplified by ENISA recommendations of prioritizing mentoring activities.

25. Use EU-level incentives in regional energy security and focus on the regionality aspect of cooperation in order to achieve the most added value. As there are multiple EU-level projects and grants opening possibilities (such as the PESCO initiative), there are possibilities for cooperation and reimbursements both within the international and regional development of capabilities.
26. Emphasize the voluntary aspect of collaboration that has to be put into force with regard to cooperation within the domain of cybersecurity. Said cooperation has to be based on prioritizing the already-established obligations and understanding that there is an added value to intra-regional cooperation from cooperative projects and incentives. This approach could be guided by the example of the NORDEFCO model of regional cooperation.
27. On the basis of the takeaways from the NORDEFCO model, develop a communication base that is flexible and tailored to each country's priorities. The process of cooperation can be made more cost effective by encouraging voluntary collaboration and by treating it a basis for further bilateral and multilateral incentives.
28. Emphasize the exchange of information and best practices of both practitioners and academics regarding strategic communication via such projects as NB8.
29. Understand that establishing similar procedures in a time of crisis management as the first step toward crisis management in the cyber domain.
30. Continuously "red team" communication processes on an international scale. Moreover, ongoing pentesting directly contributes to intra-regional security. For example, cyber-defense units of the Estonian, Latvian and Lithuanian National Guards should continuously cooperate on pentesting critical infrastructure and incident response.

31. Use "cyber ranges" in coordination with the CCD COE as an incentive to carry out incident response exercises.
32. Actively contribute to cyber hygiene usage and exercises, including public presentations for state officials and active tabletop exercises like EU CYBRID 2017, organized by the European Defense Agency.
33. Rather than defining one particular cybersecurity law, work on defining broader legal norms and a basis for intra-regional threat assessments and crisis management reactions.
34. Assess areas of cybersecurity law on an empirical basis rather than case-law or different doctrines provided by international legal scholars. It is necessary to set up consultative intra-regional dialogue, between private and public stakeholders, on regulatory approaches.
35. Understand the value of lessons learned from both the Councils of Europe's Convention on Cybercrime (Budapest Convention on Cybercrime) and the CCD COE's developed Tallinn manual.
36. Base the development of regional cybersecurity norms on preconditions set out by private actors, consciously adhering to uniformity among regulations of the state, provincial and local governments."
37. When it comes to cross-sectoral issues, aim toward establishing cooperative cybersecurity laws that strengthen intra-regional cohesiveness.
38. Create a common cyber strategy with a central operations point. Widen the cyber warfare domain, technical support should include strategic communications and intelligence operations. Link cyber issues more closely to international expertise and to internal military structures.
39. Create a cyber warfare/information warfare course at BDCOL for all officer and senior non-commissioned officer ranks.

ANNEX I – Tables

Taking into account seven transportation sectors and five security risks (military, political/governmental, terrorism, cyber and economic) we developed and populated the following comparison matrix:

	Military Status and Risks	**Political/Governmental Status and Risks**
Aviation: including aircraft, air traffic control systems, and airports, heliports and landing strips	The main risk for aviation comes from the fact that the Baltic States do not control their airspace militarily, they can only observe. Some control is provided by the NATO Air Policing mission, but military means to defend the Baltic airspace is limited. No military criteria has been applied to civilian aviation structures since the collapse of the Soviet Union. The only successful military cooperation project is the BALTNET air surveillance network.	Despite NATO and EU membership, there is no common regional perspective in the Baltics for how to develop the aviation transportation area.
Highway and Motor Vehicle Carriers: encompassing roadways, bridges and tunnels	There is no or very limited military criteria applied to roads, bridges and tunnels following the collapse of Soviet Union.	Despite NATO and EU membership, there is no common regional perspective in the Baltics on how to develop the road transportation area. All countries are acting independently. Their only common project is Via Baltica, but this is also being developed separately in each country.

