Baltic Interoperability Report

Edited by Olevs Nikers & Otto Tabuns

Baltic Security Strategy Project

2019

The JAMESTOWN
FOUNDATION

BALTIC INTEROPERABILITY REPORT

Olevs Nikers and **Otto Tabuns,** *Editors*

BALTIC SECURITY STRATEGY PROJECT

The JAMESTOWN
FOUNDATION

Washington, DC
March 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.

The views expressed in this report are those of the contributors and not necessarily those of The Jamestown Foundation or any other organization or government.

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

Front cover image credit: Lithuania in NATO Twitter.

ISBN: 978-0-9986660-6-8

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

The Baltic Interoperability Report is the first publication of the Baltic Security Strategy Project (BSSP), the largest independent security study in Estonia, Latvia and Lithuania.

These countries, the Baltic States, celebrated one hundred years of statehood in 2018. Their independence was interrupted by a world war and three occupations. However, they regained their freedom in 1990 and returned to the West, becoming members of the North Atlantic Treaty Organization (NATO) in 2004.

NATO defines interoperability as "the ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives." Additionally, the term is understood as "the capability to communicate, execute programs or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units." This explanation, given by the Official NATO Term database, has been commonly agreed upon and therefore serves as a point of reference for the defense planning of each of the Baltic States, as well as other NATO states.

For Estonia, Latvia and Lithuania, which are challenged by variations in regional stability and security over the years, enhanced military interoperability has been and still is a realistic solution to many of the most pressing security threats of the day.

Over the last year, a team of experts led by Olevs Nikers and Otto Tabuns has researched and drafted a report based on a series of commissioned articles and discussions between Baltic and American security experts and key stakeholders. The core of this expert research outlines modern interoperability challenges for Estonia, Latvia and Lithuania in developing common ground forces, air and cyber defense approaches, as well as jointly meeting hybrid warfare threats. This is put in the context of the history of interoperability between 1918 and 1940, when the Baltics established their independence. The research concludes with a long-term outlook on possible scenarios of interoperability development by 2030.

The main objective of this report is to prioritize Baltic interoperability issues from a transatlantic perspective with input from US and European policymakers and defense-sector professionals. Additionally, the resulting discussion will outline questions in need of further research.

History of Baltic Interoperability Issues (1918–1940)

Otto Tabuns

The three Baltic States were established as independent republics a century ago. Estonia and Lithuania proclaimed their independence in February 1918, while Latvia followed suit the following November. All three were among the parts of the Russian Empire that were occupied by the German Empire during World War I. Russia was in turmoil following the renouncement of the throne by the Tsar in February 1917, and the Bolsheviks overthrew the Provisional Government in November that same year. Meanwhile, Germany signed an armistice, and the Kaiser was overthrown that same month.

Previously, Estonia and northern Latvia were ruled by Sweden until the Great Northern War of 1700–1721. Eastern Latvia was controlled directly by Poland until its Second Partition in 1772. Western Latvia had been a Polish vassal formed by the German crusaders after the eradication of the Livonian Order in 1558. It was taken over by Russia after the Third Partition of Poland in 1795. The Holy Roman Empire (through the Livonian Order) and the Roman Catholic Church shared Estonia and Latvia after the two were conquered by Crusaders during the 13th century. In contrast, Lithuania kept its independence despite the Crusaders by converting to Christianity. In 1569, Lithuania and Poland established a Commonwealth.

Wars of Independence 1918–1920

The independence of the Baltic States, proclaimed in 1918, was immediately contested and led to wars of independence. All three states had to fight against Soviet Armed Forces (the Red Army) all the way until 1920. In 1919, the Baltic German Armed Forces (the Landeswehr) in Latvia broke their alliance with the temporary government of Latvia, however they were defeated by the Latvians and Estonians in a common effort. After the defeat of the Landeswehr, Latvia remained together until former soldiers of Imperial Russia and German troops led by Bermont waged war against Latvia and Lithuania. Parallel to this, the Polish-Soviet War took place between 1919 and 1921. This period saw both Polish-Latvian cooperation in dealing with the Red Army in Daugavpils and the Polish-Lithuanian conflict over possession of Vilnius.

Cooperation was inhibited by border claims. Soviet Russia recognized Lithuania’s claim to Vilnius. Latvia’s claim to what is now the Eastern part of the country was contested by both Lithuania and Poland. Estonian assistance to Latvia during its War of Independence and the decision of an international border commission led to several contested parishes, as well as Ruhnu Island, being recognized as Estonian. Estonian, Latvian and Polish claims vis-à-vis Soviet Russia gave grounds for talks of an alliance. However, Estonia and Latvia signed separate agreements once areas populated by mostly titular nations of their respective states were conquered from the Red Army.

Infrastructure

All three countries inherited a railway system mostly in the Russian five-foot gauge system. There were two standard (European) gauge (4 feet, 8.5 inches) tracks connecting Eastern Prussia to Riga, crossing cities such as Kaunas and Jelgava on the way, and Riga to Liepāja via Mažeikiai. However, the standard gauge system stopped at the Western bank of the Daugava River, disallowing any European railcars to use the railway across the river toward Russia. This was a design similar to the Warsaw rail configuration, preventing a surprise attack and fast progress on the key transit system.

The rail system interoperability, however, was useful in the Latvian and Estonian common military effort in 1919, when Estonia sent two armored trains to assist Latvian armed forces against the Russian and German troops led by Bermont. It was also useful for the Polish and Latvian common effort in the Battle of Daugavpils in August 1920. The city of Daugavpils is situated at the junction of the St. Petersburg–Warsaw, Moscow–Ventspils and Riga–Orel rail lines, which allowed both countries to move 40,000 troops, provisions, ammunition, and tanks across terrain mostly covered by hills and lakes.

Since the demobilization that followed the War of Independence in 1920, Latvian mobilization plans had a number of premises that took into account the realities of geography and transport infrastructure. In regard to a possible war with the Soviet Union, it was assumed that the Eastern part of Latvia was not suitable for spatially extensive warfare. In contrast to Western forests and Southern plains, the East of Latvia is covered in hills and hundreds of lakes up to 80 square kilometers wide and many between 100 and 200 feet deep. Therefore, the Soviet Union could be expected to use the few narrow axises of railway to provide communication and logistics.
[1] The Eastern part of Latvia was crossed by the Leningrad-Warsaw, Moscow-Ventspils, Riga-Oryol and Riga-Pskov lines, all being Russian gauge single track lines connected directly to Soviet Russia at three points with the exception of the Riga-Pskov line that had to cross Estonia via Tartu. Thus, Latvian armed forces could defend themselves in three to four narrow stretches on the front line until mobilization was completed.

In regard to communications, the Baltic States were crossed by two international telegraph cables (out of five that connected Russia to the world), and the only one (St. Petersburg–Tallinn–Riga–Liepāja) that traversed neutral waters went through the Baltic Sea and Sweden on its way to London, instead of going through Germany, Romania, Turkey, Persia or China. Using the existing infrastructure, and establishing a new, undersea cable between Estonia and Finland, both Estonia and Latvia could rapidly exchange unclassified and classified security information between themselves as well as with Finland.[2]

[1] Hugo Rozenšteins, *Latvijas kara ģeogrāfija* (Rīga: 1932), 15.

[2] Rene Niberg, *The Last Train to Moscow* (Rīga: Jumava, 2017).

Lack of a local coal and oil industry made energy supply and military logistics dependent on foreign imports. Firewood, peat and oil shale (in Estonia) dominated the market and electricity networks were isolated to cities up until the construction of the first national grids in the late 1930s (e.g. after building a hydroelectric power plant in Latvia). Although with the beginning of World War II and the following closure of overland transit the option of international waters in the Baltic Sea seemed a safe haven, the tanker with petrol procured by Latvia in 1939 was stopped in Sweden and prevented from crossing the sea due to "security reasons" and its contents were confiscated. Whereas reserve electricity capacities were provided for in case of crisis (e.g., a secret, fortified power plant in Riga), no fuel reserves were prepared, limiting both the extent of military exercises and combat mobility. No cooperation was undertaken in this direction.

Land Forces

The inception of land forces in the Baltic States stems from the permission to draft national units in the Imperial Russian Armed Forces. Permission was granted due to the grave situation at the front line, thus allowing territorial instead of political mobilization of troops.

Established in 1919, the Estonian Armed Forces fought off the invasion of the Red Army with the help of British arms, as well as support of the Royal Navy and Scandinavian volunteers. To begin with, armored vehicles were based on the American and French chassis. Later, after initial help in repairs from the British military mission, the armor was produced in the workshops at Tallinn Port using ship steel.[3] In its early days, the Estonian Army managed to retrieve many Soviet armored vehicles. As a result, in 1920, the force was complemented by 12 Renault tanks. Following the Great Depression, due to cost savings, Estonia began to invest in Polish light tanks, which were cheaper, faster and better adjusted to marshy, swampy grounds. However, a debt to Great Britain over submarine procurement prevented Estonia from further investment in the direction of armored vehicles.[4]

The Latvian Armed Forces were also established in 1919. British, French and Polish rifles, ammunition and armored vehicles provided the initial technical basis for the Latvian Army. Artillery, though abundant, included Russian, German, English and French systems of different calibers, making training, operation and supply difficult. Armored vehicles were complemented by armored trains, noting the comparatively extensive railroad network to limited and damaged roads. Latvia concluded the War of Independence in 1920 with 75,000 troops, decreasing the amount to 30,000 by 1940. Mandatory military service, initially between 10 and 12 months, was extended to 18 months in 1940.

The Lithuanian Armed Forces were established in 1918. After fighting the Bolsheviks, White Russian

[3] Marģers Esserts, *Bruņutehnika Baltijā 1915-1940* (Rīga: Zvaigzne ABC, 2018), 72.

[4] Ibid, 93.

Army, former Imperial German troops and Poland, in 1921 the Lithuanian Army consisted of 20,000 troops. At first, armored vehicles included a Fiat taken from Soviet troops and Daimler cars given by Allied troops to help the evacuation of former Imperial troops led by Bermonts.[5] Later in the 1920s, Lithuania bought Renault tanks. Following a military coup in 1926, renewed investment and modernization of the army began only in 1935 in response to changes in German foreign policy. This resulted in buying Swedish and British armored cars.

The procurement of armored vehicles and tanks was largely influenced by Allied pressure and the needs of the Baltic States to gain British and French support for their recognition and inclusion in international trade. The concept of interoperability in the sense of shared technology, upkeep and ammunition was not seriously entertained by Baltic leaders, especially once governed by authoritarian rule and the ideas of nationalism and autarchy. This was illustrated most sharply in the late 1930s, when the Latvian Armed Forces were severely limited in performing live fire exercises due to a deficiency of ammunition, thus inhibiting the firing skills, the actual battle preparedness and the morale of the troops who could observe the situation.[6]

Naval Forces and Coastal Defense

Coastal defense was a more relevant issue for Estonia and Latvia than Lithuania, having at least 300 miles of coastline each. World War I actually saw its first hostilities when Imperial German ships bombarded the Imperial Russian military installation in Liepāja, a key naval fortress by the border.

For Estonia, a significant challenge was presented by more than a thousand islands to the west and north of the mainland. This was effectively used by Imperial German troops during Operation Albion in 1917 when executing a surprise landing and taking over control of Estonia in four to eight days, with the help of blimps and gliders. With Estonia controlled by an unfriendly government, it would be easy to cut off access to the Gulf of Riga and the Baltic Sea. Therefore, a wholesome defense of the capital of Latvia, creating both military and economic consequences, would have been impossible without Latvian-Estonian cooperation.[7]

The Estonian Naval Forces were established in 1918. British help was instrumental in the establishment of the Estonian Navy, starting with giving captured Russian vessels to form the first units of the navy. One key element in the defense of Estonia was the coastal defenses, going back to the end of the Great Northern War in 1721. The importance was partially in the capability to safeguard and/or close the Finnish Bay on the way to St. Petersburg.

[5] Ibid, 94.

[6] Valdis Kuzmins, "Latvijas bruņoto spēku mobilizācijas plāni 1939.-1940.gadā", *Militārais apskats* Nr. 3/4 (132–133)(2009): 49.

[7] Latvian forces included one submarine.

This strategic aspect laid the foundation for Finnish-Estonian cooperation, as together their batteries around Tallinn and Helsinki could effectively close the gap to any naval traffic, affecting themselves as well as Russia, Sweden and Germany during a potential conflict. This might have been a key motivation for Germany offering a secret military alliance to Estonia in 1937.[8] Estonian and Finnish coastal artilleries had a common fire management system linked by an undersea radio cable. Furthermore, Estonia bought two British-made submarines and used the same torpedoes and mines as the Finnish navy, which led to Estonian personnel training in Finland and holding common war games starting in 1937.

The Latvian Naval Forces were established in 1919 and, owing to Latvian ports being among the top five trade ports for the Russian Empire, many private trade steamers and tugboats formed the initial force. It included mobile coastal artillery, submarines, naval aircraft, and light high-speed vessels armed with torpedoes and light cannons. Compared to its land and air component, the Latvian Navy was the most expensive structure of the Latvian Armed Forces.[9] The Daugava River, bisecting Latvia and flowing through the two largest cities, Riga and Daugavpils, was navigable for most of the national territory. Issues connected to its cross-border navigability by representatives of organized crime and foreign intelligence were slightly limited in 1939, when the first hydroelectric power plant was built 40 miles upstream from Riga.

Meanwhile, German-controlled (East Prussia) Memel/Klaipēda and Latvian-controlled Palanga left Lithuania without access to the Baltic Sea in 1918. In 1921, Palanga was exchanged for Aknīste in what is now southeastern Latvia. Klaipēda, detached from Germany in 1919 and made a protectorate of the Entente, was taken over by Lithuanian troops in 1923. Despite already buying a minesweeper for the defense of Klaipēda, the Lithuanian Naval Forces were established only in 1935. This might be explained by the political changes in Germany and the remilitarization of the Ruhr region, with Lithuania fearing the activation of German claims to the Klaipēda region. At the time, the region carried three-fourths of Lithuanian foreign trade and held one-third of the country's industry. In 1939, once Germany occupied Klaipēda, the Lithuanian Navy was forced to leave for Latvia.

Air Forces

The aerial domain, similar to cyber currently, was brand new at the time. The first air force was established in 1911. And that same year witnessed the first incident of aerial warfare, which an Italian plane conducted aerial reconnaissance over Libya. But World War I became the first conflict in which air forces were used extensively.

[8] Jari Leskinen, "Suomen ja Viron salainen sotilaallinen yhteistyö Neuvostoliiton hyökkäyksen varalta 1930-luvulla" (in Finnish) In *Talvisodan pikkujättiläinen*, ed. Jari Leskinen and Antii Juutilainen. (Helsinki: Werner Söderström Osakeyhtiö, 1999) 127.

[9] "History of the Navy" (in Latvian), National Armed Forces of the Republic of Latvia, accessed November 2, 2018, http://www.mil.lv/lv/Vienibas/Flotile/Par_juras_spekiem/Kara_flotes_vesture.aspx.

The Estonian Air Force was established in 1918 and saw some of its first action supporting Latvia's War of Independence in the latter country's north. Three important airfields around Tallinn, Rakvere and Tartu served as the main points of deployment for forces. The 80 foreign-made airplanes included mostly British and French models as well as a Soviet plane captured in 1920. Estonian geography, dominated by the seaside, including Tallinn being situated on a peninsula, prioritized seaplanes and kept them in balance with other types of aircraft.

The Latvian Air Force was established in 1919. Four airfields were situated in and around the capital, while four others were located in Gulbene, Krustpils, Liepāja and Usma, the latter two operating with naval airplanes. The 131 aircraft imported between 1923 and 1938 included mostly British, French and Italian fighter planes, as well as Czech, Belgian and British reconnaissance planes, with some Swedish and Finnish hydroplanes. In the late 1930s, the skills of Latvian designers and the capabilities of the State Electrotechnical Factory (VEF) permitted Latvia to begin producing locally designed airplanes domestically.

The Lithuanian Air Force was also established in 1919. Beginning with a British plane retrieved from Soviet forces, first planes were bought from Germany and some were designed and produced locally, totaling 123 aircraft. Main airbases were situated in Kaunas, Šiauliai and Paņevežis, while Palanga and Rukla were used seasonally.

Although the common procurement and usage of British planes would have given cooperation opportunities for Estonia and Latvia in regard to research and development as well as exercise and repair, the physical distance between the Baltic States and Britain prevented the delivery of British aircraft ordered in 1939 due to World War II breaking out. This was similar to Germany not allowing armored vehicles bought from Britain or the Czech Republic through, even going as far as repaying their value, but still not letting the Baltic States strengthen their military capabilities.

The failure to procure the 30 British Hawker Hurricanes was an important motivator for Latvia to establish and speed up national aircraft development and production. Between September 1939 and June 1940, five exercise fighters and 12 bombers were produced and taken into active duty.

Lithuanian domestic efforts in developing and producing domestic aircraft was motivated by limited access to sea. Therefore, the air force did not evolve as an arm of the naval forces like in Great Britain or in close connection with coastal defense as in Estonia. So there was no competition or redistribution of resources.

Even here, interoperability in the form of key procurement partners was biased by threat perception at the foreign policy level. Lithuanian experience and perception of Poland, and less so of Russia, was crucial in cooperation with Germany, in contrast to Estonian and Latvian cooperation with, mostly, the British.

Other Features

The Baltic States had the top literacy rates in the Russian Empire, and many Estonians, Latvians and Lithuanians were well-versed in Russian, the language of administration and education (since 1885, printing in everything except religious education in Lithuanian and Latvian in East Latvia was prohibited), as well as German or Polish (language of many landlords). This, combined with a lack of knowledge of Baltic languages on the other side, gave a strategic advantage in understanding decrypted communications without delay. This served the Finnish army very well, for the same reasons, during its wars with the Soviet Union.[10]

Meanwhile, the interconnections of extensive Baltic minorities in Russia, soldiers of Baltic extraction in Russian military formations (including the Red Riflemen) and family ties created serious drawbacks. The Museum of Occupation found evidence of many high-ranking Latvian army officers being agents of Soviet intelligence as far back as the 1920s and early 1930s. Therefore, it also raises the question of how those interconnections affected threat assessments and foreign and security policy considerations, including intra-regional cooperation. For example, in contrast to Lithuania, four out of the first five peacetime mobilization plans showed Germany as a primary threat to Latvia. This could partly be explained by German ethnic policy in the context of a sizeable community of Germans in Latvia (i.e. a possible German intervention, as illustrated by German actions in Ruhr, Austria, Czechoslovakia). The situation did change after repatriation of Baltic Germans to Germany. Simultaneously, the Soviets abstained from aggression up until the Winter War, in November 1939, making it easier to accept Soviet bases and troops on Baltic territory as part of "collective security measures" in October.

Latvia and Estonia saw Germany and the Soviet Union as their primary threats. This was illustrated by their mobilization plans. Whereas, Lithuania viewed Poland as its primary threat, thus seeking cooperation with Germany and the Soviet Union to contain Poland. As a result, Estonia and Latvia cooperated only among themselves. Lithuania joined them in forming a Baltic Entente once Poland concluded non-aggression pacts with the Soviet Union and Germany, preventing Lithuania from military cooperation with either Berlin or Moscow in case of a renewed conflict with Warsaw. So, it took 16 years after proclaiming statehood for the Baltic States to conclude their first common subregional cooperation framework.

Although Lithuania did not perceive Germany as a principal threat up until the late 1930s, Latvia did. Their mobilization plans included an option for a response in case of German invasion of Lithuania. Latvia and Lithuania had no defensive fortifications between them. This was used by the Soviet Union in 1940, when much of the armed forces tasked with military occupation entered Latvia through Lithuania, rather than crossing the Latvian-Soviet border in the East.

[10] Juka Rislaki, Kur beidzas varavīksne (in Latvian) (Rīga: Jumava, 2004).

Conclusions

Many givens, though not always utilized, provided cornerstones for effective military interoperability between the Baltic States. The key weakness was the elementary lack of information exchange. Mobilization plans considered both threats from the Eastern and the Southwestern flanks and were prioritized according to the current threat perception. Any changes would take at least six months to prepare, exercise, and implement. Thus, German aggression followed by Soviet pressure led to chaos in the defense planning in Latvia and the other two Baltic states. Estonia accepted the German ultimatum without even informing Latvia or Lithuania. Whereas, the Latvian Armed Forces were more combat-capable in June 1940 than in September 1939, the Soviet Army's presence in Lithuania made the premises of Latvian mobilization plans useless.

Individually, the independence of the Baltic States was not sustainable, especially considering the use or threats to use overwhelming military force on two fronts. Despite the nominal changes in state actors, and the adjusted Polish and German borders in what is now western Belarus and Kaliningrad, the source regions of military forces not allied with the Baltic States stayed the same as in 1940. In this regard, the interoperability of the rail system throughout the Baltic States, Belarus, Kaliningrad and the rest of Russia is today a double-edged sword, just as it was then.

Separately, the countries spent more resources on defense than today. For example, Latvia spent 25 percent of its budget on defense in 1939[11] compared to 5.7 percent in 2017.[12] Yet, by 1940, even that was not enough to give confidence. Common planning, procurement and upkeep opportunities, even when already using the same equipment (e.g. Renault tanks), were ignored due to political considerations of narrow interest groups becoming more important than overall national security interests. Therefore, the key lesson of needing better interoperability goes both in promoting smart defense by sharing costs, as well as instilling greater confidence by the effect of scale given by forces with high interoperability.

[11] *Statistical Yearbook of Latvia*, (in Latvian) (Rīga: Valsts statistiskā pārvalde, 1939).

[12] "How many cents each sector receives from each euro paid in taxes" (in Latvian), Latvijas Avīze, December 15, 2017, http://www.la.lv/infografika-cik-centu-sanem-nozares-no-katra-nodoklos-nomaksata-eiro.

Interoperability Challenges for Meeting Hybrid Warfare and Ground Force Threats

Glen Grant

Introduction

This article will address the challenges of Baltic military interoperability in a hybrid and conventional war context—in short, the ability of the three states to fight together. Whilst the nations do exercises together and also work closely with the integrated North Atlantic Treaty Organization (NATO) reinforcements, doing so in a crisis is a whole new ball game with many more critical considerations than just simply working together.[1] Interoperability must be looked at as coherence both in terms of political agreements and for the capability of the multinational military groupings to deliver force as a working team.

Many questions arise from this issue: Is it possible at all to have military interoperability between states with totally different security concepts? Do decision-makers understand what it means to fight seriously? Is there the political will to send troops to another country? And who can and will give the orders? It is clear that NATO interoperability training has been highly effective at the tactical level. English is now spoken widely at least by commanders and in this regard the three Baltic States stand out as NATO leaders. Also, the technical ability to work alongside others grows daily as exercises and relationships improve. But arguably this is not the biggest challenge. That challenge is how the nations will respond to an attack of any sort in those critical hours and perhaps days before NATO is fully engaged. Thus, the paper concentrates less upon developing the military capability of interoperability and more upon the question of vital political will to deliver with, and for, Baltic allies in a crisis**.**

The paper will split the work into four parts. First, the scene will be set by looking at the geopolitical environment. Second and third, the paper will look at the possible challenges of hybrid and conventional warfare. Lastly, the paper will argue how interoperability is affected by national cultures and history that will drive, or more likely hinder, rational decision-making. No matter how sensible courses of action may appear to Western thinking, non-Baltic contributors or NATO, it will likely be emotional "angst" or Russian influence that drives decisions rather than rational Western political or military logic. Any predictive paper can only hope to guess, and may prove entirely wrong. That said, this paper seeks to illuminate as accurately as possible the visible and invisible framework to allow for better understanding for outside decision-makers of how and why interoperability and cooperation may or may not work in a crisis and what needs to be done to improve things.

[1] Radina Gigova, "Massive NATO exercise starts in Poland and the Baltics", CNN, June 4, 2018, https://edition.cnn.com/2018/06/03/world/nato-exercise-poland-baltics-russia/index.html.

This paper strays into many complex national and international areas, but does not have the time nor space to do them academic justice. But as NATO security is at risk, even highlighting them as needing further thought and possible action is better than ignoring them altogether.

The Geopolitical Environment

The Baltic Sea region is complex both politically and geographically. The three Baltic States are often lumped together within NATO as one distinct grouping, likely for ease of description, or perhaps just because of intellectual laziness. This grouping has merits but it is also culturally problematic. Thinking that the three will always act together in common interest and unison in a crisis may lead decision-makers down dangerous false alleys. Even taken as a conceptual grouping, the three states do not stand alone. The rest of the Baltic region and the many countries providing NATO reinforcements must also be considered.

The three Baltic States are on the south side of the Baltic Sea with the smallest, Estonia, in the north, middle-sized Latvia in the center, and the largest, Lithuania, to the south. Estonia is bounded by Russia to the east and Latvia to the south. It has just over one million people. "The average size of the Estonian regular Armed Forces in peacetime is about 6,000 persons, of whom about half are conscripts. Thus, the reality is about 2,500 regular personnel exist at all ranks and in all three services. The Voluntary Defense League is highly recruited, with about 15,000 members."[2] The planned size of the operational (wartime) structure is 60,000 personnel, with the high readiness reserve at about 21,000 personnel. This largely conscript system is based upon a mix of historical desire for high numbers, a tactical approach to defending territory at all costs, Soviet legacy thinking from the original designers and a heavy influence from Finland. The system is designed to produce and deploy reserve battalions, a single small regular mechanized infantry battalion and a large volunteer, lightly armed National Guard (the defense league) of over 26,000 men and women (6,500 for combat).[3] It creates two brigades. One of these currently includes a regular battalion and a reserve mechanized battalion, it should be fully mechanized by 2016. NATO's Enhanced Forward Presence (eFP) also provides a large British battalion group and artillery support guns. However, it would struggle to deploy outside of Estonia for any sustained period. A second brigade exists that is completely made up of reserve infantry with limited operational mobility.

The strength of the Estonian nation is its almost fanatical religious desire to retain independence from Russia and the exceedingly high intelligence level of the soldiers. Its weaknesses are logistics, the reliance upon reserves and part-time soldiers as well as the small number of professional officers

[2] "Estonian Defence Forces," Estonian Defence Forces, accessed November 5, 2018, http://www.mil.ee/en/defence-forces.

[3] *Report of the National Audit Office to the Riigikogu,* (National Audit Office: Tallinn, 15 May 2018).

available to the system in crisis and war.[4] Many of these are double-hatted and they cannot fill the posts needed to train the defense league.[5] There are also questions about the ability to mobilize and absorb the large number of reservists for any sustained period without bankrupting the country. Estonia has a small navy based upon mine warfare and an air force base. Its justifiable pride is the NATO Cyber Warfare Center of Excellence.

Latvia is a country of 1.9 million people and dropping daily. It has a small professional army but this was starved of resources for a decade after the international financial crisis in 2007. As a result, it is now playing catch-up in terms of procurement. It has 5,500 professionals and can deploy a regular brigade of two mechanized Latvian battalions and a Canadian mechanized battalion. It is actively purchasing artillery. It has only aluminum coastguard vessels that cannot go to sea in the winter, three helicopters and an air force base. The army is highly trained and arguably the most well-led, active and dynamic force of the three states. It has a small National Guard with largely territorial tasks and limited equipment and training. The brigade could move anywhere in the Baltics to fight, although there would be questions in cases of extreme range, logistics and sustainability. The big vulnerability and challenge is the complete lack of engagement (I would even go as far as complete indifference) to military affairs by the political body and the lack of true operational coherence between the army and the National Guard.

Lithuania is the largest of the three Baltic States and in the 15th Century along with Poland was the major power in Europe. Greatness still hangs heavy over national decision-making and Vilnius is seen as the center of Europe. Lithuania does not really engage itself as one of the three states, looking more to Poland and Germany for support. Lithuania's operational focus is towards Headquarters (HQ) Multi-National Corps Northeast in Poland rather than toward its two neighbors. Lithuania is also the only one of the three large enough to create a comprehensive defense system. The major challenge for Lithuania is the strategically vital "Suwałki Gap"—the short, roughly 100-kilometer land connection with Poland, between Belarus and Kaliningrad. It is the key both to keeping Lithuania joined to Poland and to maintaining the capability of land reinforcement for defense of the Baltic States. It creates a double-facing operational focus of NATO responsibility that makes it hard to imagine sending the best Lithuanian troops away from the country unless back-filling reinforcements came from Poland or the United States to assume the responsibility.

Lithuania adopted professionalization in 2008 with mainly British organizations, training and structures making it clearly the most operational of the three. Yet, after the invasion of Ukraine in 2014, Lithuania decided to go back to conscription to double its forces. This immediately watered-down the quality, stretched the system and brought equipment and readiness problems across the

[4] Dario Cavegn, "National Audit Office: Combat readiness, staff, equipment of Estonian Defence Forces has improved," Eesti Rahvusringhääling, February 8, 2017, https://news.err.ee/120613/national-audit-office-combat-readiness-staff-equipment-of-estonian-defence-forces-has-improved.

[5] Ibid.

whole force. Now, Lithuania has 20,500 professionals and can deploy four brigades of mixed professionals, reservists and volunteers. It is not at all clear how many units are to be reserves or how they will be brought quickly to operational readiness. The rapidly increased size of the force has serious budget implications dropping the amount spendable on each serviceman to less than half that of Latvia.[6] This means that there must still be severe shortfalls somewhere in training, logistics and equipment. Only the Iron Wolf brigade is mechanized and truly deployable outside the country. But as the only true fighting force, sending it elsewhere would be a military and political risk. Lithuania has a navy but for mine hunting and patrols. It does not have any capacity to face the Russian fleet. The air force has transport aircraft regularly used by NATO but, like the other two Baltic States, no fighters. The country is supported by a German mechanized eFP battalion group, including a large Czech mechanized company and a French contingent with artillery.

A strong point is that the soldiers of all three countries have shown themselves on international operations to be highly professional in attitude, capable and courageous. If allowed or ordered, they will easily integrate with one another and work together. There is no reason to doubt that the National Guard will be any different, although mastery of the English language is less common. What should concern all three countries are the command and control arrangements at higher levels between peace and crisis, how the organizations will function in a fast moving mobile war with Russian air and artillery and the readiness standards of all reserve units and individuals to meet a serious war.

The most Eastern country on the Baltic Sea is Russia. Significant factors here include the Port of St. Petersburg hosting the Baltic Fleet and the NATO eastern frontier of Estonia and Latvia, where close to the border Russia deploys the large Western Group of Forces. Also notable, with a dominant military position on the Baltic, is the heavily armed and fortified Russian exclave of Kaliningrad, partially separating the three Baltic States from the remainder of NATO. According to a recent piece in *Bloomberg*, "It is perhaps the most strategic piece of real estate in Europe."[7] Fielding a huge number of air-defense, ground and sea systems this exclave can effectively deny access to the northern Baltic. US analysts even suggest that Russia has also based nuclear weapons there.[8] The Russian forces are arguably the most ready for war in the region and pose a constant existential threat.

The most northeastern Baltic Sea country is Finland. While Finland is not a member of NATO, it does share a 1,300 km border with Russia. It has a small professional force of 8,800, but a vast, well-motivated and highly intelligent reservist force, including ready volunteer units of 300,000. It is also

[6] *The Military Balance* (IISS, 2017).

[7] James Stavridis, "Putin's Big Military Buildup Is Behind NATO Lines," *Bloomberg*, October 20, 2018, https://www.bloomberg.com/view/articles/2018-10-20/putin-s-big-military-buildup-is-behind-nato-lines?fbclid=IwAR213Ez30xz8v2N-mgvIFnSPV_ND0II0KGB0wVdTrIzIYHBG1Duh2iUXnTA.

[8] Hans M. Kristensen, "Russia Upgrades Nuclear Weapons Storage Site In Kaliningrad", Federation of American Scientists, *Strategic Security*, June 18, 2018, https://fas.org/blogs/security/2018/06/kaliningrad/.

modernizing how it uses its conscripts.[9] The country spends much of its defense budget on simple but high-quality modern equipment. It has a modern air force with F-18s and modern missiles. It has a small navy but with high-speed missile boats. If there is political will to fight, it would be a tough nut to crack. It is strongly increasing its military contact with the US, but at the same time politically it has recently re-declared it will not join NATO.[10] From the outset of any discussion about the region, the value of this country as an ally *against* Russia in times of need must be questioned. Recent discussions show that geographic *realpolitik* still dominates its thinking about NATO[11] and there is no real clarity about how deeply *Finlandization* still runs as a national security concept.[12]

On its Western side, the Baltic Sea is bounded by Sweden, another historically neutral country. But Sweden is in a state of flux when it comes to its defense and security policies. After 15 years of neglect, it has increased defense spending greatly, reintroduced conscription and has been exercising more with NATO countries, especially the US. But most of Sweden's current forces are reservists with much less training than is needed for an anti-Russian environment. It is pulling equipment out of storage to equip them. In addition, Sweden now has an officially recognized national policy that it needs support from allies if attacked by Russia.[13] Despite this, Sweden has an ambivalent attitude toward NATO membership, and arguments usually link the country to joint membership only if Finland joins.[14] Sweden also owns the geographically dominant, but highly vulnerable and expensive to defend Island of Gotland. The Nord Stream Two pipeline will run close to the island, making it clearly inside a zone of Russian interest should they wish to meddle. Sweden like Finland both possess navies and air forces that could do Russia harm.

The lower part of the Baltic Sea is bounded and dominated by NATO members Poland, Germany and Denmark but these arguably inhabit a different operational space for NATO.

Into this international mix another level of complexity has been introduced to the Baltic States by the reinforcements of NATO. These include the eFP headquarters and units from many NATO countries. Small NATO HQs are deployed, one in each Baltic State, to manage reinforcements, and are a very visible presence of NATO structures and bureaucracy. In truth, eFP has brought major contributions

[9] Michael Peck, "Forget Russia: Is Finland the Hybrid Warfare Champion?", *National Interest*, October 27, 2018, https://nationalinterest.org/blog/buzz/forget-russia-finland-hybrid-warfare-champion-34362.

[10] "Finnish president: Finland not ready to join NATO yet because of Russia's position", *UA WIRE*, September 17, 2018, https://uawire.org/finland-not-ready-to-join-nato-because-of-russian-position.

[11] Ibid.

[12] Anna Nemtsova, "Finland and the Bear. Russian meddling is a rising concern in Helsinki", *Foreign Policy*, July 31, 2018, https://foreignpolicy.com/2018/07/31/finland-and-the-bear-russia-putin-trump-finns-helsinki/.

[13] Aaron Mehta, "Fortress Sweden: Inside the plan to mobilize Swedish society against Russia", *Defense News*, March 14, 2018, https://www.defensenews.com/global/europe/2018/03/14/fortress-sweden-inside-the-plan-to-mobilize-swedish-society-against-russia/.

[14] Michael Miklaucic, "Why Finland and Sweden still flirt with joining NATO", *The Hill,* September 4, 2018, https://thehill.com/opinion/national-security/404298-why-finland-and-sweden-still-flirt-with-joining-nato.

to the defensive and deterrence mix. The United Kingdom has provided a battalion for Estonia, Canada for Latvia, and Germany for Lithuania. Virtually all other NATO countries are contributing company-size or smaller groupings on everything from medical to de-mining engineers. But these turn the eFP battalion groups into slightly unwieldy multi-flagged, multi-lingual forces. Coordinating them in a fight would be a serious task in itself. Further south is a US rotational armored brigade based in Poland.[15] Notably, neither Finland nor Sweden has added any contributions to eFP despite being just across the sea. Arguably, they would be involved immediately by sheer geographical necessity should any serious Russian activity occur in Estonia or Latvia.

An additional operational step forward for the region occurred on the first day of the recent Brussels Summit when Denmark, Latvia and Estonia agreed to create a new Northern Multinational Division Command, with Canada, the UK and Lithuania also signing on as contributing countries. A recent article in *Defense News* articulates that "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—all with an eye on being prepared in case conflict breaks out on the Baltic Sea."[16] But this HQ does not have formal NATO endorsement and adds a further layer of political, military and cultural complexity to the region without any real operational clarity on how it would manage its task legally and what it would do in the event of a crisis.

Two final comments for the regional geopolitical environment concern NATO and the EU. First, NATO has shown little coherent leadership in terms of creating cooperative defense within the Baltic States or in trying to manage the now almost Byzantine military organization they have accepted. The simple act of creating three separate eFP HQs and not endorsing the new divisional sized headquarters as a full NATO HQ sharply reduces the coherence of any future Baltic military response. There are dangerous gaps in authority and responsibility that need closing. It also creates multiple decision centers for any future NATO and national activity. Some eFP contributions are NATO, and in some cases like with the Canadian troops in Latvia, there are also deployed an additional national contribution as well. This also creates further political decision-making incoherence. That said, it could be argued equally that, if Russia understands the challenge, it may also grasp that this can add political and operational uncertainty for Moscow as well. Russia cannot isolate one country easily without engaging many more nations.

The EU, through the European Security and Defense Policy (ESDP), has so far not taken a serious attitude toward Baltic defense because NATO is fully engaged. But this argument misses the complexity of the region both for NATO and the EU. Sweden and Finland are not engaged as part of

[15] Will Morris, "Fort Hood armored brigade arrives in Europe, ready to roll into Poland", *Stars and Stripes,* May 22, 2018, https://www.stripes.com/news/fort-hood-armored-brigade-arrives-in-europe-ready-to-roll-into-poland-1.528383.

[16] Aaron Mehta, "NATO has a new Baltic command structure", *Defense News,* July 11, 2018, https://www.defensenews.com/smr/nato-priorities/2018/07/11/nato-has-a-new-baltic-command-structure/.

any cooperative venture, and the EU could play a serious role by trying to link the two more firmly into a cooperative battle space. The EU is also creating political uncertainty for the region by the vacillation of some countries regarding the continuance of sanctions against Russia for their invasion of Ukraine. This vulnerability will be exploited by Russia and will almost certainly be reflected by some within discussions in the Baltic political spaces as arguments for supporting a Russian line in a crisis. There has not been complete EU coherence in this matter. Several states, like Italy and Spain, are showing general weakness in their resolve against Russia,[17] opposing the introduction of EU sanctions and favoring a "business as usual" approach with Russia."[18] It is questionable if the political responses like those of Italy indicate a deeper problem dealing with Russia, or if they may appear disastrously as a NATO weakness if a crisis occurs in the *distant* Baltics. Current Baltic structures now rest heavily upon eFP contributions and do not need to be disturbed by political machinations, delays or withdrawals as any Russian activity commences.