Cyber Threats	**Terrorism Threats**	**Economic Status and Risks**
No common regional perspective exists in the Baltics on how to develop joint resilience against cyber threats in the transport and infrastructure areas. NATO and EU policies are generic and have no regional implementation plans. NATO's Cyber Cooperation Center of Excellence is one place where military cooperation in global terms is exercised.	No common regional perspective exists in the Baltics on how to develop joint resilience against terrorist threats in the transport and infrastructure area. NATO and EU policies are generic and lack regional implementation plans.	Aviation transport is a costly, but rapidly developing business. The unilateral implementation of aviation transportation policies in each country brought about bankruptcies involving several Estonian and Lithuanian air companies.
		The best situation with highways exists in Lithuania. But again, since the Soviet collapse, no military criteria is applied to roads, bridges and tunnels throughout the region.

	Military Status and Risks	**Political/Governmental Status and Risks**
Maritime Transportation System: consisting of coastline, ports and waterways	No military criteria were applied to ports after the Soviet collapse. The Baltics have limited ability to militarily defend sea borders. Military sea surveillance has to rely on civilian sources. The only success story of maritime cooperation is the BALTRON joint de-mining squadron.	No common regional perspective exists in the Baltics on how to develop the maritime transportation area.
Mass Transit and Passenger Rail: including terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, etc.	No military criteria have been applied to infrastructure. The Russian gauge for railways defines the influence area.	The construction of Rail Baltica, the Baltic States' first joint passenger railway infrastructure, enjoys political support today. But the project could face danger if financing or a political agreement fail in any one of the participating countries.
Freight Rail: consisting of carriers, railroads, smaller railroads, freight cars, and locomotives	No military criteria have been established or applied for railways. The Russian gauge defines the Baltics' area of influence.	The construction of Rail Baltica, the Baltic States' first joint freight transportation railway infrastructure, enjoys political support today. But the project could face danger if financing or a political agreement fail in any one of the participating countries.

Cyber Threats	Terrorism Threats	Economic Status and Risks
		No common regional perspective exists in the Baltics on how to develop the maritime transportation area.
No common regional perspective exists in the Baltics on how to develop joint resilience against cyber threats in the transport and infrastructure areas. NATO and EU policies are generic and have no regional implementation plans. NATO's Cyber Cooperation Center of Excellence is one place where military cooperation in global terms is exercised.	No common regional perspective exists in the Baltics on how to develop joint resilience against terrorist threats in the transport and infrastructure area. NATO and EU policies are generic and lack regional implementation plans.	Rail Baltica is the first attempt at developing a common, cross-border, joint transportation-sector enterprise.
		Railway transport infrastructure is expensive, but is strongly emphasized by the EU as necessary for economic development. The unilateral implementation of railway transportation policy in each country makes the Baltic countries more vulnerable than if they developed it jointly.

	Military Status and Risks	**Political/Governmental Status and Risks**
Pipeline Systems	The Baltics only have limited sized gas pipeline systems that are not applicable to the military.	Only Lithuania has rejected Russian gas. Latvia and Estonia remain dependent on Russia's political good will for their gas supply. No common perspective exists in the Baltics on how to develop intra-regional pipeline networks.

Cyber Threats	**Terrorism Threats**	**Economic Status and Risks**
No common regional perspective exists in the Baltics on how to develop joint resilience against cyber threats in the transport and infrastructure areas. NATO and EU policies are generic and have no regional implementation plans. NATO's Cyber Cooperation Center of Excellence is one place where military cooperation in global terms is exercised.	No common regional perspective exists in the Baltics on how to develop joint resilience against terrorist threats in the transport and infrastructure area. NATO and EU policies are generic and lack regional implementation plans.	A joint energy security policy, especially addressing the gas supply, would improve the security situation in the region.