Hybrid Warfare

The Helsinki-based Hybrid Warfare Centre of Excellence (Hybrid COE) characterizes hybrid warfare with two points standing out strongly. These are the focus of an enemy upon *vulnerabilities* and the act of *influencing decision-making.*[19] It is these two areas that need the most attention within this paper as interoperability between nations is largely a political not military activity and demands that the political elite both understand the significance to themselves, their neighbors and NATO. Equally they may need the will to make a decision that for many appears directly against the perceived national interest.

Phases of hybrid activity are identified by the COE as *priming* and *operational*. The first can be observed clearly in the three Baltic States as Russia monitors the situation, improves assets, exercises influence and prepares for operations. Operational activities in the cases of Georgia and Ukraine were waged as part of a brutal conventional war not only advanced by little green men. The attempts to influence decisions and to exploit weaknesses in all three states are ubiquitous although not always clear on the surface.

The hybrid warfare report by the Rand Corporation about the Baltic States simplified the activities into three categories. These are "nonviolent subversion, covert violent action, and conventional

[17] Maria Shagina, "EU sanctions policy towards post-Soviet conflicts: Cases of Crimea, Eastern Ukraine, South Ossetia and Abkhazia", *UNISCI Journal* #34, January 2017, https://www.ucm.es/data/cont/media/www/pag-91857/UNISCIDP43-4SHAGINA.pdf (Page 77).

[18] Maria Shagina, "EU sanctions policy towards post-Soviet conflicts: Cases of Crimea, Eastern Ukraine, South Ossetia and Abkhazia", *UNISCI Journal* #34, January 2017, https://www.ucm.es/data/cont/media/www/pag-91857/UNISCIDP43-4SHAGINA.pdf (Page 81).

[19] "Hybrid threats", The European Centre of Excellence for Countering Hybrid Threats, accessed November 14, 2018, https://www.hybridcoe.fi/hybrid-threats/.

warfare supported by subversion."[20] The report concludes that, in the Baltic States, improving economic situations and increasing integration of Russian speakers makes it hard for nonviolent subversion to gain traction. This author would argue otherwise and suggests that the Rand team was looking too much on the surface at universally recognized weaknesses like the historical language split. Furthermore, Rand suggested that violent covert action is also likely to be caught and smothered by improving security forces. This assumes a scaling of any Russian operation that fits the forces available to the Baltic States rather than what Russia could do if it wanted to overwhelm the region. They may not be as kind as the Rand report thinks. The Russian forces sent into Donbas were initially quite large but not overwhelming as Russia expected much more support and less opposition than they actually experienced. Russia may not be so forgiving next time if it follows the same operational path. Also, this statement by Rand cannot be fully confirmed as it is possible that Russia has simply not prepared, needed nor wanted to use this activity yet. This would be especially so if other activities were already working to their advantage. If anything, Russian activities today seem not to cow the Baltic authorities or public, but on the surface serve to galvanize them to greater public action to integrate and create stronger structures against Russia.

Clearly having NATO and the EU delivers a strong undercurrent of confidence in this regard. But this should not be taken at face value. The Russian roots in the post-Soviet world run deep and much deeper than the West realizes. The current Bulgarian president serves as a clear warning. He was, until recently, a NATO-positive chief of the Air Force; but after his election to the presidency, it became apparent he was and always had been a firm Russian supporter. No one, even in his own country, knew or suspected this development.

The main conclusion from the Rand report is that the main challenge to security comes from Russian conventional superiority. According to the report, "A large-scale conventional Russian incursion into the Baltic's, legitimized and supported by political subversion, would rapidly overwhelm NATO forces currently postured in the region."[21] But in hybrid warfare terms there is no reason for Russia to go to war if the states or one of the states can be captured without fighting against a wider NATO coalition and risk losing. Thus, political subversion, state financial destruction, or worse state capture, are the greatest dangers. Unfortunately, neither NATO nor the EU takes this type of threat seriously. The EU even chooses to ignore serious cyber threats from Russia.[22] Latvia for many reasons is clearly the most vulnerable of the three countries in this regard and losing Latvia or allowing Russia to gain strong political influence could undermine the cohesion of the Northern arm of NATO. This is where the capacity to unravel NATO activities or reduce Baltic international cohesion is greatest. But arguably, understanding this problem is also where NATO and international actors are at their

[20] Andrew Radin, *Hybrid Warfare in the Baltics*, (Santa Monica: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1577.html.

[21] Ibid.

[22] Laurens Cerulus, "Russia dodges bullet of EU sanctions on cyber – for now", *Politico,* October 18, 2018, https://www.politico.eu/article/russia-dodges-eu-sanction-on-cyber-for-now/amp/.

weakest. They find it easier to analyze the surface than to look deeply at problems.

The key to understanding hybrid warfare is to comprehend the systemic vulnerabilities of each country and how those can affect decision making at crucial moments. The current pro-Russia actions of Italy show that policy can be easily skewed toward support of Russia through any manner of means and over a wide range of national domains.[23] There is a need to *look beyond defense* at key areas like financial and political influence to judge where key vulnerabilities lie and why they may affect support for other states at a critical juncture.

Of the three Baltic States, Estonia has been in the news most often regarding Russian aggression and also for its stubborn public defiance against Russian activities. The attempts to influence and threaten Estonia have been both visible and covert. In 2002, Russia conducted a full mock airborne attack against Estonia turning away at the border at the last moment. The author saw the video. In 2007, there was a crippling cyber-attack on the country, the first of its kind against a NATO ally.[24] Most recently, Russian President Vladimir Putin flew cynically and illegally over Estonian airspace on his way to meet US President Donald Trump in Helsinki. The Russian Ministry of Defense (MOD) simply refused to comment.[25]

Covert hybrid threats against Estonia include active spying and suborning politicians or members of the public. The most notable spy case involved Herman Simm, who was head of security in the Estonian MOD and was sentenced to 12 years imprisonment in 2009. He gave Russia perhaps the biggest intelligence haul of modern times. His handler was a Russian masquerading as an EU citizen.[26] More recently, the director general of Estonia's Foreign Intelligence Service, Mick Maran, said in the US, "We [Estonian intelligence] have detected a network of politicians, journalists, diplomats, business people who are actually Russian influence agents and who are doing what they are told to do [by the Kremlin]."[27] The most recent spying case happened in 2018, with the arrest of an Estonian Russian-speaking Army major and his father.[28] This small country is clearly high on the Russian

[23] Carly Read, "It's been too long!' Italy invites Kremlin to Rome after blasting Russian sanctions", October 25, 2018, https://www.express.co.uk/news/world/1036518/russia-news-italy-guiseppe-conte-vladimir-putin-US-sanctions.

[24] Damien McGuiness, "How a cyber attack transformed Estonia", *BBC,* April 27, 2017, https://www.bbc.com/news/39655415.

[25] Tyler Durden, "Putin's Plane Illegally Crossed Into NATO Airspace, Estonia Says", *ZeroHedge,* July 18, 2018, https://www.zerohedge.com/comment/12029413?sort_by=thread&sort_order=ASC&items_per_page=50&page=1%2C0%2C0%2C0%2C0%2C0%2C0%2C0%2C1.

[26] Fidelius Schmid, Andreas Ulrich, "Betrayer and Betrayed: New Documents Reveal Truth on NATO's 'Most Damaging' Spy", *Der Spiegel,* May 10, 2010, http://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-693315.html.

[27] Jeff Seldin, "Estonia Spy Chief: Network of Operatives Pushing Russian Agenda in West", *Voice of America,* July 21, 2018, https://www.voanews.com/a/networks-of-operatives-pushing-russian-agenda-in-west/4492266.html.

[28] "Estonia Arrests Army Officer, His Father On Suspicion Of Spying For Russia", *Radio Free Europe/Radio Liberty,* September 5, 2018, https://www.rferl.org/a/estonia-arrests-army-officer-his-father-on-suspicion-of-spying-for-

espionage list. The latest catch indicates that the counter intelligence system works, but equally that the country is still highly vulnerable to Russian attacks.

The financial system has also been rocked recently by knowledge that Danske Bank has been engaged in suspicious transactions with Russian clients from 2007 to 2015, with 15,000 customers doing a staggering €200 billion ($225 billion) in business. According to Organization for Economic Cooperation and Development (OECD) data, this is equivalent to the total national GDP for Estonia during that period.[29] This is a shock for a country that prides itself deeply upon integrity. It should have raised concerns at the government level. The official Danske Bank lessons report highlights that "only part of the suspicious customers and transactions were historically reported to the authorities as they should have been," but this indicates that some suspicious transactions *were* reported and therefore were known (and the amounts of money would have been seriously large).[30] Thus, Mick Marran's comments about an extensive web of *agents of influence* not only highlights that Russia is highly active below the horizon in this small country but also indicates that some senior politicians were likely in full knowledge of the Danske Bank facts if not overtly involved themselves. The possibility of blackmail or exposure of public figures during a crisis is large and may have severe ramifications for national and NATO decision-making should Russia target Estonia or even isolate Latvia next door. However, equally importantly, the comments of Marran should also raise serious questions about the lack of a similar open discussion from and within Latvia. What has not appeared in Estonia is any serious attempt to create social division on anything other than Russian issues or to create unhelpful discussion about the defense system or its vulnerabilities. It could be argued that national cohesion in this regard is so strong that it would be energy wasted or conversely that Russia has no wish to highlight any perceived vulnerability because, like today in Ukraine and Bulgaria, it does not want it fixed.

To outsiders and on paper, Latvia appears to be the most vulnerable to hybrid warfare because of its large Russian-speaking population. This is assessed at 25 percent of the roughly two million people in the country, although many are actually from Ukraine, Belarus and elsewhere. These others do not follow Russia with the same zombie-like adoration of Putin as those of Russian extraction, but they do tend to vote Russian as the Latvian-speaking parties do not welcome them. The population includes now over 50,000 Russian immigrants. This language split and apparent vulnerability to Russia is what attracts the most attention in the foreign media. Inside the country, the main concern is the specter of education in Latvian for Russian-speaking children and the severe lack of good teachers. Yet, despite this thorny issue, the thought of unrest is far from most minds as there is actually considerable harmony within the country. The sports teams bear witness to this. It would be hard to

russia/29473872.html.

[29] "Gross domestic product (GDP)," OECD, accessed November 14, 2018, https://data.oecd.org/gdp/gross-domestic-product-gdp.htm.

[30] "Findings of the investigations relating to Danske Bank's branch in Estonia," Danske Bank, last modified on September 19, 2018, https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018.

galvanize many Russians to react in the way that occurred, for example in Odesa. There is also no linkage at all with Estonian Russian speakers. However, the Russian-speaking media within Latvia has produced a veritable onslaught of pro-Russian messaging which is also strongly anti-NATO, -US and -EU. This comes from *respected* sources like Russian historians, actors and writers and is highly divisive culturally. These messages are far too well-structured and on similar themes to be anything other than coordinated and government-backed by Russia. But the strength of the messages may actually be harming the Russian cause as many Russian speakers leave what they are told repeatedly is a deeply unfriendly and failing country. Many of these attacks seem to pass by the Latvian government, leading to questions about the loyalty of many leading politicians and if state capture has already taken place covertly. Certainly, Oleg Grechenevsky, the Russian analytical expert in the Federal Security Service (FSB), has no doubts about this and makes it clear in his writings that many well-known Latvian politicians past and present are under the influence of the FSB.[31] Thus, the question arises: is this heavy influence real or strong enough to sway politics away from Latvia and towards Russia in a time of crisis?

State capture as an act in Latvia should be viewed as complex and below the surface, like in all post-Soviet countries. Corrupt politics may never provide sufficient excuse for a Russian invasion but it may give Russia enough influence to stop improvements to the cooperative defense system of the Baltic countries, delay NATO reinforcements, and slow mechanisms for improved defense interoperability with Sweden and Finland.

Despite having the smallest percentage of the Russian-speaking population of the Baltic states, Lithuania is just as much a target for Russian mischief as the other two, but is likely to be a harder nut to crack. A December 2016 leaflet published by the Russian embassy in Vilnius tried to highlight the economic disparity between Lithuania and Kaliningrad and offered a better life for those who moved to the Russia's Baltic exclave. Reportedly, just 180 citizens left for Kaliningrad, and half of those apparently did not stay long there.[32] Russia exploits the legacy of Polish speakers within the country, too. This has been challenging for both countries. The minority group has strong links with Russia and supports the Russian narratives.[33] Nevertheless, this is unlikely to be sufficient to upset either country. Despite strong political arguments recently, Poland and Lithuania have 1,000 years of joint history and actively work to establish stronger links.[34] They are both Russia skeptics, members of

[31] Oleg Grechenevsky, *The sources of our "democratic" regime*, (Saint Petersburg, 2018), http://grechenevsky.com/html/sources/index.html.

[32] Sergey Sukhankin, "Lithuania: The Old-New Target of Russian 'Hybrid Warfare?'", *The Jamestown Foundation,* January 27, 2017, https://jamestown.org/lithuania-old-new-target-russian-hybrid-warfare/.

[33] Piotr Maciazek, "Moscow is getting ready for a hybrid war with Lithuania. Is the Polish minority going to be the flashpoint?", *Defence24,* February 19, 2015, https://www.defence24.com/geopolitics/moscow-is-getting-ready-for-a-hybrid-war-with-lithuania-is-the-polish-minority-going-to-be-the-flashpoint.

[34] Zbigniew Rokita, "Where two are fighting", *New Eastern Europe,* August 20, 2018, http://neweasterneurope.eu/2018/08/20/where-two-are-fighting/.

NATO and the EU, and the formation of the Polish- Lithuanian-Ukrainian brigade is evidence of the real direction of cooperation. The recent attempt to smear the eFP German troops with accusations of rape of a minor were met with decidedly swift rebuttals.[35]

Other Baltic areas of weakness for hybrid attack are the ports and harbors, airfields, and railways. They are closely linked to NATO plans for reinforcement. Control of all or some of these would make a Russian attack much easier. The importance of these is highlighted by the recent Latvian spy case involving railway traffic. There is also the problem of the slowness of starting to build the Rail Baltica link from Warsaw to Tallinn. This would provide a huge improvement in logistic support for early reinforcement from Poland and would cement the relationship between the four countries as well as create a further important physical and cultural link between Helsinki and the South. At the moment, the Baltic rail network mainly runs East–West and is largely controlled by Russia (Russian Railways historically controls traffic within the three countries). There are no direct North–South links between the capitals or with Poland. This makes the few roads in the Suwałki Gap more significant for reinforcements. Russian trade largely feeds the warm-water Baltic ports, and freight owners have every reason to support Russia as it provides for their livelihood. The Baltic ports thus retain their importance for Russia and are clear targets. Additionally, Russia has a rail link to Kaliningrad through Belarus and Lithuania. This exposes the major weakness inherent in the fact that the three countries have a strong degree of transit separateness that works completely against NATO whilst the railway system in existence works directly in Russia's favor.

The issue that is most worrying and suspicious to this author is that *Russia has taken fewer obvious hybrid warfare steps* than should be expected within the Baltic States. They have even been less aggressive than with Sweden. At the same time, Latvia has taken fewer steps to counter Russian activities than they reasonably should. This begs the question, *is something happening we cannot see, and if so what is it*? It could be argued that Russia wants just sufficient-enough threat and activity to keep the countries on edge but not enough for them or NATO to take things seriously. This line has merit. In a recent exercise at the Baltic Defense College, there was a war game where students had to look at the US national security strategy and then engage with US officers in the three Baltic States (the "US Ambassadors") and try to push for adding items that would benefit them and improve their security. Each Baltic State delegation went to the US diplomat separately with its own country-specific requests and proposals. This speaks volumes about how the countries think, or do not, about cooperating among themselves, and how they seek to maximize their bilateral relationships with the US.[36] Russian hybrid pressure may be working better than we realize.

[35] John Sparks, "Lithuanians stock up for 'hybrid' war with Russia", *Sky News,* March 3, 2017, https://news.sky.com/story/lithuanians-stock-up-for-hybrid-war-with-russia-10788574.

[36] Mark Voyger, Baltic Defence College notes to Jamestown Foundation on Hybrid Warfare, September 2018.

Conventional Warfare

The conventional threat can be viewed in three ways: attack overland, from the sea or from the air. It could also be seen as trying to destroy, intimidate or encircle. Dangerously, the attacks on Crimea and Donbas have set a precedent of having to fight little green men. This has dominated Baltic military war-gaming and is likely to the detriment of preparing to fight a real war. Even Finland and Sweden may be confused by this.[37] The most recent Latvian exercise focused exactly upon this type of action despite the fact that it is a scenario dangerously far from reality.[38]It is doubly dangerous in that conventionally-thinking military leaders can lull politicians into thinking that this war can be won early and relatively easily by police-type actions against early subversion.[39] As Donbas shows, it cannot. It is also likely preparing forces against yesterday's war.

The conventional threat can be looked at in many scenarios, but one point is fundamental: Russia will act with little or no warning and with deception. Thus, the importance of communication and decision-making is paramount.

The first scenario considered is the one currently most practiced, the appearance of little green men and declarations of independence. This would inevitably be linked to other activities like cyberattacks on communications. All three countries have declared they will fight this problem immediately. In the initial stages, if the strength and activity was similar to Crimea or Donbas, they would likely be able to contain the activity nationally themselves. But there is an inevitability of rapid Russian conventional reinforcement now that Russia has had success with this mode. It could even be a feint whilst conventional activity happens elsewhere. The first moral challenge could be a legal one for eFP troops, if they are faced with firing against apparent host nationals. A second challenge would be the reaction in eFP home nations to the activity and what orders they would give. If the action is minimal, then some countries may be loath to engage militarily if that means probable escalation to real fighting. The boundary for determining hybrid or conventional warfare is a line best judged by the Russian use or not of indirect fire.

In all this, obtaining early agreement on NATO Article V is paramount. The challenge here is one of communication. There is no common operations or intelligence cell for the contributing states or NATO, so gaining a full understanding for NATO and eFP contributing countries at arms length will

[37] Michael Peck, "Forget Russia: is Finland the Hybrid Warfare Champion?", *The National Interest,* October 27, 2018, https://nationalinterest.org/blog/buzz/forget-russia-finland-hybrid-warfare-champion-34362.

[38] "Namejs 2018 military exercise underway", *Latvian Public Broadcasting,* August 20, 2018, https://eng.lsm.lv/article/society/defense/namejs-2018-military-exercise-underway.a289322/.; "Hedgehog 18 military drills to start in Latvia", *Latvian Public Broadcasting,* May 3, 2018, https://eng.lsm.lv/article/society/defense/hedgehog-18-military-drills-to-start-in-latvia.a277112/.

[39] "Estonia Ready To Deal with Russia's 'little Green Men'", *Financial Times, https*://www.ft.com/content/03c5ebde-f95a-11e4-ae65-00144feab7de.; "Latvia says it is ready to repel Russian little green men", *UAWIRE,* September 12, 2016, http://uawire.org/news/latvia-says-it-is-ready-to-repel-russian-little-green-men#.

be extremely difficult. Any political delay on deployments may prove fatal. The need for cross-border support could be vital if an attack is single-country focused. A clear level of uncertainty also exists about whether an attack on one country will lead to further attacks on others or if it is simply a diversion to pull limited troops out of position. Activities like this have been practiced between countries, including with National Guard units, but not with any stress on enabling political and government activities. Commanders now have permission to act immediately in the case of "little green men" or a cross-border attack; but the scenario of crossing to support an ally is another political matter entirely. The logistics alone would stress any system. Not to mention, who pulls the strings in the early stages of a crisis is not at all clear.

A second scenario involves the Russians launching a "no warning" minor ground attack on one of the three countries, for example across the ice into Estonia to seize part of an Estonian town or hamlet, or to take a small part of Latgale in Latvia. Estonia says it would mobilize and fight immediately; but unless there was significant warning, NATO would initially only have the scouts battalion and the British battalion to deploy. The problem would be if Russia attacks on multiple fronts and stretches the Estonian mechanized brigade beyond capability. Estonia would then rely upon the National Guard, which has no fire support and would be quickly overwhelmed. It is highly unlikely at that stage that Latvia would leave itself unguarded and deploy to Estonia. However, the Canadian battalion might politically be able to redeploy. Even so, at present this has not been practiced. Troops from Lithuania would face the same problem but even more so as their logistic support is simply not designed for such distances.

Much greater internal discussion could be expected in Latvia on whether to deploy to fight or to defend against deeper incursions and to protect Riga. Hybrid activities would be used to create diversions to draw forces away or even to pin them down elsewhere. There would be an immediate political challenge internationally about deploying eFP forces to either fight or to block deeper incursions. In this case, both the UK and Canada have shown political resolve to fight, but other reinforcing countries would likely have to gain political authority to deploy to a hot conflict. Some smaller countries may withdraw if the situation looks likely to escalate as their forces are simply not geared for a serious fight. This could seriously break up the operational cohesion established as a result of training and organization. The role of the new headquarters would also be placed in immediate jeopardy as they might want to take urgent operational decisions using all nations' forces in a coherent fashion but the authority at that stage constitutionally lies with nations not with the HQs. Even when Article V is invoked, the cultural challenge for nations will become paramount. This will be discussed later.

A third scenario would be an all-out attack on one of the three Baltic countries using all means, including naval forces attacking ports and airborne forces taking the airfields. Each country is different in this respect. Estonia, as an example, would mobilize and fight. How well and for how long they could fight would depend upon many factors not the least of which is the level of brutality that

Russia would use. If they strike as they have in Donbas and Syria with massive artillery and destroy habitations, then the battle could be short. It also depends upon weather. The terrain is more accessible in midwinter, when the frozen Baltic Sea, lakes and swamps can be crossed, often even by armor. It would also depend upon which routes were chosen and how much warning was given. In all cases, the national troops from Latvia and Lithuania would likely mobilize and stay put, expecting that they will be next. There would need to be a substantial time for the US to bring armored forces to bear, although light ground forces and air reinforcements could be flown to any of the three countries in one to three days if the order is given. The US brigade in Poland would likely stay there to ensure that Polish security is sustained as the main point of entry for NATO forces. In this case, the most likely reinforcements would come from reallocating eFP troops. As they are non-national, they already have a different mindset about the battle space. They are more willing and able to cross borders if ordered. The Czech company based in Lithuania recently trained successfully in Latvia with both the army and the National Fuard.[40] The big question is who will decide that someone needs to move and how much, and who can and will give the order? The whole issue of Baltic region interoperability rests upon this factor and it is a very gray area**.**

A fourth scenario would be an attack on all three countries simultaneously. In this scenario, Russia would likely need access through Belarus. Simultaneously, this would ensure that there could be no reinforcement from one country to another nor would countries consider it. This scenario may give longer warning time but it would also ensure that each country kept its forces close out of fear. There would almost certainly be a heavy increase in hybrid activities before this. There might be chances that the three eFP nations commanding battlegroups could also reinforce but likely only Germany could come overland with ground troops, and the other two with air forces. Even though Germany might also have problematic politics and delay. Nations with eFP forces would not want to deploy air forces directly to the Baltic States as the risk of loss would be too high. The NATO or EU ESDP relationships with Sweden and Finland at that point would be crucial.

In all cases, there is vulnerability within the Baltic States from the sea and the air as not one has a fighting navy able to stop invading forces, nor sufficient air defenses to deter or defend against airborne or heliborne attack. There is Baltic air policing, but this is currently meant for policing not defense. To change this prior to Article V being agreed upon (not just invoked) would take planning and agreements with nations beforehand and a serious political change that does not look likely yet. Chances are that only a few committed states like the UK, US, Poland and Canada would fight immediately without orders.

The Ukraine invasion has encouraged much greater cooperation and training between Estonian and

[40] "NATO battlegroups exercise across Baltic borders", NATO, last modified September 7, 2018, https://www.nato.int/cps/en/natohq/news_157988.htm.

Latvian forces in joint maneuvers.[41] The danger, as previously mentioned, is the focus on soft warfare rather than the nastiness seen in Donbas or Syria. The Lithuanians have done less with their Baltic neighbors, but they did host the large US-led exercise Saber Strike this year, with both countries involved.[42] They also hosted a US airborne exercise flying direct from US.[43] The Lithuanian focus has had to be inwards as they are dealing with returning to conscription and the inevitable stress on professional forces in the process.

Conscripts in Estonia and Lithuania can never gain sustainable interoperability, firstly because their training time is too short and secondly because the soldiers leave before they can ever realize any multinational interoperability benefits. As reserves, the chances that they exercise with other countries is also small and likely only once annually at best. The younger officers also cannot reach professional levels in mobile warfare as training is always by definition more simple. Lithuania has in effect condemned itself to positional defense by policy. The International Institute for Strategic Studies (IISS) budget figures for 2017 indicate that with its enlarged force, Lithuania is spending just $39,000 per soldier in their force compared to $95,000 for Latvia.[44] The discrepancy highlights a considerable difference, much of which will reflect either a lower standard of equipment or heavily reduced operations and maintenance budgets and in effect, less training. The final point about interoperability for conventional warfare is that many of the current exercises reflect considerable preparation time, including internal lines of communication and logistics. Hybrid or mobile warfare operations against Russia are unlikely to be so kind.

Possibly the most complex fault lines are the constitutions of the three states. These empower the president as commander-in-chief. This problem has been discussed in depth by Thomas-Durell Young (2018).[45] Without discussing the complexities of this in detail it is sufficient to say that in a crisis the interaction between the president, parliament, prime minister and commander-in-chief will be crucial. If they are in opposition to each other then there could be critical delays but equally if they are not, there runs the serious risk of groupthink. These complexities are rarely if ever practiced but they will form the cornerstone of decision making pre-NATO mobilization should Russia attack without warning. Or, if Russia acts in a hybrid manner but less than what would warrant triggering Article V. Further complexity is added by the eFP forces who would possibly have to deal with their

[41] ”Estonia’s largest military exercise Siil to partially take place in Latvia,” *Postimees,* March 16, 2018, https://news.postimees.ee/4441173/estonia-s-largest-military-exercise-siil-to-partially-take-place-in-latvia.; “Hedgehog 18 military drills to start in Latvia” [..], op.cit.

[42] Ibid.

[43] “Paratroopers drop in Baltics for swift response exercise”, *Defense News,* June 13, 2018, https://www.defensenews.com/smr/nato-priorities/2018/06/13/paratroopers-drop-in-baltics-for-swift-response-exercise/.

[44] *The military balance 2017,* [..] op. cit.

[45] Thomas-Durell Young, “Can NATO's “new” allies and key partners exercise national-level command in crisis and war?” *Comparative Strategy*, 37:1, 9-21, http://www.tandfonline.com/loi/ucst20.

own personal duality of orders and instructions, creating delay at a crucial time.

Cultural Considerations

To understand if interoperability will or will not work in the Baltic States, one has to look at the culture and history of the region as well as to look for clues on how this will affect decision-making at *le moment critique* of crisis or war. The cultural norms of Hofstede[46] will be used as the framework with added emphasis from Richard Lewis.[47]

Estonia

A key cultural dimension that affects the Estonian defense system greatly is that of *power distance*. This deals with the fact that all individuals in societies are not equal. The cultural dimension expresses the attitude of the culture toward acceptance of inequalities. Power distance is defined as *the extent to which the less powerful members of institutions and organizations within a country expect and accept that power is distributed unequally*. Estonia scores very low on this dimension (40/100), suggesting that the Estonians do not readily obey and respect people in positions of authority based merely on their rank and status as power-holders. Lewis describes Estonians as cynical about power.[48] Estonians in general welcome managers that give them the opportunity to state their opinions and express disagreement, as well as to be included in the decision-making process. But in the defense system the country has a serious cultural fault line. The military leadership largely retains the old Soviet ways of thinking and acting and demonstrates very high power distance tendencies. The military boss-subordinate relationship is visibly more hierarchical than the national score. This brings reduced capacity for independent thought or for proactivity. This is much less so with the volunteers in the National Guard where hierarchy works more by friendship than by order. Power distance also creates a difficult relationship between the military and MOD. The Soviet-thinking norms based upon power have little time for civilians or women and their non-military judgement. Civilian control of the military has often proven difficult if not impossible. This has created tension in the recent past concerning the direction that Estonian defense should take. This has reflected in how the budget should be spent, with a fundamental disagreement between a desire for *numbers* on the side of the military and *coherent and affordable capability* on the side of MOD. There is significant improvement as reflected in audit office reports but key areas of weakness still exist.[49]

Estonia is also an *individualist* country with a score of 60/100. Most Estonians believe that everyone should be allowed to do their own thing, reach new heights or even dig their own graves. They

[46] "Compare countries", Hofstede Insights, accessed on November 14, 2018, https://www.hofstede-insights.com/product/compare-countries/

[47] Richard D. Lewis, *When Cultures Collide, Leading across Cultures*, Edn 3,(London: Nicholas Brealey International, 2006)

[48] Ibid

[49] Dario Cavegn, op. cit.

certainly do not see themselves as "Baltic," but rather more Nordic or European. Work situations are driven more by a task-orientation than by a relationship-orientation, which is to say that for Estonians, work relations serve a functional purpose. Achievement is reflected directly on the person responsible. Estonians tend to be direct communicators. They usually say what they mean and mean what they say and there is limited time for small talk. It is therefore not surprising that they tend to gravitate towards culturally like-minded countries such as Finland, the US and the UK for theirdefense relationships. Fortunately, the UK is deployed with them in eFP. Given the respect that the Estonian military has for the UK after many years of working together on NATO operations, it is unlikely there will be personal tensions about strategy or the need to change. But this Estonian characteristic makes it very hard to assess if in a time of crisis and with differing views on strategy, civilian control of the military would remain solid against a combination of individualistic and power-based military tendencies. In World War II, the Estonian Signal Battalion disobeyed the political order to lay down arms when Russia threatened and attacked Narva.[50] This act is lauded highly in both the military and the country and forms the cornerstone of much of the motivational folklore in the army and defense league. As a result, it would now be seen as treasonous not to defend the country even if the politicians capitulated. But if the threat is simultaneous against both Latvia and Estonia, an order to move and help Latvia could create deep cultural stress across the whole defense system.

With a score of 60/100, Estonians have a high preference for *avoiding uncertainty*. Countries exhibiting high uncertainty avoidance maintain rigid codes of belief and behavior and are intolerant of unorthodox behavior and ideas. This fits well with high power distance organizations and creates an inability to be frank with those in power. Communication travels downwards but rarely upwards. There is an emotional need for rules and regulations (even if the rules never seem to work). This trait shows itself in a desire to stick to the perceived orthodoxy of a given strategy. This shows itself strongly in the near religious significance given to the chosen defense system copied from Finland. Conscription and territorial defense by reserves form a core cultural belief. To argue that this may be wrong, even in part, or is against the lessons from Ukraine is to set up a level of cognitive dissonance that causes visible mental pain. To question this strategy is to be a heretic or worse, a traitor and to be destroyed socially, and perhaps even physically. If this very inward=looking strategy needs to be changed in wartime even by the president, the level of collective and individual uncertainty about what to do next would likely create military chaos

However, a further strand of internal tension within the defense system is caused by a longer-term dimension that is in conflict with many of the previous traits. Estonian culture is shown to be highly *pragmatic* (score of 82/100). People believe that truth depends very much on situation, context and time. They show an ability to adapt traditions easily to changed conditions (again, unlike the military system) but with a strong propensity for perseverance in achieving results. This appears to be reflected in several traits. One is the inviolability and sanctity of the long-term plan for defense spending. The

[50] "51 years from the Raua Street Battle" (in Estonian), Estonian Defence Forces Home Page, accessed on November 4, 2018, http://www.mil.ee/?id=297&sisu=uudis.

second is the complete difference between the political pragmatism of the MOD versus the very different and more inward-looking character of the military staff. Both see international interoperability as a good thing but the underlying motivation is totally different. In MOD it is seen as a political necessity for joint and cooperative NATO action against Russia (outward looking), for staff it is a way to obtain more resources for the defense of Estonia (inward looking).

Latvia

Latvia also has a low score on the *power distance* dimension (44/100). Latvians show a tendency to prefer equality and a decentralization of power and decision-making. Control and formal supervision is generally disliked among the younger generation, which demonstrates a preference for teamwork and an open-style of management. However, within the military there still exists a caucus of older officers similar to those in Estonia who favor control and discipline as the key tools for leadership. Long meetings and some intolerance of ideas are still in vogue. But the low power distance overall likely reflects the ease with which the country was able to move to professional forces in 2004. The authoritative power-based style of conscription is seriously disliked by the public as a Soviet hangover. Conversely, despite the low power distance, there is a normal military sense of loyalty and deference towards authority and status. This attitude makes Latvian forces respectful of political authority and thus more likely to cross borders if ordered than their northern counterparts.

Latvia is an *individualist* country with a high score of 70/100, and it is important to remember that Latvians remained individualist during Soviet occupation. The score accentuates the aversion to being controlled and told what to do. Historically, this came out as delaying or trying behind the scenes to reshape unpopular orders; something that still occurs today in all walks of life. The younger generation is more focused on individual performance rather than that of groups. This means that the professional military takes personal professionalism as soldiers extremely seriously. This fits well with professional structures and Latvian soldiers are very Western in a results-focused way. This innate professionalism also cuts across culture to create a level of team flexibility Estonia and Lithuania would find hard to deliver.

As a *feminine* country with a score of just 9/100, Latvians are modest, keep a low profile and do not wish to offend anyone. Conflicts for Latvians are usually deeply threatening. This makes them very solid as a group for obeying orders and far more likely to follow a politically difficult line. Although the Latvians are considered a relatively reserved culture, they are tolerant towards the culture of other nations mainly due to their long experience of mixing with others nationalities. For the military, working with allies and sharing is a more common theme than trying to keep secrets. This may have both good and bad aspects.

With a score of 63/100, Latvians have a high preference for *avoiding uncertainty*. This manifests itself with allies as accepting that an idea is good but then not passing the idea further up the chain for fear of disturbing things. This frustrates the Canadian eFP troops greatly as they think a problem or matter will be resolved because they have aired it in meetings with the Latvians. In actuality, it goes nowhere. This desire not to "concern" more senior staff in a crisis could have serious implications and lead to breakdown in chain of command communications and understanding, especially between the National Guard and regulars.

Lithuania

For Lithuania, the *power distance* dimension has a low score of 42/100 and this extends more into the military culture than in Estonia and Latvia. Lithuanians show clear tendencies to prefer equality and a decentralization of power and decision-making. Non-commissioned officers are highly respected and can and do act above their rank. Control and formal supervision is generally disliked among junior staffs, who demonstrate a preference for teamwork and an open management style. The senior leadership still have a power based attitude but seemingly less than the other two states. Similarly, there is a strong sense of loyalty and deference towards authority and status amongst the older generation who experienced Russian and Soviet dominance.

The relatively high *individualism* dimension in Lithuania of 60/100 reflects the strength of inward loyalty and looking after one's own family first. Lithuanians speak plainly without any exaggeration or understatement; this too represents individualism. They are tolerant in that they do not care too much about what other people do as long as it does not annoy them; what you do and how you live your life is your business. This has reflected in their Baltic Cooperation stance where they judge activities for their military by improved performance rather than any desire for a better joint system.

As a *feminine* country with a very low score of 19/100, Lithuanians are modest and keep a low profile. They usually communicate with a soft and diplomatic voice in order not to offend anyone. Conflicts for Lithuanians are usually threatening, because they endanger the well-being of everyone, which is also indicative of a feminine culture. Although the Lithuanians are considered a relatively reserved culture, they are tolerant toward the culture of other nations and welcome the other eFP members as their own. Like Latvia, this is partly due to their long experience of mixing with other nationalities. But this tolerance and wish to not offend could also have serious implications for interoperability both with the Germans and perhaps with allies if they need to give an order for a critical and perhaps dangerous task.

The high score of 65/100 on *uncertainty avoidance* reflects a built-in worry about the world around them. This worry joins the natural softness and some aspects of power reflecting in a respect for finding managers who need to be seen as knowing everything and able to lead. This respect takes the uncertainty away from themselves. It also explains why qualifications and formal titles are lauded and often included on business cards. Other signs of high uncertainty avoidance among Lithuanians are reluctance to taking risks, bureaucracy and emotional reliability on plans, rules and regulations. It deserves serious note that plans may not be followed but their existence is vital for reducing stress as they reduce uncertainty. The importance here for interoperability is clear. If it is not already written, it may simply not happen. Flexibility is not a Lithuanian trademark.

One cultural conflict within the system likely comes from the individualism and uncertainty avoidance dimensions. These underscore the change back to conscription bringing the need for a *safe* Lithuanian solution rather than face the uncertainty of reliance upon NATO or other allies. But these traits also work strongly against the high risk to the country of deploying precious troops outside of borders. They will go if ordered because internal national conflict would be frowned upon but they might not "rush" to do so.

The Others

It is hard at present to identify how culture would affect each of the neighbors or eFP contributing countries. In some, such as Finland, the *realpolitik* of its large neighbor and history may well overwhelm the desire to assist. Sweden will likely wait to see what Finland does before reacting. That said, Sweden would likely host US forces, not because it wishes to contribute but because of the selfish reason of added security. Poland has no choice but to react. History tells the Polish nation that if the Baltics are lost so is Poland. The UK and Canada have both made it politically clear that they take this role seriously and expect their troops to fight. Like the US, both countries score very low on *uncertainty avoidance* and high on *individualism*, so risk taking and flexibility as well as a desire for results come natural to them. This seriousness is tangible when talking to officers and men of all three countries who see this very much as an operational tour. The wild card is Germany. The country's cultural shift to political passivity and "agreement" with Russia linked to a high degree of *uncertainty avoidance* (65/100) and searching for *long-term perspectives* (83/100) may lead to dangerous decision-making delays that Lithuania and the other Baltic States cannot afford.