ANNEX II – Key Project Dates

Year 2017	
October 15	Seminar in Tallinn
October 17	Seminar in Tartu
October 19	Seminar in Vilnius
December 6	Seminar in Riga
Year 2018	
March 27	Workshop on defense and deterrence in Tartu
April 11	Workshop on societal security in Riga
April 18	Workshop on economic security in Vilnius
May 2	Workshop on defense and deterrence in Tartu
May 10	Workshop on economic security in Vilnius
May 25	Workshop on societal security in Riga
June 2	Panel at the AABS Conference at Stanford University
June 18	Participation at the IV Congress of Latvian Scientists
September 29	Panel at Riga Conference
November 14	Presentation at the Jamestown Foundation
November 23	Panel at Riga Readings in Social Sciences
December 3	Presentation at Hudson Institute
December 4	Presentation at US Congress
December 5	Presentation at the Jamestown Foundation
December 6	Presentation at New York University
December 11	Presentation at Latvian Representation at the EU
Year 2019	
January 25	Presentation at the Baltic Assembly

Author Biographies

Mr. Edmunds Āķītis works as an independent consultant and advisor on multinational Disaster Risk Reduction projects since 2008 and supports the European Commission and national governments in addressing Risk Management and Resilience issues. Mr. Āķītis was a Seconded National Expert for four years at the European Commission, DG ECHO, Emergency Response and later at the Disaster Risk Reduction Unit and has performed Policy Officer's and Liaison Officer's roles. He has organized and taken part in a dozen international response and advisory missions, mostly in Ukraine and Bhutan. Mr. Āķītis is a Fulbright scholar and earned an MSc in Homeland Security at San Diego State University, USA. He has researched resilience issues in Ukraine and internationally (EU). Mr. Āķītis has been in Crisis Management for more than 18 years and has worked in the Government of Latvia and held a leadership role as the Acting and Deputy Director of the Emergency Medical Center. Mr. Āķītis has two decorations: State Award—Chevaliers Order (Knight) and the Order of the Ministry of Defense of Latvia.

Ms. Dalia Bankauskaitė is an Adjunct Fellow at the Center for European Policy Analysis (CEPA), Washington, DC, and an associated professor at Vilnius University. Her research focus includes strategic communication, societal resilience and trust building, as well as societal mobilization and motivations. She has extensive professional experience dealing with the public and private sectors in strategic and integrated communication, and with project management in Lithuania, Ukraine, Bosnia-Herzegovina and Georgia in the field of European integration. In addition, she has diplomatic experience with the Lithuanian Embassy in Moscow. Ms. Bankauskaitė holds a Master's degree from the London School of Economics (LSE), in the UK, and an EMBA from the Baltic Management Institute (BMI), in Lithuania.

Ms. Alina Clay is currently pursuing a Master's of Science in Foreign Service at the Edmund A. Walsh School of Foreign Service at Georgetown University with the support of the Pickering Foreign Affairs Fellowship. She was a 2017–2018 Fulbright Student Researcher affiliated with the Latvian Institute of International Affairs and also taught media literacy classes across Latvia. She holds a BA from the University of Tennessee. Her research interests include Baltic security, disinformation, and societal resilience, as well as theoretical approaches to power and knowledge. She has previous work experience in non-profits, academic institutes, policy centers, and the government.

Dr. Giedrius Česnakas is an associate professor and the Director of Political Science Studies at the General Jonas Žemaitis Military Academy of Lithuania. He received his PhD in Political Science from the Vytautas Magnus University. His dissertation, "Energy Resources in Russia's Foreign Policy towards Belarus and Ukraine (2000–2012)," was awarded by the Lithuanian Research Council for the best research in the fields of social and humanitarian sciences in 2014. Dr. Česnakas initiated a yearly collection of articles, "Lithuanian Energy Security: Annual Review." His current research interests cover military security of small states and the changing contemporary international order.

Capt. (ret.) William "Bill" Combes is a Lecturer at the Baltic Defense College in Tartu, Estonia. Before moving to Estonia, Capt. Combs completed a 27-year career in the US Navy as a submariner and strategist. In addition to commanding a ballistic missile submarine, serving as Chief of Staff of a carrier strike group deployed to the Persian Gulf, and his last position as the branch head for US Navy strategy in the Pentagon, he was the US Navy's Fellow to Oxford University and the Changing Character of War Program.