Conclusion

Many suggest that because of the exercises and eFP interoperability in a crisis, all will be "*all right on the night*." However, when factors like Russian meddling in US elections, Catalonia, Brexit, the drive to force immigrants into Europe, the perfidiousness of Italy, the unsettling comments about Russian influence on senior people from Latvia and Estonia, as well as the general military and cultural complexities of the region are taken into account, it would be nothing short of a miracle if it did all work smoothly. It is a harsh conclusion. But added to these factors there is little open-source evidence that interoperability or deep operational cooperation between the three states is a politically working concept. In fact, there is much evidence to suggest that national cultures and history and Russian interference will coincide to keep the Baltic States as separate countries and in their individual battle spaces.

This is further reinforced by NATO HQ, which has accepted a split into two divisional areas without formalizing the command and control arrangements. NATO has also moved toward an eFP deterrence posture that reinforces the split among three separate eFP headquarters and channeled eFP allied contributions to individual countries rather than supporting the region as a whole. This may appear fine as a deterrent posture and for *nice to have* cooperation, but it would be a total mess if forces actually have to fight. NATO leadership is still not supporting change to the command-and-control arrangements in the pre-conflict stages. The lessons from Ukraine about political centralization of command being too slow to match Russian actions have not been properly addressed. The NATO structures now put in place actually serve to make interoperability and proper military cooperation across all three countries near impossible. NATO and contributing allies also need to grasp that uncertainty avoidance affects the political level equally as much as the military. Politicians need plans and prior direction as much as military leaders if they are to be effective. The current posture actually creates instability and uncertainty and will likely contribute to a decision-making failure at the highest levels of the three states (and maybe allies) unless taken seriously.

Each country has its own distinct political and cultural gremlins. It is hard to judge how Estonians will deal with a more complex battle than one just on their homeland. In simpler and slower world of 1919, they fought for Latvia freeing Cēsis after the provisional Latvian government had been ousted by the Germans in a coup d'état.[51] But they returned quickly to Estonia to fight against the Russians at Narva. There have also been so many cultural tensions, both within the national character and in the very starkly different cultures between the military and the professional elite. The reality is that Estonia has a defense infrastructure that is designed for one thing and one thing only: to defend Estonia. It has no capacity to be used NATO-wide beyond company level, and if there was any risk to the homeland they would not move anyway. The best that can be done is to identify how best to use what is there to optimize and accept that.

Latvia has a greater capacity to move but is cripplingly short of indirect fire power and logistics. It is also the hardest of the three to call in terms of "will we, won't we" because of Russian influence in the political sphere. Lithuania has more troops but it also has two fronts to defend and a cultural propensity to look inwards first. The eFP support in all three states is deterrence-based and simply not militarily coherent. None of this bodes well for dealing with a surprise battle let alone a complex hybrid attack on political, cyber, financial, social and military fronts.

The logical step is to take reality and reshape it. In the first place, at the military-political level split the battle space into two with clear divisional boundaries between Lithuania and Latvia. Give the tasks of ensuring the Suwałki Gap stays open and fighting in Kaliningrad firmly to the division using the available US ground support. Accept that, in the short term, US armor is unlikely to traverse the Baltic Sea and will need to come overland from Poland. Keeping the gap open is vital to this task.

[51] Andrew Parrott, "The Baltic States from 1914 to 1923: The First World War and the Wars of Independence," *Baltic Defence Review* No 8, (Vol 2, 2002).

The second division should be made up of Estonia and Latvia. It should be accepted by NATO that their troop contributions are too small to do anything other than defense of capitals, key ports and airfields. The eFP contributions should be pooled and a reserve brigade created. This should be commanded alternatively by the UK and Canada and not Denmark. This will create greater deterrent uncertainty and actually increase the divisional force's capability in terms of mobility. Reinforcement from the US and ground-attack support is likely to be delivered by air, and both countries have worked at having a good liaison for this.

The ESDP contribution must tie the division into one battle space with Finland and Sweden. This is important because in any Russian attack, the airbases in Estonia and Latvia are likely to be untenable because of extremely limited cover. Bases in Sweden and Finland would be needed for US air reinforcements. Both countries must be encouraged to contribute to forward defense in terms of ground and air and to take greater responsibility for sea access. It should be considered that the new divisional HQ will also include Swedes and Finns on the staff. This would be a considerable political "ask" for both countries and would require a two-pronged political approach from both NATO and the EU, not to mention bilaterally from the US. Asking the Finns to command the division would be taken extremely seriously by them and would upset the Swedes, not to mention the Russians. If Finland refuses, then Sweden would be asked. This may provide the tipping point both need to take full NATO cooperation seriously politically. Again doing this would greatly enhance the legitimacy of deterrence and would create greater military coherence in a much more complex battle space that concerns a number of nations other than just Estonia and Latvia alone.

NATO needs to focus hard upon its overall command structures and the actual fighting and support structures on the ground used by member countries. Reading the excellent Estonian audit office reports would help to understand the fault lines in all three Baltic States. Then, there needs to be a greater focus upon the pre–Article V stages of political decision-making and how all three countries interact in cooperation with each other, NATO and non-NATO allies. On the surface, it appears that too much is left to chance, national public relations and uncoordinated bilateral cooperation.

What this paper sees as most important is that the knee-jerk response to create deterrence has actually created a military monster that is increasing the military capabilities of the three Baltic States but not in a coherent military way. It actually serves to weaken the political aspects of cooperation and interoperability by seemingly proving a solution for war. It does not. This solution has not taken the political, military and cultural realities into full account, but rather simply assumed a set of conditions that are in fact absent or worse, totally different from those considered. The region now needs a hard restructuring to concentrate not upon deterrence (which is not a military task) but upon combat. This needs more serious thinking.

Challenges in Developing a Common Baltic Air Defense

Anthony Lawrence

Introduction

At the moment, the Russian Federation poses the only conceivable military threat to the Baltic States. The importance that Russia attaches to military aviation as a means of achieving political objectives is made clear in its military doctrine, which recognizes the key role of air and space forces in wartime, and directs the strengthening of air -defense capabilities as a top priority for military development.[1] In the event of a military crisis involving the Baltic States and Russia, Russia would be expected to take efforts to secure air superiority over the Baltic region and to use air assets to attack Baltic and NATO targets.[2] Air superiority would also make possible the use of airborne infantry forces, which is one of Russia's key rapid reaction capabilities in seizing strategic locations and disrupting defensive operations.

Against such a threat, the Baltic States presently possess only very limited air-defense capabilities. A comprehensive air-defense system, however, is well beyond their financial reach. This situation creates vulnerabilities not only for the three states themselves, but also for NATO, whose reinforcement of the region in the event of a crisis would be hindered by a lack of air cover. Thus, air defense is probably the most pressing military capability shortcoming in the Baltic region.

This paper describes the Russian air threat to the Baltic region, and the capabilities that Estonia, Latvia and Lithuania currently possess to deal with this threat. It examines the challenges the Baltic States face in responding to this air threat and then makes recommendations for a cooperative approach—between the Baltic States and with NATO and other regional allies for improving the situation. Much of the material in this paper is drawn from a recent report on this subject, written at the request of the Ministry of Defense of Estonia and co-authored by the present author.[3]

[1] "The Military Doctrine of the Russian Federation", The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 29 June, 2015, https://rusemb.org.uk/press/2029.

[2] General Philip M. Breedlove, "Toward Effective Air Defense in Northern Europe," *Atlantic Council Issue Brief*, February 2018, http://www.atlanticcouncil.org/publications/issue-briefs/toward-effective-air-defense-in-northern-europe.

[3] Sir Christopher Harper, Tony Lawrence, and Sven Sakkov, *Air Defence of the Baltic States* (Tallinn: ICDS, 2018), https://icds.ee/air-defence-of-the-baltic-states/.

The Need for Baltic Air Defense

The Russian Air Threat

Russia's strategic goal of undermining the European and global security architectures has been evident in, for example, its invasion of Georgia, its annexation of Crimea and its occupation of the Donbas, its involvement in the Syrian civil war, and its interference in the US presidential elections. Although Russia frequently characterizes NATO as an adversary and a threat to Russian interests, the probability of a direct Russian military attack on NATO member states is still assessed to be low.[4] Nonetheless, an ability to deter and, if necessary, defend against Russia in all domains should form the baseline for prudent defense planning for the Baltic region. The air domain poses a particular challenge in that operations here are conducted at high speeds and the potential for surprise is great. Furthermore, the geography of the Baltic region and the militarily non-aligned status of Finland and Sweden gives the Baltic States little strategic depth and makes air operations over their territories inevitable in the event of a conflict.

Worldwide, NATO has a considerable advantage in jet fighter capability in both quantity and quality. Analysts assess that overall, NATO has a greater than fourfold lead in numbers of fourth-generation or newer combat-capable aircraft.[5] However, more than half of the NATO total is based in the continental US and almost none of it is in the Baltic States, where combat air presence is normally limited to the eight aircraft conducting the NATO air policing and enhanced air policing missions. As such, reinforcement of the region by fighter aircraft would take time. Rand's well-known wargaming of the defense of the Baltics, for example, assumed that with a week's warning NATO could muster 18.5 squadrons of combat air by D-Day.[6] Russia's Western Military District, meanwhile, is home to some 27 combat air squadrons, six battalions of attack helicopters, and a division of airborne infantry.[7] In a crisis, this capability could be quickly and substantially reinforced from other Russian military districts.

Further complicating air operations in the Baltic region, Russia has also invested considerably in its

[4] Välisluureamet (Estonian Foreign Intelligence Service), International Security and Estonia 2018, (Tallinn: Välisluureamet, 2018), 18, **https://www.valisluureamet.ee/security_environment.html**.

[5] Worldwide totals: NATO – 5,457; Russia – 1,251. Scott Boston, Michael Johnson, Nathan Beauchamp-Mustafaga, and Yvonne K. Crane, *Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority* (Santa Monica: Rand, 2018), 8, https://www.rand.org/pubs/research_reports/RR2402.html.

[6] David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO's Eastern Flank. Wargaming the Defense of the Baltics* (Santa Monica: Rand, 2016), 5, https://www.rand.org/pubs/research_reports/RR1253.html.

[7] 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), (Defense Intelligence Agency, 2017), 55 (available from http://www.dia.mil/News/Articles/Article/1232488/defense-intelligence-agency-releases-russia-military-power-assessment/, accessed 12 July 2018).

air-defense systems, which can engage targets over large areas of NATO territory. Its sophisticated ground-based air-defense capabilities include the long-range S-400 system, whose variants boast (likely exaggerated) intercept ranges of 250 and 400 kilomters.[8] Russia has also deployed Iskander ballistic missiles close to its border with Estonia and in the increasingly militarized Kaliningrad exclave.[9] Furthermore, it will complement its offensive air capability during 2018 by augmenting the Baltic Fleet with corvettes armed with *Kalibr* cruise missiles.[10] The anti-shipping variant of this missile is estimated to have a range of 430–660 km, while the ground-attack variant has an estimated range of 1,600–2,400 km. Taking into account the high speed and potential short notice of an air campaign, it is apparent that Russia holds a substantial local advantage in the air domain in northeastern Europe.[11]

Vulnerabilities in the Defense of the Baltic States

Russia's local advantage in offensive and defensive air capabilities coupled with a lack of air defense assets in the inventories of the Baltic States creates vulnerabilities, both for the three states themselves and for NATO. In their own defense planning, the Baltic States assume that there may be a period in which the Alliance is unable to come to their assistance and during which only those forces present in the region will be able to fight. These include local forces, those of allies deployed under NATO's enhanced Forward Presence (eFP) and an occasional US rotational presence. During this "initial self-defense" period, mobilization would be vulnerable to disruption by attacks from the air (for Estonia, which retains conscription and relies on reserve forces to build its wartime force structure, this is a particular challenge). Defensive operations by maneuver forces would be frustrated. Key strategic assets, such as national capitals, communications and energy infrastructure, military locations, and command and control nodes would also be susceptible. Under such circumstances, analysts estimate that Russian forces could reach the outskirts of Riga or Tallinn in less than 60 hours.[12]

NATO's defense plan for the region, meanwhile, relies on large-scale reinforcement. This would be threatened by the destruction of air and sea ports of debarkation, and the vulnerability to air attacks on air, land and sea transport routes. Russia's air defenses, meanwhile, would frustrate allied offensive counter-air operations. The lack of effective air defense for the Baltic region is thus a critical

[8] "Russia's Western Military District to get four S-400 missile systems this year," *TASS*, January 13, 2017, http://tass.com/defense/924840; "Restoring the balance on NATO's Eastern flank," *Defense News*, May 17, 2017, https://www.defensenews.com/land/2017/05/17/restoring-the-balance-on-natos- eastern-flank-commentary/.

[9] 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.

[10] Välisluureamet, op. cit., 19.

[11] Sebastien Roblin, "Why Russia's Enemies Fear the Kalibr Cruise Missile: Moscow's 'Tomahawk'", *The National Interest*, 22 January, 2017, https://nationalinterest.org/blog/the-buzz/why-russias-enemies-fear-the-kalibr-cruise-missile-19129.

[12] David A. Shlapak, op. cit., 1.

weakness not only for the Baltic States themselves, but for NATO too.

Baltic Air-Defense Capabilities and Shortfalls

A contemporary integrated air-defense system brings together a range of offensive and defensive capabilities to deter, or prevent an enemy from employing its offensive air and missile weapons. In practical terms, it is a combination of sensors, weapons systems or effectors, and a command, control and communications network that connects the sensors and weapons, and conducts battle management functions. This sub-system level decomposition provides a convenient framework for describing and analyzing an air defense system.

For their primary air-defense sensors, Estonia, Latvia and Lithuania have invested in a network of long-range air-surveillance radars that cover their territories and are the basis for the generation, at air command-and-control nodes, of a Baltic Recognized Air Picture—an authoritative listing and identification of all aircraft in flight within a volume of airspace that supports the further tasking of air-defense sensor and weapons assets. While the air surveillance provided by these radars conforms to, and sometimes exceeds, NATO minimum military requirements, there are some gaps in coverage, in particular as concerns slow, low-level targets such as Unmanned Aerial Systems.[13]

In terms of weapon systems, Baltic capability is limited to (very) short-range ground-based systems. The main missile systems, the Raytheon-built Stinger (Latvia and Lithuania) and MBDA's Mistral (Estonia), are complemented by older systems such as the Saab RBS-70 and Polish Grom as well as some legacy anti-aircraft cannons. With missile ranges typically up to 5 km, these systems are useful only for point defense or the protection of small maneuver units. The organic sensor capabilities of these ground-based missile systems may also be used to supplement and fill gaps in the long-range surveillance network; in the Baltic case, however, they are usually operated in a standalone configuration and are linked to the wider integrated air defense system by procedural means only.

Lithuania has begun the procurement of two batteries of a more capable medium-range ground-based system, the Kongsberg Norwegian Advanced Surface to Air Missile System (NASAMS), which will allow targets to be engaged over a range of almost 25 km.[14] Estonia and Latvia also intend to acquire medium-range ground-based systems as funds allow, but have no programmed plans to do so at present. Meanwhile, the Baltic States do not possess or play permanent host to long-range air defense weapons systems such as the ground-based Patriot, sea-based systems such as Aegis, or fighter/ground-attack aircraft (the Baltic air policing and enhanced Baltic air policing missions are

[13] Joint Chiefs of Staff (US), *Countering Air and Missile Threats.* Joint Publication 3-01, 2017, 10-11, http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/.

[14] 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 30 July 2018; "Finland is updating its air defence systems", *Defense Industry Daily*, January 26, 2014, https://www.defenseindustrydaily.com/finland-updating-its-air-defense-systems-05398/.

not mandated for air defense). There is also virtually no prospect of them being able to afford such systems in the future. Baltic air defense capability is thus a long way from the military ideal of a layered system in which assets of varying capabilities are integrated to provide comprehensive defense of military forces, populations and critical infrastructure.

The Baltic command-and-control network, developed under a cooperation framework known as the Baltic Air Surveillance Network (BALTNET), comprises four command-and-control nodes connected to each other and to the NATO Integrated Air and Missile Defense System by secure communication links. The nodes—three Command and Reporting Posts at Ämari (Estonia), Lielvārde (Latvia) and Karmėlava (Lithuania) and a Combined Command and Reporting Center also at Karmėlava—are collectively responsible for the acquisition, coordination, distribution and display of air surveillance data within the three Baltic States, and also for limited air command and control.[15] While this configuration is sufficient to meet the demands of the Baltic air policing and enhanced Baltic air policing missions in peacetime, the communications network has insufficient redundancy to guarantee the high availability that would be needed to provide air command and control in a crisis. Similarly, the command-and-control nodes have insufficient trained personnel at each location—in particular fighter controllers, surface-to-air missile allocators and data link managers—to rotate battle management functions and ensure continuous operations during times of crisis. Finally, across the three states there is insufficient technical means (Link 16 terminals) to allow allied air defense assets deployed to the region to "plug and play" with the Baltic air command-and-control network. In summary, the command-and-control network provides for peacetime operations, but is insufficiently robust to support a NATO air defense posture in times of crisis.

Local Baltic capability is also supplemented on an occasional basis by the deployment and exercise of NATO and allied air-defense assets in the region. These include surveillance, command-and-control assets such as the NATO Airborne Warning and Control System and the NATO Deployable Air Command and Control Center, weapon systems such as Patriot and Rapier, and fighter aircraft. Notably, however, none of the eFP units located in the Baltic States have deployed with air defense assets.

Challenges in Developing Baltic Air Defense

Finance

The main obstacle to developing a common Baltic air defense is a financial one. Although in 2018 all three states will approach or exceed the NATO targets of spending 2 percent of their GDP on defense and 20 percent of their defense expenditure on equipment, the cash amounts available for building defense capability are still small. A key obstacle to enhancing Baltic air defense is thus the high cost

[15] Kaitsevägi (Estonian Defence Forces), "BALTNET", Kaitsevägi, accessed July 30, 2018, http://www.mil.ee/en/defence-forces/international-co-operation/baltnet.

of acquiring and operating the necessary systems. For an illustration of typical costs, Lithuania's 2017 acquisition of two NASAMS batteries, including training, additional equipment, logistical support and system integration was reported to have cost some €109 million ($123 million), while Sweden's contract with Raytheon to procure four Patriot systems is estimated to be worth almost €1 billion ($1.13 billion).[16] Neither figure includes costs of ownership and upkeep. The Baltic States will thus need to look to NATO and other allies for assistance if they are to develop a comprehensive air-defense architecture for their territories.

Interoperability and Cooperation

Given the high cost of developing an air defense system, the three Baltic States would realize considerable benefits through cooperation. In addition to saving resources through economies of scale, cooperative programs should: improve interoperability by taking advantage of, for example, common operating procedures and training; ensure that air defense is continuous over the territories of the three states, both technically and in policy terms (with the high speed of military operations in the air domain, the small territories of Estonia, Latvia and Lithuania, and their relative geographical isolation from the rest of the NATO European area, it makes great sense that their airspaces should be treated as a single volume); and earn greater support from other allies by adopting best practices promoted through NATO and EU programs such as smart defense and Permanent Structured Cooperation (PESCO).