Mr. Glen Grant is a defense and reform expert in Ukraine, working for the Ukrainian Institute for the Future. He is also a Senior Fellow

in the UK Institute for Statecraft on their Building Integrity Initiative countering Russian influence. Glen graduated from the Royal Military Academy Sandhurst, the Junior Staff Course Warminster and the Joint Staff Defense College at the Royal Naval College Greenwich. His key work in the last 20 years has been delivering reform and change for defense and security organizations in Europe. He has worked in the defense ministries of Ukraine, Latvia, Estonia, Bulgaria, Macedonia, Montenegro, Moldova, Poland, Albania, Kosovo, Slovenia, Serbia and Chile. As a business consultant, he has worked with telecoms, agriculture, publishing and manufacturing. During his 37-year military career, Mr. Grant commanded the UK Military Prison and an Artillery battery of eight tracked guns. He worked on the operational and policy staffs in many different British and NATO Headquarters and MOD UK. This work involved him supporting many operations, including both Gulf wars, Bosnia and Kosovo. He was Defense Attaché in Finland, Estonia and Latvia. In 2016, Glen was Project Manager in MOD Ukraine running a one-year UK-funded project "Reform of Defense Housing" and, in January 2018, published a groundbreaking paper on reform of the Ukraine military in the *Kyiv Post*. He is a skilled change manager with a Master's degree in Leadership of Innovation and Change from York St. John University, in the UK. Mr. Grant lives in Latvia and is a faculty member of the Riga Business School, lecturing on the Bachelor of Business Administration course in Strategy, HRM, Crisis Management and Entrepreneurship.

Mr. Aivar Jaeski is RB Rail A.S. Estonian branch director, and Finland-Estonia Country manager. The fast-speed, European-gauge, greenfield railway Rail Baltica is the main goal for the three Baltic countries' (Estonia, Latvia and Lithuania) joint venture RB Rail A.S. Mr. Jaeski joined the team 1.5 year ago. Previously, he served 25 years in the Estonian Defense Forces, finishing his career at the rank of colonel. His last position was as deputy director of the NATO Strategic Communication Center of Excellence. He has experience building up the Estonian Military Delegation to NATO in Brussels,

being its first deputy military representative (DEPMILREP). He also has expertise reforming NATO Joint Force Command in Brunssum. Mr. Jaeski served as a defense planner at the Estonian Defense Forces General Staff and has command experience with the Estonian Peace Operation Center (EPOC). He was a builder and first commanding officer of a logistics battalion in the Estonian Defense Forces. Aivar Jaeski has mission experience from ISAF Afghanistan and Iraq, where he worked at the NATO Training Mission in Iraq as Deputy Chief of Staff on Support Matters. Besides his military education, Aivar earned a civilian degree in logistical engineering.

Dr. Tadas Jakštas is an Energy Security Expert at the NATO Energy Security Center of Excellence (NATO ENSEC COE). He was appointed NATO Civilian Expert on energy security in the Baltic Sea Region. His main expertise is on kinetic and non-kinetic threats to energy supplies, the protection of critical energy infrastructure, and resilience. Before joining NATO ENSEC COE, Dr. Jakštas worked at NATO Allied Command Transformation and the Council of the European Union, where he focused on cyber security and defense policy issues. He holds a PhD in Government from the University of Essex and two postgraduate degrees in International Relations and Security Studies from Leiden University and the University of Southampton.

Dr. Ivo Juurvee as part of the ICDS team, focuses on security and resilience—i.e., the countermeasures applicable to the wide variety of threats to Estonia and more widely to NATO and the EU. These include: intelligence/counterintelligence, terrorism/counter-terrorism, information warfare/psychological defense, and other means of non-conventional foreign pressure as well as the national resilience required to cope with them. Prior to joining ICDS, he worked as the head of the Internal Security Institute of the Estonian Academy of Security Sciences (EASS). Ivo has also taught security-related topics at the University of Tartu, the NATO School at

Oberammergau and in the FRONTEX Master's program on border management.

Mr. Vytautas Keršanskas is the Deputy Director of the Eastern European Studies Center (EESC). Mr. Keršanskas has worked at EESC since 2013, he is also an associate of Lithuanian national radio *LRT*. Prior to EESC, Mr. Keršanskas worked at the Ministry of Foreign Affairs of Lithuania, he was also a foreign policy observer at the weekly journal *Veidas*. Mr. Keršanskas holds a BA and an MA from IIRPS VU. His scholarly interests include foreign and security policy of Lithuania and Eastern Europe, information wars and propaganda, the development and European integration of the Eastern Partnership countries, as well as domestic and foreign policy of Russia.