When it comes to cooperation in air surveillance, command and control, at least, the Baltic States have a great deal of success to build on. They have developed, through the framework of BALTNET, a valuable arrangement which has encouraged habits and mindsets of cooperation among the three air forces. Notably, the Combined Command and Reporting Center at Karmėlava has been operated by personnel from all three states under rotational command since its creation in 2000. More widely, cooperation and interoperability in air surveillance, command and control are also encouraged by the standardization policies adopted by NATO, which have ensured the integration of BALTNET systems into the NATO Integrated Air and Missile Defense System. The adoption of common standards for tactical data links makes it relatively easy to integrate deployed or newly procured weapons systems into the local Baltic network. For example, although the Baltic States have acquired different short-range ground-based missile systems (Stinger and Mistral) these can both be integrated into the BALTNET air command and control network (although so far they have not been) using appropriate data exchange standards and protocols.

Interoperability in air defense, however, is less a technical challenge than it is a policy and political

[16] Hughes, "Lithuania, Indonesia Sign for NASAMS"; "Sweden set to close $1 billion Patriot missile deal," *Reuters*, May 30, 2018, https://www.reuters.com/article/us-sweden-defense-raytheon/sweden-set-to-close-1-billion-patriot-missile-dealidUSKCN1IV1MM.

one. Generally speaking, defense cooperation in Europe has proved challenging and the results have fallen far short of what would be necessary to address Europe's military credibility problems.[17] The Baltic States, on the surface natural partners, have also struggled to work together, despite successive sets of defense ministers declaring their support for Baltic defense cooperation.[18] Since joining NATO in 2004, defense cooperation has suffered due to competition and a lack of trust between the three states. This period has seen little fresh defense cooperation, certainly by comparison with the preceding period during which the prospect of NATO membership and the support and practical assistance of other states encouraged Estonia, Latvia and Lithuania to create the flagship projects, alongside BALTNET, of the Baltic Peacekeeping Battalion, Baltic Naval Squadron and Baltic Defense College. Even cooperation in BALTNET has been occasionally fragile—the project came close to failure in the late 1990s following a bitter dispute about the number and location of command and control nodes.[19] Baltic defense cooperation, then, while offering great benefits to the development of an air defense system, cannot be taken for granted. It will require renewed political leadership and courage.

Strengthening Air Defense in the Baltic States

The air-defense challenge in the Baltic States is formidable and its solution is beyond the reach of the Baltic States alone. Progress can only be made if the Baltic States and the rest of NATO take a shared, coherent approach to enhancing air defense and deterrence in the Baltic region. This is in the Alliance's interests, too, as its defense plans for the Baltic region—upon which its credibility partly rests—can be thwarted by an adversary determined to exploit local weaknesses. While air-defense shortfalls cannot reasonably be addressed by the Baltic States alone, NATO collectively, or the allies individually, they should thus be ready to take actions to enhance air defense and deterrence in the region. Also, given the geography of the region, NATO's Enhanced Operational Partners Finland and Sweden should also consider supporting Baltic efforts to strengthen air defense and deterrence in the region.

[17] Christian Mölling, Marie-Louise Chagnaud, Torben Schütz and Alicia von Voss, "Working Paper FG3-WP No 01", *European Defence Monitoring,* (Berlin: Stiftung Wissenschaft und Politik, 2014), 4, https://www.swpberlin.org/fileadmin/contents/products/arbeitspapiere/WP_EuropeanDefenceMonitoring_Jan2014.pdf . For a good overview of the difficulties of European defence cooperation see also: Dick Zandee, Margriet Drent, and Rob Hendricks, *Defence Cooperation Models. Lessons Learned and Usability* (The Hague: Clingendael, 2016), 38-47 (available from https://www.clingendael.nl/publication/defence-cooperation-models, accessed 1 August 2018).

[18] Pete Ito, "Baltic Military Cooperative Projects: A Record of Success," in *Apprenticeship, Partnership, Membership: Twenty Years of Defence Development in the Baltic States*, ed. Tony Lawrence and Tomas Jermalavičius (Tallinn: International Centre for Defence Studies, 2013), 264-6, https://icds.ee/apprenticeship-partnership-membership-twentyyears-of-defence-development-in-the-baltic-states/

[19] Uģis Romanovs and Māris Andžāns, "The Trilateral Military Cooperation of the Baltic States in the 'New Normal' Security Landscape," in *Security in the Baltic Sea Region: Realities and Prospects: The Rīga Conference Papers 2017*, ed. Andris Sprūds and Māris Andžāns (Riga: Latvian Institute of International Affairs, 2017), 17, http://liia.lv/en/publications/security-in-the-baltic-sea-region-realities-and-prospects-the-riga-conference-papers-2017643

The Baltic States

Modern air-defense systems make use of air command-and-control capability (a combination of information technology and personnel serving in a variety of roles) to integrate and more effectively and efficiently manage sensors and weapons against a range of targets. Command and control is thus a force multiplier, and a robust command-and-control network is the mainstay of an operational air-defense architecture. As a priority, the Baltic States should focus on enhancing the air surveillance, command-and-control network they have developed under BALTNET, both to improve their own abilities to conduct air-defense operations before and during a crisis, and to ensure that Allied air-defense assets deployed to or exercising in the region can integrate smoothly into local air command and control. The three Baltic air force chiefs have recently agreed to develop a BALTNET Future Configuration, which will go some way to addressing the shortfalls. Enhancing a command-and-control arrangement is, however, rarely interesting to decision makers and publics, especially when compared to major hardware procurements Even so, it is important that this project continues to receive the attention and level of political support it deserves.

Action is needed in two broad areas. First, redundancy is needed in the communications networks that connect Baltic command-and-control nodes, both within Baltic territory and to the outside world. Where single links exist, they should be duplicated, while additional routes should be created to ensure that the network can continue to function even if some links are non-functional (e.g. through technical failure or deliberate attack by an adversary). This can be achieved relatively inexpensively, and the Baltic States may be able to call on funding from the NATO Security Investment Program to assist.

Second, command-and-control capability needs to be enhanced, both through the introduction of technical upgrades and through the recruitment and training of personnel. The goal of these measures would be to create command and reporting centers in the three states, each capable of assuming battle management roles on a continuous (but rotational) basis, thus ensuring the functioning of Baltic air command and control even if some locations were unavailable. The necessary technical upgrades essentially amount to the provision of Link 16 capability at Lielvārde and the acquisition of a number of Link 16 terminals to accommodate Allied air-defense assets deployed to the region. More challenging will be the recruitment and training to NATO standards of the personnel required for 24/7 operations at each site. The Baltic States may wish to consider unconventional staffing solutions, perhaps using civilian personnel, or building on Estonia's experience of creating a voluntary Cyber Defense Unit.[20]

Training, and the retention of currency in certain air command-and-control roles, can be partly

[20] Sharon L. Cardash, Frank J. Cilluffo and Rain Ottis, "Estonia's Cyber Defence League: A Model for the United States?" *Studies in Conflict & Terrorism*, 36:9 (2013): 777–787.

accomplished using simulation. In particular, so-called blended live, virtual and constructive training, in which operators are tested against a range of simulated targets using a combination of real and simulated systems and fellow operators, seems to offer promise.[21] As the Baltic States decentralize their air command-and-control operations, it will be important—since Baltic airspace would continue to be treated as a single volume—that they work together to develop a common training plan and conduct common training events.

With measures to enhance air surveillance as well as command and control either programmed or implemented, it will make sense for the Baltic States to invest in additional air-defense weapons systems. As an immediate priority, existing short-range ground-based systems need to be fully integrated into the Baltic air command and control network. Otherwise, friendly aircraft operations will be constrained by a need to keep away from areas in which Baltic air-defense assets might be operating. Air-defense weapons coverage can then be enlarged by the acquisition of medium-range ground-based systems, allowing local area defense, rather than the point defense currently possible. Lithuania has already taken the lead in this area with its acquisition of two NASAMS batteries. This will be an expensive venture, and it may be necessary for the three states to re-evaluate their current force development priorities. High costs could, however, be partly offset through Baltic cooperation. The three states should commit themselves to the greatest extent possible to common acquisition, maintenance, logistics support and training (e.g. the creation of a single air-defense school). It may also be possible to secure US financial assistance in, for example, acquiring US manufactured missiles. Opportunities for doing so through the European Deterrence Initiative or other US support programs should be explored.[22]

These recommendations require a substantial level of Baltic defense cooperation which is a potentially risky proposition. In order to maximize the chances of success, the three states should consider building upon the BALTNET framework to develop a new cooperation mechanism, reminiscent of those successfully established and operated with Nordic support in the 1990s, to manage cooperation across the board in air defense.[23]

NATO

The Baltic States, then, should be able to strengthen their air surveillance, command and control and, in the slightly longer term, field a number of short- and medium-range ground-based weapons systems. But this will still fall short of the layered, integrated air-and-missile-defense system they will need to confidently defend their airspace. Building this will require assistance from NATO and

[21] NATO, Centre of Excellence for Operations in Confined and Shallow Waters, "Initial NATO LVC-T Demonstration," http://www.coecsw.org/our-work/spotlights/initial-nato-lvc-t-demonstration/, accessed 2 August 2018.

[22] The White House, "President Donald J. Trump's Support for Estonia, Latvia, and Lithuania," April 3, 2018, https://www.whitehouse.gov/briefings-statements/president-donald-j-trumps-support-estonia-latvia-lithuania/.

[23] Ito, "Baltic Military Cooperative Projects," 246–247.

individual allies. NATO and the other allies cannot be expected to simply supply the Baltic States with air defense assets, nor is it reasonable to believe, in the current political climate, that allies will be ready to deploy such assets to the Baltic region on a long-term basis. Nonetheless, there is much that the Alliance can do—in exercising, in short-term deployments and in policy formulation—to demonstrate its readiness to support air defense in the Baltic region should the security situation deteriorate. Bringing more capable air-defense assets into the Baltic region for exercising and short-term deployments not only trains deploying and local forces, but also conveys an important message of deterrence.

In air surveillance command and control, NATO should continue to operate the Airborne Warning and Control System and other Allied air surveillance assets in and around the Baltic region. Similarly, the Deployable Air Command and Control Center, a NATO organization based in Northern Italy that would supplement local air command and control in times of crisis, should continue to exercise its component parts in the Baltic States, as it did most recently during exercise Ramstein Dust II, in 2017.[24] NATO's own command-and-control procedures also need some attention. In particular, the Supreme Allied Commander should be given the ability to mobilize the Joint Force Air Component without the prior authorization of NATO's political authorities. This component, which would provide air command and control at the NATO level in times of crisis, exists only as a skeleton in peacetime and takes some (potentially highly critical) days to be brought up to full strength. Authorizing the Supreme Allied Commander to bring the Joint Force Air Component up to strength of his own volition would bring his authorities in the air domain into line with those he already holds in the land domain, where he can unilaterally alert, prepare and stage the Very High Readiness Joint Task Force.[25] As Baltic air command and control is strengthened to permit crisis-time operations, NATO should also consider putting its air policing mission and enhanced air policing missions on an air-defense footing.[26]

While command-and-control assets are essential for effective air defense, their presence is less visible (and arguably, therefore, their deterrent effect less) than that of weapon systems. NATO and the other allies should also step up the exercising of longer-range air-defense weapons systems to Estonia, Latvia and Lithuania—particulary if Baltic air command and control is enhanced so such assets can readily "plug and play" with local systems. Patriot batteries, for example, have been present in the region only twice, including once to participate in a military parade in Estonia.[27] In addition

[24] NATO, Allied Air Command, "Italian radar element supports NATO deployable air surveillance unit," Allied Air Command, September 20, 2017, https://ac.nato.int/archive/2017/italian-radar-element-supports-nato-deployable-air-surveillance.

[25] Klaus Olshausen, "NATO's Readiness Action Plan for Assurance and Deterrence – Progress & Challenges on the Road from Wales to Warsaw," *ISPSW Strategy Series*, no. 402, January 2016, 3, http://www.ispsw.com/en/publications/.

[26] Breedlove, op. cit., 5.

[27] "U.S. deploys advanced anti-aircraft missiles in Baltics for first time," *Reuters*, July 10, 2017,

to exercises, it would be helpful if ground-based air-defense units were deployed to the Baltic States for longer periods, for example alongside the eFP battalions or through the US European Deterrence Initiative. NATO should also step up its exercising of fighter aircraft in the region. Not only are fighters a key air-defense asset, but they are vital for the training of fighter allocator personnel in air command-and-control nodes; without fighters to train with, the task of bringing Baltic air command-and-control capability to a level at which it can support an air-defense posture will be considerably more challenging.

Finally, in addition to exercising individual capabilities, NATO should also plan and exercise in a more comprehensive manner the step-by-step transition from peacetime air policing to a Baltic air-defense posture in times of crisis. This should include actions such as deploying NATO air command-and-control capabilities, increasing Airborne Warning and Control System sorties, deploying long-range air-defense missile systems and additional fighter capability to the region, and increasing fighter operating locations.[28]

Finland and Sweden

While not members of NATO, it is inevitable that Finnish and Swedish air defenses be activated in the event of a Baltic crisis. At the very least, Finland and Sweden would need to be ready to respond to incursions into their airspace that stem from the lack of strategic depth of the Baltic States. In these circumstances, Finland and Sweden on the one hand, and NATO on the other, will share similar goals for air defense, and each will benefit from cooperation.

At present, limited arrangements, justified on the basis of flight safety, permit the exchange of air-surveillance data between Finland, Sweden and NATO. In a crisis, a fuller exchange of data will be in the interests of both parties, but this is not something that can be achieved without prior planning and rehearsal. Finnish and Swedish sensitivities make this difficult; nonetheless, NATO should pursue appropriate information exchange arrangements with Finland and Sweden, to be activated on a dual-key basis, and regularly exercised.

Conclusions

The most worrying gap in military capabilities in the Baltic region is in air defense. The limited capabilities possessed by the three Baltic States for air command and control are adequate for the

https://uk.reuters.com/article/uk-usa-baltics-patriot/u-s-deploys-advanced-anti-aircraft-missiles-in-baltics-for-first-timeidUKKBN19V286; Dario Cavegn, “Defense minister: Bringing Patriot system to Estonia a symbolic move,” *ERR News*, February 23, 2018, https://news.err.ee/685484/defense-minister-bringing-patriot-system-to-estonia-asymbolic-move.

[28] 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, https://www.japcc.org/portfolio/airpowerafterwarsaw/, accessed on July 12, 2018.

peacetime air policing and enhanced air policing missions, but fall far short of being able to support a robust NATO air-defense posture in times of crisis. Estonia, Latvia and Lithuania also possess air-defense weapons that can provide only modest coverage of their territories. As a result, the three states themselves would be vulnerable in times of crisis. Furthermore, reinforcement routes on land and sea and in the air would be at risk, threatening the ability of allies to come to the aid of the Baltic region, thus undermining the credibility of NATO itself. Addressing the air-defense gap is essential for the security of the Baltic States, but also for the security of NATO as a whole.

Financial considerations will prevent the Baltic States from addressing air-defense shortfalls alone. They can, however, by enhancing air surveillance as well as command and control, ensure that they have the ability to support a robust NATO air defense posture in times of crisis, and the ability to exercise such a posture during peacetime. There are also steps they can take to enhance ground-based air-defense coverage. For its part, NATO can take measures to improve its readiness to contribute to air defense of the Baltic region, by exercising and deploying assets and by adopting appropriate policy changes. To maximize the chances of success, Estonia, Latvia and Lithuania will also need to improve cooperation among themselves, both to achieve material benefits and to demonstrate to the rest of the Alliance that their efforts should be supported. Baltic-wide solutions, in conjunction with active backing from NATO and other Allies can substantially increase deterrence and air defense in the Baltic region.

Challenges in Developing Common Cyber Defense

Edgars Poga

Introduction

In the crucial domain of cybersecurity, the three Baltic States have significantly diverging capabilities due to the lack of common educational approaches and, most crucially, limited state capacity. Estonia, thanks to its extensive efforts at researching and contributing to the securitization of the cyber domain, has advanced the furthest not only within the Baltic region but globally as well. Sharing its expertise with Latvian and Lithuanian cyber authorities can help to further develop their systems, but for now the gap remains. It is important to point out that because of how different the cyber domain is from the physical domains of warfare on land, in the air, or at sea, actors can significantly improve their offensive and defensive capabilities within a matter of months rather than years. This means that the Baltic States may be able to reach a similar level of capabilities within a relatively short period of time.

Currently, intra-regional cooperation is lacking both institutionally and practically, however. Cooperation with think tanks, tech startups, and other related groups will need to be considered and utilized to improve this structure. More intensive Baltic cooperation on cybersecurity awareness, training and exercise initiatives is, therefore, one of the most important tasks for the upcoming years within the cybersecurity domain. Thus, determining the existing challenges and possible solutions that would enhance intra-regional cooperation would serve as the building blocks for a common Baltic cyber defense environment. In order to clarify, the following chapter will firstly explicate the current challenges to intra-regional cooperation within the domain of cybersecurity, which will then be exemplified by the cooperation of the Baltic States within cyber-defense live-fire exercises. Secondly, after determining the areas where challenges are most prominent, specific types of challenges shall be identified—for instance, physical Internet infrastructure and its protection, legacy infrastructure and also general limitations to cooperation. Finally, the analysis and recommendations will be summarized, providing for possible further actions toward the goal of developing common cyber defense within the Baltic region.

Intra-Regional Approaches to Cybersecurity

The intra-regional approaches to cybersecurity have varied throughout the years as the Baltic States have enhanced their cyber defense capabilities. Therefore, the situation calls for a deeper analysis of the gradual development of cooperation within the cyber domain on the basis of a framework established by the North Atlantic Treaty Organization's Cooperative Cyber Defense Center of

Excellence (NATO CCD COE). That cooperative framework has enabled Alliance-wide exercises, academic research and various initiatives.

The NATO CCD COE has persuasively shown that the cyber domain hinges on multiple areas of interdependence not only among the Baltic States themselves, but within the wider North Atlantic Alliance as well. Hence, from its consciously chosen location in Tallinn, the CCD COE is tasked with not only examining the global scale of cyber domain processes but also assesses the possibilities for intra-regional cooperation within the cyber realm.[1] A prime example of cooperative measures is the popular, annually hosted live-fire exercise Locked Shields (examined in more detail below), which initially tackled cybersecurity in the Baltic region. However, within the original exercises up until 2014, the only two main regional contributors were representatives of concerned institutions from Sweden and Estonia.[2] This suggests that, from the very beginning of the exercise, neither Lithuanian nor Latvian institutions had the necessary capacity or capability to take part, due to the novelty of the domain. In turn, this negatively impacted the willingness of Latvian and Lithuanian policymakers to increase investment. The countries were also in the process of recovering from the 2008 financial crisis. This highlights the core divergence among the Baltic countries—Estonia chose to pay closer attention to the issue, since it experienced attacks in 2007; the other two Baltic States did not.

In contrast to Estonia, Latvia and Lithuania have been relatively slower in developing their own cyber capabilities. The first cybersecurity strategy for Latvia was adopted only in 2014[3]; and Lithuania followed with the Cyber Security Act[4] that same year. Thus, at its inception, in 2008, the NATO CCD COE lacked the actors to provide a truly effective role in the development of an intra-regional cybersecurity partnership. However, a positive attribute, especially within the national cybersecurity strategies of Latvia and Lithuania, is the fact that, both in the previous iterations and those published more recently, collaboration between the Baltic States has been established as one of the priority areas of cooperation alongside NATO and the EU. Moreover, the commitment to Baltic cooperation with regard to further development of the domain can prove to be a crucial factor in facilitating intra-regional support as capacities and capabilities are on the rise for both Latvian and Lithuanian cyber defense forces due to the 2 percent pledge to NATO.

In terms of the current status quo, regional best practices tend to be acquired based on joint exercises. Cyberspace, which NATO deemed a domain of operations in the 2016 Warsaw Summit, lends itself to a much different exercise methodology than traditional military exercises on land, in the sea or in

[1] Libicki, Martin, "For a Baltic Cyberspace Alliance?" *NATO CCD COE CyCon Conference*, https://ccdcoe.org/uploads/2019/06/Art_01_For-a-Baltic-Cyberspace-Alliance.pdf.

[2] NATO Cooperative Cyber Defence (CCD) Centre of Excellence (COE), “Estonian-Swedish Cyber Defence Exercise Conducted,” https://ccdcoe.org/estonian-swedish-cyber-defence-exercise-conducted.html.

[3] Ministry of Defense of the Republic of Latvia, “NATIONAL CYBERSECURITY STRATEGY 2014-2018,” https://www.unodc.org/res/cld/lessons-learned/lva/latvijas_kiberdrobas_stratija_html/Kiberdrosibas_strategija.pdf.

[4] Ministry of National Defense Republic of Lithuania, “Cyber security strategy,” https://ccdcoe.org/sites/default/files/strategy/LTU_CSAct_lt.pdf.

the air. In other words, cyberspace exercises are more of an information-sharing platform for technicians and government representatives to be able to more effectively address their national cyber domains and improve general threat-prevention practices. These include domestic exercises carried out by state institutions such as Computer Emergency Response Teams (CERT) to test and update systems. These practices can extend to live-fire exercises such as Locked Shields, organized by the NATO CCD COE. The aim of these procedures is to define the possible weak points of national CERT responses as well as provide a platform for sharing information and expertise. Two main forms of penetration testing (pentest) exist. The first is digital pentesting, in which operators trying to breach systems are actively countered by operators who aim to defend them or react in case of a breach; and the second, physical pentesting, involves professionals trying to gain access to protected data through physical systems with the aim to find the possible routes that an adversary could exploit to gain access to sensitive information. Currently, the focus largely remains on the digital form of pentesting, which, as cybersecurity professionals point out, underemphasizes the physical portion of cybersecurity. Instead, it is advisable to carry out not only data-protection trials, but also physical tests in order to achieve a more resilient cyber domain.

It is vital to assess the impact of the involvement of the Baltic States in the NATO CCD COE in order to recognize the ways in which the lessons learned from exercises such as Locked Shields have been implemented nationally as well as to conclude how this has shaped intra-regional cooperation.

Firstly, for Latvia, cooperation in this space has greatly impacted the operational capabilities and different methodologies for the Strategic Communications (STRATCOM) COE, located in Riga. It has provided direct expertise and strategies on handling disinformation and manipulation of algorithms within social media platforms from a technical perspective of information communication technology (ICT). In turn, this has provided an informational basis for the Ministry of Defense's national whole-of-society defensive approach. The system directly approaches strategic communications and was built on the findings of NATO STRATCOM COE through case studies and publications.

Secondly, Lithuania, has used information provided by the Energy Security Center of Excellence (ENSEC COE) to create a project that evaluates cyber risks concerning the operation of the Central Europe Pipeline System (CEPS) and has proposed recommendations on improving the safety and availability of CEPS. The scope of the study is focused on the aspects of cybersecurity relevant to the operational technology typically used in attacks, allowing Lithuania to acquire the necessary knowledge regarding energy security.

Finally, Estonia has not only created an organizational structure capable of rapid response to attacks, but, notably, it has modified its legal framework, requiring all vital services to maintain a minimal level of operation if they have been cut off from the Internet. The measures taken by Estonia have established it as the highest-ranked European country when it comes to cybersecurity.[5]

In conclusion, the NATO CCD COE has had a considerable amount of intra-regional impact on the approaches taken by the governments of the Baltic States. Each of the states have adopted lessons from the CCD COE findings published in technical, legal and policy research—focusing on strategic communications in Latvia, energy security in Lithuania or infrastructure stability and legal frameworks for Estonia. Whilst positive impacts can be recognized in each country, the challenges for Baltic State cooperation remain prevalent with regard to taking action. This shows the necessity to assess previous experiences within live-fire exercises, which foster knowledge about the required steps forward to ensure development of a common cyber defense.

Challenges to Foster Intra-Regional Cooperation Within Live Fire Exercises

Last year's Locked Shields multinational cyber exercise, organized by the NATO CCD COE, provided many important lessons and experiences to all involved. The first cyber exercise in the region was Baltic Shield 2008, specifically aimed at fostering regional security. The only major participants were Sweden and Estonia.[6] This was either due to unwillingness on part of other allies or their inability to provide the required officials at the time. But since then, the exercise, which has evolved into the annual Locked Shields, stresses the development of cybersecurity measures for all of NATO.[7] At the same time, the tradition of intra-regional cooperation has been continuously fostered by the Baltic States, which endorse blue team efforts in exercises, a prime example of which was the joint team of Latvia and Lithuania in 2015.[8]

Lithuania participated for the first time in 2012,[9] while Latvian representatives joined only in 2014.[10] Therefore, the cooperation efforts in cybersecurity exercises are still quite recent. In 2015, the joint Latvian-Lithuanian team clearly signaled the possibility of interoperability of the national cyber emergency teams within the Baltic region.

[5] International Telecommunications Union, "Global Cybersecurity Index (GCI) 2017," https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

[6] NATO CCD COE, "Estonian-Swedish Cyber Defence Exercise Conducted," accessed on November 10, 2018, https://ccdcoe.org/estonian-swedish-cyber-defence-exercise-conducted.html.

[7] NATO CCD COE, "Locked Shields 2012," https://ccdcoe.org/locked-shields-2012.html.

[8] CERT.LV, "Latvijas-Lietuvas komandai 4.vieta kiberdrošības mācībās 'Locked shields 2015,' " (in Latvian), accessed on November 4, 2018, https://www.cert.lv/lv/2015/04/latvijas-lietuvas-komandai-4-vieta-kiberdrosibas-macibas-locked-shields-2015.

[9] NATO CCD COE, "Locked Shields 2012," accessed on November 4, 2018, https://ccdcoe.org/locked-shields-2012.html.

[10] NATO CCD COE, "International Cyber Defence Exercise Locked Shields 2014 Begins Today," accessed on November 4, 2018, https://ccdcoe.org/international-cyber-defence-exercise-locked-shields-2014-begins-today-0.html.

A majority of the takeaways regarding Locked Shields 2018 have to be drawn from the evaluation of the tasks of the blue teams, which tackled the protection of critical infrastructure during the crisis simulation.[11] In said exercise, the teams had difficulties filtering malicious traffic in the provided Internet Protocol Version 6 (IPv6) and protecting custom web applications. Furthermore, the blue teams had difficulties with "sharing actionable information with each other and writing good situation reports under serious time pressure." [12] This highlights brittle communication and cooperation during a crisis situation, thus opening the possibilities for a spillover effect if one of the three Baltic countries were to come under a real cyber threat.

While undoubtedly valuable, analysis of the CCD COE's yearly Locked Shields reports is seriously hampered by the fact that only years 2012–2014 are accessible publicly. Locked Shields 2015 was kept covert following the inclusion of additional experts and participating states. These changes required new policies for sharing information about state practices on cybersecurity. As noted above, if these practices are being kept classified, it prohibits state institutions from coming under the scrutiny of academics and private-sector professionals, resulting in less efficient public spending and policymaking regarding domestic and intra-regional cybersecurity activities. Concerning the Baltic States, transparency is required as the gap in knowledge—the lack of understanding by both public officials and the leaderships of the critical infrastructure companies under threat—remains prevalent. Such a report would allow for condensed and simplified technical information to be distributed to the general public as well as policymakers, increasing cyber hygiene and societal resilience to cyber threats.

While it is important to underline the general argument that national security rests on the ability to protect sensitive information, a report in the form of a general analysis compiled from reports of individual state security institutions would be sufficient to provide an outlook on attack vectors, different trends in hacking techniques as well as recently used malware. This would, in turn, allow for academic discussion and further analysis based on evidence provided by Baltic State governments rather than leaks of classified information. Currently, Baltic State cyber-defense institutions create annual or quarterly reports of incidents based on information gathered in their respective countries, but a joint report would allow for work on analysis of interdependencies and foster joint steps toward a common understanding of possible further developments within the cyber-defense domain.

Once the data and experience from live-fire exercises have been assessed, areas of attention can be problematized in order to tackle the current challenges and find possible solutions with intra-regional cooperation in mind.

[11] The exercises are structured so the two main teams, Blue Team (defenders) and Red Team (attackers), carry out different malicious cyber activities.

[12] NATO CCD COE, "Locked Shields 2014 After Action Report Executive Summary," accessed on November 10, 2018, https://ccdcoe.org/sites/default/files/multimedia/pdf/LS14_After_Action_Report_Executive_Summary.pdf.

Physical ICT Infrastructure and Its Protection

In each of the three Baltic States, physical Internet infrastructure is mainly secured by private organizations, with maintenance and check-ups being carried out by state authorities. Jani Antikainen, the chairperson of the board of Sparta Consulting & Huginn, points out that the security of the current physical network in the Baltic States is quite underdeveloped, allowing for physical acts to have a massive impact on the overall infrastructure. Thus, as spending on cybersecurity increases, it would be strongly advisable to not only invest in data protection but also in the physical protection of data transmitters. Increased security standards in regard to persons who have physical access to parts of infrastructure as well as inclusion of physical penetration tests within exercises are also of high importance to state security. Notably, the Stuxnet virus exploited physical weaknesses in systems to spread and cause considerable damage.

Therefore, the Baltic State governments could actively practice a "bottom–up" approach, involving both domestic and intra-regional parties and state institutions in joint exercises. The main goal of these exercises should be to secure physical Internet infrastructure as well as carry out pentesting on public networks and public critical infrastructure such as hospitals, telecommunications networks and banks. This particular aspect of cooperation would provide governments with not only the capability to outsource help while under threat from attacks on public infrastructure but also ensure protection against cyberattacks for the contractors working for the state, allowing them to retain classified information. Furthermore, mutual support could prevent incidents such as the recent attacks against Russia, in which a Federal Security Service (FSB) contractor was hacked and large amounts of data on state projects and initiatives were released to the public.[13]

Intra-regional preparation, rehearsal events and wide-scale assessment would truly challenge the capacity of the three Baltic States' institutions. The task would be even greater under their preexisting obligations toward cybersecurity initiatives such as regulations and directives stemming from the European Union's General Data Protection Regulation (GDPR) and the EU Network and Information Security (NIS) directive—not to mention the ever-increasing amount of exercises organized by NATO, such as Locked Shields, CMX and Crossed Swords.

Finally, cyber exercises to date have primarily focused on data protection during crisis situations; whereas, core physical infrastructure, upon which telecommunication and energy distribution networks rely, have only recently been included within live-fire exercises. Consequently, in order to achieve necessary cohesion within the cyber domain and prevent possible spillover of damage in interconnected areas, the Baltic States will need to focus on intra-regional cooperation. This would involve data protection measures as well as building more resilient ICT systems that constitute

[13] Doffman, Zak. "Russia's Secret Intelligence Agency Hacked: 'Largest Data Breach in Its History,' " *Forbes*, https://www.forbes.com/sites/zakdoffman/2019/07/20/russian-intelligence-has-been-hacked-with-social-media-and-tor-projects-exposed/#1779543e6b11.

physical infrastructure. To do this, it is necessary to build upon the data provided by NATO CCD COE exercises and regional initiatives.

The arguments in favor of the necessity of increased physical protection of critical infrastructure systems, similar to those that emphasize the need to accommodate and provide operators for initiatives outside NATO and the EU, can be approached in the following ways.

First, the "international umbrella" approach can be employed to include cyber-defense attributes within other joint exercises. For example, this was done with regard to pentesting in the NATO exercise Trident Juncture,[14] which focuses on testing the Alliance's capabilities in an Article 5 scenario. The annual exercise covers cyber defense, as well as sea, land and air situations. However, going forward, Trident Juncture could be extended to include rapid-reaction CERT teams tasked with dealing with physical threats to infrastructure. The inclusion of national CERT teams in this way would allow them to gather experience from real-life situations while considering guidance from the international strategic standpoint of NATO and the EU. This would move participating countries closer to an already-established cyber troops concept employed in the United States.[15]

Second, regarding the cooperation of private and state organizations, the example of cooperation in pentesting can be utilized. For example, the telecommunication providers Tet in Latvia, Telset in Estonia and Splius in Lithuania could participate in joint drills with the CERTs of the Baltic States and even utilize the special training environment popularized by IBM in Tallinn.[16] This would serve to not only contribute to the protection of physical infrastructure but also to establishing common practices among specialists in the region.

In conclusion, not only could the Baltic States make use of various pre-existing platforms created by international organizations to better cooperate within exercises, but there are also opportunities to approach the regional industry with security of critical infrastructure in mind. This provides the basis for the whole-of-society approach toward training that is necessary to enhance the physical security of ICT infrastructure.

Vulnerability of Legacy Infrastructure

Rapid technological advance can result in spillover of threats or vulnerabilities if the new systems are not regularly updated, repaired and secured (both physically and technically from possible viruses). This implies that the problems created by lack of proper testing in conjunction with vulnerabilities such as outdated hardware, lack of operators and uneducated staff pose considerable threats to state

[14] North Atlantic Treaty Organization, "Trident Juncture 18," https://www.nato.int/cps/en/natohq/news_158620.htm.

[15] U.S. Cyber Command, "USCYBERCOM," https://www.cybercom.mil/.

[16] IBM, "Train with the world's premier cyber special forces team," https://www.ibm.com/security/services/managed-security-services/security-operations-centers.

security. However, in terms of the impact, in the context of cross-border dependencies, three key sectors are singled out: energy, banking and telecommunications. Together these three create an attack plane that could cause the assailant to impact not only local, but also systems in other countries.

It is worth mentioning a number of fairly recent attacks that crippled energy infrastructure in Estonia (2007),[17] Iran (2010),[18] Saudi Arabia (Aramco—2012),[19] and Ukraine (power plant—2014).[20] Common to all of these examples is the fact that they were sponsored by foreign states, highlighting the criticality of the protection of these systems. The current process of protection is managed through Transmission System Operators (TSO). The current version of exchange of TSOs provides an environment for quick identification and mitigation of security disturbances and challenges in the online environment. But it lacks informational collaboration with state CERTs, thus forcing them to singlehandedly tackle problems that could otherwise be handled cooperatively.

Therefore, regarding the energy sector, close cooperation between the three Baltic States' energy companies is strongly advised. This could be done by active pentesting of both physical attributes of data storage devices and critical electronic information-sharing devices within the energy bases. Development of real time visualization of data flow would allow efficient monitoring for malicious activity or data alteration. State-backed exercises are also recommended.

The second type of infrastructure with potential security vulnerabilities is the banking sector. Banks are targeted both by non-state actors motivated by financial gain as well as state actors aiming to more broadly destabilize society. Exacerbating the threat is the interconnected nature of the banking sector and its impact on the regional economy. Although there are examples, such as the Bangladesh heist, where a state-sponsored group was the main adversary,[21] attacks in this area are mainly conducted by non-state actors for whom the primary interest is not to raise havoc or achieve a political goal but rather to gain financial benefits. Thus, if the economic sector of a country is vulnerable, lack of cross-border cooperation allows a malicious actor to execute the same attack in neighboring countries' associated banks. Institutions can also be directly affected on the basis of malware crossing over and disrupting operations and/or blocking access to information. This was precisely the scenario created by the infamous NotPetya malware, which was promulgated by the Russian military cyber unit and

[17] International Journal of Cyber Warfare and Terrorism (IJCWT), "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security," https://www.igi-global.com/article/estonia-after-2007-cyber-attacks/61328.

[18] Marco De Falco, "Stuxnet Facts Report. A Technical and Strategic Analysis," NATO CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf.

[19] Nicole Perlroth, Krauss Clifford, "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *The New York Times*, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html.

[20] Kenneth Geers, "Cyber war in perspective: Russian aggression against Ukraine," NATO CCD COE. https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf.

[21] Hammer, Joshua. "The Billion-Dollar Bank Job," *The New York Times*, May 23, 2018, https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.

had an impact on a wide range of international actors, resulting in up to $10 billion in damages worldwide.[22]

The third type, which is associated with the rise of the 5G debate, highlights the future importance of data security and critical infrastructure impacted by telecommunications. It requires a sustainable and cautious policy approach taken by the Baltic governments regarding supply chain security. The policy approach needs to focus on interoperability of networks as well as minimizing the spillover effect in case of an attack. Thus, developing a coordinated intra-regional approach will be essential in maintaining stability of critical infrastructure in the telecommunications environment of the future.

As to how the Baltic States governments can work together to address regional spillover effects more proactively: the governments have the possibility to individually maintain their national infrastructure by actively conducting pentests on possible spillover areas as well as participate in live-fire exercises hosted by NATO and the EU. Cooperation with the energy sector to educate and prepare operators of electric-grid systems to enhance cyber hygiene as well as situational awareness of possible threats to critical infrastructure is essential for the security of the state.

Internal Limitations to Cooperation

To begin with, one of the major problems hampering closer intra-regional cooperation in the cybersecurity realm is the covert aspect of cyber operations—specifically within the context of information sharing.[23] Joint approaches could lead to a necessary evaluation of the capabilities of defense systems within the Baltic States, allowing for effective updates and patches of vulnerabilities on the basis of expertise provided by allies. When assessing institutional differences, the legal aspect of the cooperation between the three countries shows the necessity to harmonize approaches to different regulations within the cybersecurity domain.[24] The prime example, as noted above, is the EU's network and information systems directive, or NIS, which, in essence, requires member states to move toward a more harmonized legal basis of actions within the sectors associated with the ICT industry.[25]

On this basis, an argument of fragmentation must be made. As opposed to having a multilayered approach, like that of the United Kingdom, the Baltic States struggle with the question of "who does

[22] Andy Greenberg, "The Untold Story of Notpetya, the Most Devastating Cyberattack in History, *WIRED*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[23] Herb Lin, "Fundamentals of Cyber Conflict," Stanford University, https://seclab.stanford.edu/courses/cs203spring2017/lectures/lin.pdf.