Dr. Didzis Kļaviņš is a Senior Researcher at the University of Latvia, Faculty of Social Sciences and Advanced Social and Political Research Institute. Dr. Kļaviņš obtained a PhD in International Politics at the University of Latvia (thesis title: "Transformation of the Foreign Ministries in the Baltic and Scandinavian Countries, 2004–2012"). He holds the Europaeum's MA in European History and Civilization, jointly offered by Leiden University, Université Paris I–Panthéon–Sorbonne, and the University of Oxford. Dr. Kļaviņš also holds an MA in Political Science from the University of Latvia. He has also studied at Uppsala University, the University of Oslo, and the University of Wisconsin–Eau Claire. For several years, Dr. Kļaviņš worked at the Ministry of Foreign Affairs of the Republic of Latvia.

Mr. Anthony Lawrence is Head of the Defense Policy and Strategy Program at the International Center for Defense and Security, in Tallinn. His major projects have included chairing a multidisciplinary study of options for the future of NATO's Baltic Air Policing mission, supporting Estonia's EU Presidency with a study of military capability development for the EU's Global Strategy, and managing a study on air-defense requirements for the Baltic States. Between 2005 and 2013,

Mr. Lawrence was also an Assistant Professor at the Baltic Defense College, responsible for the design and delivery of around 50 percent of the annual Higher Command Studies Course. He spent the first half of his career as a civil servant in the UK Ministry of Defense, including appointments in scientific research and procurement, and policy positions dealing with NATO issues, operational policy in the Balkans, the CSDP, and ballistic missile defense.

Col. (ret.) Vaidotas Malinionis is the director of the National Defence Foundation (NDF), a non-profit organization dealing with processes and projects that contribute to the security of the Baltic Region. Col. Malinionis specializes in defense and security affairs in the Baltic Region, and he provides expertise on defense and security matters for local media, politicians and other organizations. Col. Malinionis has written extensively on security and defense issues and published articles in local media outlets *Delfi*, *Alfa* and other publishers. He served in the Lithuanian Armed Forces from 1991 to 2014, and retired with a rank of Colonel. He is fluent in English, Russian and proficient in Polish; his native language is Lithuanian. Col. Malinionis received a Master's degree from the Lithuanian University of Agriculture (1995), graduated from the Lithuanian Military Academy (1997), and participated in the Command and General Staff College's (USA) Command and General Staff Course (2003) as well as the Naval War College (USA)'s Naval Command Course (2012).

Ms. Ieva Miļūna is a Lecturer in International Law at the Riga Graduate School of Law. She also serves as a Government Advisor to the Latvian Ministry of Foreign Affairs. Her main fields of expertise are international and European law, peace and security, rule of law, and law of armed conflict. Ms. Miļūna's professional activity has been related to the Fordham Law School and the University of Amsterdam. She has chaired the EU Council Working Group on the International Criminal Court (COJUR-ICC) during the Latvian Presidency in the

EU. Recently, she joined the European Centre of Excellence on Countering Hybrid Threats as a Legal Expert.

Dr. Arunas Molis works as a professor at the Vytautas Magnus (Kaunas, Lithuania) and Bologna (Italy) universities, where he teaches courses on security and international relations. He is also Klaipeda LNG Terminal director at "Klaipedos nafta," a company that operates the only LNG terminal in the Baltic States. Since 2014, Dr. Molis worked for four years as an advisor to the President of the Republic of Lithuania at the economic and social affairs group, where he was responsible for energy and communication affairs. Dr. Molis joined the team of advisors after successful work at the NATO Energy Security Center of Excellence, where he managed research projects aimed at raising energy awareness among military personnel. He completed his international relations and business law studies at Vilnius, Vytautas Magnus (Kaunas) and Bremen universities, and he has been working on various projects in Estonia, Germany, the Czech Republic, France and South Korea.

Mr. Olevs Nikers is a senior analyst at The Jamestown Foundation and a member of the Association for Advancement of Baltic Studies. A Fulbright alumnus, Mr. Nikes earned his Master's degree in International Affairs at the Bush School of Government and Public Service, Texas A&M University, in 2016. He graduated from the Baltic Defense College Civil Servants Course, in 2003, as well as the University of Latvia in Political Science, in 2001. He is an army and defense professional since 2001. From 2009 to 2010, he was the chairman of the international affairs and security policy think tank for the political party "Jaunais Laiks" (New Era). Mr. Nikers was a recipient of the Transatlantic Fellowship Program of The World Affairs Institute, in 2018. He is Director of the Baltic Security Strategy Project and a PhD student at the Riga Stradins University.

Dr. Žaneta Ozoliņa is a Professor of International Relations in the Department of Political Science, University of Latvia. Her research

interests focus on European integration, Transatlantic security, regional cooperation in the Baltic Sea Region, as well as foreign and security policy of the Baltic States. Dr. Ozoliņa is the author of more than 90 scholarly articles and editor of several books, including *Latvia-Russia-X* (2007), *Rethinking Security* (2010), *Gender and Human Security: A View from the Baltic Sea Region* (2015), and *Societal Security: Inclusion-Exclusion Dilemma. A portrait of the Russian-Speaking Community in Latvia* (2016). She is a member of the editorial boards of several journals, such as the *Journal of Baltic Studies*, *Defense Strategic Communications*, and the *Lithuanian Annual Strategic Review*, and is editor-in-chief of the journal *Latvijas Intereses Eiropas Savienībā* (*Latvian Interests in the European Union*). She was a chairwoman of the Strategic Analysis Commission under the Auspices of the President of Latvia (2004–2008) and a member of the European Research Area Board (European Commission) (2008–2012). She was engaged in different international projects commissioned by the European Parliament, the European Commission, NATO and other international bodies. She chairs the Foreign Affairs Council of the Latvian Ministry of Foreign Affairs and is a member of the European Council of Foreign Affairs (ECFR) and the Baltic Development Forum.

Ms. Piret Pernik is a Researcher in Cyber Security at the Estonian Academy of Security Sciences, Tallinn, Estonia. Between 2013 and 2018, she worked at the International Centre for Defence and Security (ICDS), Tallinn, as a Research Fellow in Cyber Security. During that time, she published extensively on cybersecurity, and comprehensive security and defense issues. Before joining ICDS, she was an advisor to the National Defense Committee of the Estonian Parliament. Before that, she worked from 2003 at the Ministry of Defense on defense policy planning issues.

Mr. Edgars Poga studied Law and Diplomacy at the Riga Graduate School of Law and is a specialist in cybersecurity. His experience

includes Research Lecturer at the National Defense Academy of Latvia, participation in the European Youth Parliament, as well as traineeships at the Ministry of Defense of Latvia and the Permanent Delegation of Latvia to NATO. His research covers Latvian cyber resiliency and Baltic challenges in developing a common cyber defense.

Ms. Anne-Ly Reimaa is Head of International Relations on Integration Issues at the Cultural Diversity Department of the Ministry of Culture of Estonia. She has been engaged in societal security issues since 2007 and has been the leading official (Undersecretary) in the sphere of Estonia's Integration Policy between 2007 and 2016. She conducted a compilation of the current Integration Strategy "Integrating Estonia 2020," which formulates the forthcoming seven-year objectives of the integration policy of the Republic of Estonia and the activities needed to achieve them. The general objective of the country's integration policy is to increase social cohesion and ensure the social inclusion of people with different linguistic and cultural backgrounds. Ms. Reimaa is also responsible for creating conditions for the development of cultures of minority and Finno-Ugric kindred populations living in Estonia. Moreover, she coordinates the cultural life and activities of compatriots living outside Estonia. Ms. Reimaa holds a Master's degree from the University of Tartu. She has been engaged in different international projects, including in Moldova.

Mr. Jako Reinaste serves as Manager of Energy Markets in the Energy Market Division, at the Estonian Ministry of Economic Affairs and Communications.

Mr. Ēriks Kristiāns Selga is a PhD candidate in the University of Hong Kong, where he is studying the interaction between legal frameworks and innovation. Among his interests are foreign policy,

in particular, issues of defense and state collaboration, and human rights.

Col. (ret.) Dr. hab. Zdzisław Śliwa is the Dean of the Baltic Defense College in Tartu, Estonia, as well as a visiting professor at the Latvian Defense Academy in Riga. He completed his education at, among others the Polish National Defense University, in Warsaw; the US Army Command and General Staff College, in Fort Leavenworth, Kansas, USA; and also in the Center of Strategic Studies of the People's Liberation Army National Defense University, Beijing, China. During his military service, he served as the Chief of the Operational Branch J-3 in KFOR Headquarter, in Kosovo, and also as the Chief of Operational Planning Branch J-5, at the Polish Armed Forces Operational Command in Warsaw. When working for Polish military educational institutions, he was the Chief of Combat Service Support Chair, Mechanized Forces Military Academy in Wrocław and also the Head of the Military Studies Branch, at the National Defense University, in Warsaw. He has published books and papers related to current developments in Asia and Europe, especially in relation to the security dimension.

Mr. Romas Švedas worked for 20 years as a civil servant, and from 2011 he has been an Independent Expert, Professional Board Member and Lecturer at the Institute of International Relations and Political Science at Vilnius University. He is a former Vice-Minister of Energy of the Republic of Lithuania (2009–2011), Director of the Economic Security Policy Department (2007–2009) and Economic Relations Department (1999–2003) at the Ministry of Foreign Affairs, former Deputy Permanent Representative of Lithuania in the European Union in Brussels (2003–2007) and Counselor at Lithuania's Permanent Mission to the United Nations Office and other International Organizations in Geneva (1995–1999).

Mr. Otto Tabuns is a visiting lecturer at the Riga Graduate School of Law and co-host of the *Latvia Weekly* current affairs podcast. He has previous experience in strategic communication and defense planning. Mr. Tabuns is an author of articles on Latvian and European security in fields such as regional military cooperation and societal security. He is the Executive Director of the Baltic Security Strategy Project, a member of the Latvian Association of Political Scientists, Latvian Japan Alumni Association, and the Association for Advancement of Baltic Studies.

Mr. Gunārs Valdmanis is an executive director of the Latvian Association of Power Engineers and Energy Constructors, a non-governmental organization representing the largest companies in the Latvian power sector, with total turnover annual exceeding 1.5 billion euros and including the transmission grid operator JSC Augstsprieguma Tīkls, the distribution system operator JSC, as well as the largest power producer of the Baltic region, JSC Latvenergo. Previously, Mr. Valdmanis worked as the Deputy Director of the Department of Energy Markets and Infrastructure in the Ministry of Economy of Latvia. His earlier professional experience also involves several years of journalism work, as well as in management in the information service and transport sectors. Mr. Valdmanis earned a Master's degree in Political Science at the University of Latvia, as well as a Master's degree in environmental science and energy at the Riga Technical University and the Vilnius Gediminas Technical University. Currently, he is pursuing doctoral studies in energy and the environment at Riga Technical University.

Dr. Viljar Veebel is researcher in the Department of Political and Strategic Studies, at the Baltic Defence College. He holds a BA in International Relations from the University of Tartu, an MA in International relations from the University of Tartu ("Spill-over barrier in European integration process") and a PhD in political science from the University of Tartu. He has worked as an academic

advisor of the Estonian government in the European Future Convention and as a researcher for several research institutions, including the OSCE, SIDA, the European Council on Foreign Relations, the Estonian Foreign Policy Institute, the Latvian Institute of International Affairs, and Eurasia Group. He lectured at the University of Tartu, the Estonian National Defense College, the Ukrainian Diplomatic Academy, the OSCE Border Management Staff College and the Estonian Diplomatic Academy.

Ms. Rasa Zdanevičiūtė is a Legal and Policy Officer at the Ministry of Culture of the Republic of Lithuania, specializing in Media Law.

Ms. Laima Zlatkutė is Advisor for Defense Policy Department, in the Ministry of National Defense of the Republic of Lithuania.