[24] Anna-Maria Osula and Henry Rõigas, "International Cyber Norms Legal, Policy & Industry Perspectives," NATO CCD COE, https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf.

[25] European Commission, "The Directive on security of network and information systems (NIS Directive)," https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

what" internally.[26] This means that there are multiple institutions in charge of different cybersecurity fields and, hence, no common approach to policy creation and mitigation of cross-border vulnerabilities. Instead, there are different approaches to the same problem within a single country.

Latvia exemplifies this issue most noticeably. Three separate Latvian institutions are charged with dealing with cybersecurity for the state. First is the Ministry of Defense, which has a dedicated department for cybersecurity established in 2014 that also supervises the National Guards Cyber division.[27] Second is the national Cyber Emergency Response Team. A third is the Ministry of Transport. The three approaches consequently create dissonance in responses to different threats limited to certain areas. For example, the energy sector in some cases is tackled by the CERT and, in others, by the Ministry of Transport.

It can be argued, that these problems could instead be tackled by having a multi-layered approach based on linkages between cyber commands. If successful, this would establish the necessary framework for technical, legal and policy levels moving toward the approach of active cooperation in cybersecurity through such exercises as the aforementioned Locked Shields and other collaboration projects. This would, in turn, make it possible to further establish a suitable joint approach with the shared aim of security for the Baltic States. Furthermore, even though the problem of covert information sharing on the basis of a hub is still quite out of reach, attempts to coordinate pentesting of different state systems by Estonia could lead to the establishment of a common practice of cyber resilience on an intra-regional level, thereby fostering cooperation among cybersecurity professionals as well as fortifying interconnected areas of security such as energy, the information space (media, social networks) and telecommunications. Such a goal would be made possible by conducting nation-wide cyber exercises, which would involve both domestic and international professionals, enabling further opportunity for information and expertise sharing.

Lastly, it is vital to mention that, apart from the capabilities of Estonia, some governments are starting to pay more attention to these issues. But some remain quite reluctant due to there being a *de facto* lack of understanding of the threats posed by malicious malware, examples of which are Latvia's[28] and Lithuania's[29] unsound state investments in their national ICT systems. The problem can be resolved on the basis of educational workshops that would explain in detail the different aspects of

[26] HM Government, "NATIONAL CYBER SECURITY STRATEGY 2016-2021," https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[27] Ministry of Defense of the Republic of Latvia, "Zemessardzes Kiberaizsardzības vienība" (in Latvian), accessed on November 4, 2018, http://www.zs.mil.lv/Zemessardzes%20vienibas/kiberaizsardzibas_vieniba.aspx.

[28] Ministry of Defense of the Republic of Latvia, "Transcript of revenue and expenditure of the State basic military budget by programmes and sub-programmes," accessed on November 4, 2018, http://www.mod.gov.lv/~/media/AM/Ministrija/Budzets/Budzets%202018gadam.ashx.

[29] Ministry of National Defense of Republic of Lithuania, "APPROPRIATIONS FOR NATIONAL DEFENCE 2018," accessed on November 4, 2018, https://kam.lt/en/budget_1065.html.

cyberwarfare focusing on non-state actors, such as hacktivist groups and criminals, while also maintaining a cautious approach toward state-sponsored attacks, thus creating more efficient communication between the policymakers and technicians.

Established Challenges Infringing Upon Intra-Regional Cooperation

Based on the information provided in the previous sections, it could be argued that there are plenty of possibilities and structures in place to consistently and actively work on intra-regional cooperation. However, the majority of current initiatives and exercises are primarily being carried out within the frameworks of NATO and the EU, making it necessary to look deeper at the common shortcomings limiting cooperation within cybersecurity at the regional level.

Capacity

One of the main obstacles in the way to achieving efficient intra-regional cooperation is based on two factors. First, the Baltic governments are *de facto* in competition for skilled personnel with private firms, which provide IT operators with better wage options. Second, there is no such thing as a single "jack of all trades" operator due to the inherent nature of cybersecurity: there are an immeasurable amount ways in which bugs can manifest themselves, dozens of different programming languages, as well as multiple approaches to pentesting and protecting data and infrastructure.[30] As a result, governmental institutions require an ever increasing number of professionals who are able to provide either technical, legal or policy expertise with regard to the cyber domain. This lack of personnel capacity has become a major issue for Baltic State governments, including when it comes to boosting cooperation. The numbers of Baltic professionals dealing with the myriad of topics is low and, therefore, severely impacts the number of multilateral initiatives the states can take part in effectively. This issue requires more active support for educational and training programs on cybersecurity in such institutions as the Baltic Defense College (BALTDEFCOL) and universities in Riga, Tallinn and Vilnius in order to increase the amount of professionals working in the region.

Societal Awareness

Even though such buzzwords as "cybersecurity," "artificial intelligence" and "quantum computing" have become more prevalent in the mainstream media as well as more expert policy discussions, the majority of society nevertheless remains largely unaware of the consequences posed by cybersecurity threats. Driving causes of this challenge include the aging, and thus not computer-literate, population as well as widespread ignorance about the dangers of possible spillover effects or the damage that continued inattention to cybersecurity could bring. Such a situation stagnates the process of governance and possibly leads to different vulnerabilities. In particular, public institutions can be

[30] INFOSEC institute, "The Types of Penetration Testing [Updated 2018].", https://resources.infosecinstitute.com/the-types-of-penetration-testing/#gref.

disrupted by threats such as phishing campaigns that enable malware to take control of systems by encrypting files stored in them.

Furthermore, despite the rapidly developing sphere of cybersecurity, the aforementioned lack of expertise in the public sector negatively impacts new regional initiatives or degrades maintenance of already-existing systems and networks. This requires further government involvement in cyber hygiene initiatives aimed at both publics as well as policymakers, with the aim to develop general understanding of possible threats and necessary actions to be taken regarding operations of ICT devices.

Political Will

The current political implications for cybersecurity vary among the three Baltic States, and intra-regional cooperation still essentially lacks the necessary frameworks in Lithuania and Latvia. Consequently, the full political comprehension of the threats posed by zero-day vulnerabilities[31] are not fully understood, thus resulting in a "cyber skills gap."[32] Moreover, cybersecurity is deemed necessary for the fulfillment of obligations toward NATO and the EU to "develop the fullest range of capabilities, allocate adequate resources, reinforce the interaction amongst relevant stakeholders, improve understanding of cyber threats, enhance skills and awareness, foster cyber education, expedite [the] implementation of agreed cyber defense commitments and track the following of deliveries of the pledge."[33] It is also necessary to meet European regulations such as the GDPR and NIS directive.[34] This, if assessed in light of the previously established difficulties with capacity and limited awareness of the public and policymakers, creates the challenge of a lack of willingness to allocate larger resources and establish new incentives to increase both national capacity and intra-regional cooperation.

Attribution and Response

Cyber ethics as well as international norms act as the principal building blocks upon which the core questions of attribution and proportionate response can be approached. The question remains

[31] "*Zero-day vulnerabilities* are vulnerabilities for which no patch or fix has been publicly released. The term zero-day refers to the number of days a software vendor has known about the vulnerability" (Libicki, Ablon, and Webb, 2015). Ablon, Lillian and Andy Bogart, Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits. Santa Monica, CA: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1751.html.

[32] Leigh E. Potter, *What Skills do you Need to Work in Cyber Security? A Look at the Australian Market*, (Brisbane: Griffith University, Australia), https://dl.acm.org/citation.cfm?id=2751967.

[33] "Cyber Defence Pledge," North Atlantic Treaty Organization, https://www.nato.int/cps/su/natohq/official_texts_133177.htm.

[34] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 "concerning measures for a high common level of security of network and information systems across the Union."

prevalent as the Baltic States aim to establish a stable ICT environment as well as acquire the necessary legal and political tools for attributing a cyberattack and utilizing said information to gain the help or support of the international community.

The Tallinn Manuals 1.0 and 2.0, published by the NATO CCD COE, set out rules for responding to an attack on the sovereignty of ICT systems as well as for operations conducted in cyberspace; but these are of an advisory nature, thereby limiting the scope and impact of them on different states. The nature of the current *status quo* regarding treaty-making or creating international legal acts is also quite lackluster. Here, the primary example is the Council of Europe's Cybercrime convention, which has been accepted by the Western democracies as well as the Baltic States but has been disregarded and even attacked by such countries as Russia and China.[35] The problem of this lack of consensus regarding international norms in cyberspace extends to the currently active clash between the values represented within the UN Governmental Group of Experts (GGE) and the Open Ended Working Group (OEWG). Specifically, the two bodies differ on approaches to regulating cyberspace activities carried out by state actors: the authoritarian regimes' preference for direct control directly collides with the Internet freedom approach of the liberal democracies.

Nonetheless, since the 2014 Wales Summit, NATO allies have agreed to consider a cyberattack that threatens the sovereignty of a member state as sufficient argumentation for the invocation of Article 5 of the Washington Treaty. That consensus, in turn, has created the necessity to establish common procedures with regard to information-sharing of evidence and attribution data that would be required to gain the political unanimity to justify invoking Article 5.

Therefore, in order to move forward, the Baltic governments should first establish a shared understanding of the existing norms as well as cooperate on developing common attribution rules and position with regard to invoking Article 5 (effectively sharing information on cyberattacks that threaten the sovereignty of one or all of the Baltic States). Consequently, this would serve to provide information that is supported and recognized by other allies and NATO member states. Thereafter, the Balts must establish a common approach regarding the proportionate response to an attack. This would not only provide the basis for deterrence but also create a framework on establishing a code of conduct for intra-regional cooperation during a crisis.

A second important challenge is the fact that the majority of attacks are carried out by non-state actors. Like when it comes to responding to state-sponsored cyber threats, the Baltic States could address the threat of non-state hackers by focusing on cooperation and regional information sharing. Additionally, they should consider following Princeton requirements regarding the universality principle of law, relating to requirements of universal jurisdiction of the most serious crimes

[35] "Cybercrime Digest," Council of Europe, https://www.coe.int/documents/9252320/43971234/Cyber+Digest+CPROC+2019-02-02.pdf/96642ac2-c845-2127-5c02-92661b0a9da7.

(violation of *jus cogens* norms). When it comes to the field of cybersecurity, universal jurisdiction means that any state can put on trial any individual for a crime committed against it even from another state's territory. Cybercrime is on its way to being admitted into universal jurisdiction, as it can be committed from any state in the world; and any state will have a legal interest in punishing the perpetrator. All three Baltic countries need to strengthen existing data protection rules, pass proportionate criminal statutes regarding attacks on critical infrastructure, as well as adopt rules guiding the indictment of individuals involved in cross-border attacks. Moreover, the Balts will need to focus on due diligence of both the private and public sectors to prevent domestic non-state actor interference in elections and day-to-day bureaucratic processes. The most rational approach, legalistically speaking, is to base new laws addressing cyberspace on *lex lata* (the law as it exists) and international law while further developing them via the principle of *lege ferenda* (the future law).

In conclusion, the Baltic States could approach intra-regional security from the perspective of regional security. Proportional cybercrime rules need to be in place to prevent non-state actors from both attacking critical infrastructure for financial gain as well as threatening the stability of democratic processes such as elections and state institutions in general. A special focus is, therefore, needed to assess the cross-border impact and develop effective law enforcement. That must be combined with adopting rules in international organizations for reaching consensus on attribution of cyberattacks. It is crucial for the Baltic countries to define a concrete, common position regarding credible attribution that would allow for an effective and proportionate response in cooperation with NATO allies and fellow EU member states.

Conclusion

Current institutional and operational cooperation/coordination on cyber issues among the three Baltic States leaves plenty of room for improvement. Gaps exist between national Computer Emergency Response Teams on the exchange of information relating to recommendations on best practices, threat assessments, cooperation and coordination of cybersecurity exercises, as well as the coordination of the Baltics' interdependencies on mapping and assessing. This coordination will need to be improved through the framework of NATO COEs on cross-sector issues and by seeking effective ways to combat propaganda/fake news. Taking a more rigorous approach toward cooperation/coordination between national CERTs and private-sector cyber response teams is necessary. For example, this could involve establishing cooperation on penetration testing of critical infrastructure and incident response.

Creating a common annual Baltic Cyber Security Threat Assessment Report in the future could also allow for more intense cooperation on information exchange. Furthermore, the creation of a regional task force could improve the means for countries to exchange information, best practices, methodologies, common tools, assessments, and so on.

Baltic Interoperability by 2030

Olevs Nikers

Land Force Interoperability: A Way Forward

Before 2030, the North Atlantic Treaty Organization (NATO) and the European Union must show more coherent leadership in terms of creating cooperative defense within the Baltic States, as was emphasized by Glen Grant in this report. The simple act of creating three separate Enhanced Forward Presence (eFP) Headquarters (HQ) and not endorsing the new divisional-sized HQs as a full NATO HQ sharply reduces the coherence of any future Baltic military response.

The EU, through the European Security and Defense Policy (ESDP), needs a more serious attitude toward Baltic defense. Sweden and Finland should become part of a cooperative venture within the EU in order to play a serious role by trying to link the two more firmly into the cooperative battle space.

Politicians need plans and prior direction as much as military strategies if they are to be effective. The current posture actually creates instability and uncertainty and will likely contribute to a decision-making failure at the highest levels of the three states (and maybe allies) unless taken seriously.

The ESDP's contribution must be to tie the division into one battle space with Finland and Sweden. This is important because in any Russian attack, airbases in Estonia and Latvia are likely to be untenable due to extremely limited air-defense cover. Bases in Sweden and Finland would be needed for US air reinforcements. Both Nordic countries must be encouraged to contribute to forward defense in terms of ground and air and to take greater responsibility for sea access. The new NATO divisional HQ should potentially also include Swedes and Finns on its staff. This would be a considerable political "ask" for both countries and would need to be a two-pronged political approach from both NATO and the EU, not to mention bilaterally from the United States. However, this would greatly enhance the deterrence effect and would also create greater military coherence for what is a much more complex battlespace than just Estonia and Latvia alone.

NATO needs to focus hard upon the overall command structures and the actual fighting and support structures on the ground used by the Baltic States. On the surface, it appears that too much is left to chance, national public relations and uncoordinated bilateral cooperation.

NATO actions in the Baltics should serve to strengthen the political aspects of cooperation and interoperability. The region now needs a hard restructuring to concentrate not upon deterrence (which is not a military task) but upon war fighting.

In the years to come, it is necessary to create an intra-regional "whole of government" approach utilizing well-coordinated intra-governmental use of military and non-military means in selected areas. Each country could lead in specific areas based on expertise and willingness. An example are Centers of Excellence (COE), which represent national initiatives to play key roles in specific domains followed by involvement of other Baltic countries and partners. Another issue to consider is the fact of constant Russian information operations and propaganda toward Russian-speaking communities in Estonia and Latvia but also toward the West in general.

Cross-border operational cooperation among the three Baltic States (B3) in crisis/pre-crisis periods ("gray times") should be enhanced. In the future, the Baltic States will need to continue with common exercises that closely model real scenarios (where an adversary is trying to create situations itself, not just "reacting"), in order to make cooperation among the B3,Poland, Finland and Sweden more operationally possible—building practical developments based on political trust (which still has to be developed).

In the near future, a sub-regional "military Schengen area" for ground, air and sea should be developed, including Poland, Denmark, Germany, Finland and Sweden. This should assist in continuing to develop a common and harmonized space for the introduction of NATO military command structures, by creating common B3 operational policies, procedures, laws, doctrines, plans and training in advance of a crisis.

Also, regional combat coordination by a standing operational divisional HQ should be created either independently or with NATO. Coordination efforts should focus on creating a recognized "standing" NATO operational reserve for B3 of at least brigade strength from the nearest countries, Poland, Germany, Denmark, Finland and Sweden. Stronger and more visible cooperation on brigade-level exercises and the creation of a strategy and operations course at the Baltic Defense College (BDCOL), for senior officers and officials, is an ultimate prerequisite in the training and education of multinationally functioning officers.

A B3 Ammunition Agency, with the primary role of harmonizing public tenders, building weapons stocks, providing a gateway for cooperation with the NATO Support and Procurement Agency (NSPA) and the US, as well as for coordination other allied support, is instrumental for Baltic interoperability and should be set up in the nearest future. If necessary, there should be acceptance of the differing concepts, structures and equipment in the future. But a lead nation "B3 Center of Excellence" concept should be established for technical areas like communications, special operations forces, maintenance, artillery, cyber, etc. This would include setting up a Multinational/Baltic Formation HQ, with the primary task of operationalizing the Joint Operational Area. It should not replace national responsibilities, command and control (C2), nor freedom of action of national forces, but should become a hub for operational/tactical thinking. These, in turn, could be used to transform the synergy among B3 structures and tasks. Contingency planning and readiness to exercise command through different phases would be essential, but functions such as a training and exercise platforms as well as a point of contact for Allied interaction and cooperation would be important as well.

What is important is not only the creation of a division HQ but also the creation of all division-level enablers—something not currently within the Baltic States' abilities and which would require significant resources to build and maintain. As such, the Baltics would need to rely on other NATO countries (only some of them possess such capabilities), and it is questionable if those could be provided.

A Baltic Maritime Security Strategy for the Future

Currently, Baltic countries have focused on the development of their land forces, while air forces, except for air defense systems of different levels, and navies have been neglected. According to maritime security expert William Combes, who took part in the Baltic Security Strategy Project, this might create significant problems during a conflict by making it more difficult to ensure the successful arrival of allies to the region.[1] Military cooperation becomes more successful when decisions are taken at the NATO level. This suggests that assistance from more powerful actors will be needed to bring about cooperation between the B3 in the years to come.

The Baltic States do not have enough capabilities to deny the adversary from projecting power into their exclusive economic zones, territorial waters, port facilities and other littoral areas, or from establishing temporary sea control in those regions. Individually and collectively, they are susceptible to the type of naval tactics Russia used against Georgia in the August 2008 Five Day War.

Surprisingly, and unfortunately, Baltic countries also do not have fully integrated and shared awareness across the maritime surface, sub-surface and air domains. Each country has some of these capabilities, to varying degrees, across multiple agencies, with varying success at sharing this information. There also is no full-time command center in place to direct the appropriate level of armed response in a timely manner.

A maritime security strategy is needed that should be developed in the short-term future. Such a strategy would address the maritime situation, the threats, and the importance of the maritime domain to the B3's national economies and security as well as describe how to efficiently and effectively tackle the maritime missions needed to ensure security. This strategy, according to Combes would identify the important investments required in order to ensure a robust maritime domain awareness, capable and responsive operational centers, and coordinated or shared maritime security purchasing between the Baltic States to ensure compatibility and reduce acquisition costs.[2]

[1] Bill Combes, in *Baltic Security Strategy Report*, (Washington D.C.: The Jamestown Foundation, 2019).

[2] Ibid.

A combined and cooperative Naval Operational Center, or the maritime capability of a Joint Operational Center, would best focus the Baltic States' maritime security capabilities to mutual benefit. Some high-end naval warfare missions must inevitably be accomplished by NATO forces. A standing operations center would facilitate the planning, rehearsal, and implementation of the needed high-end NATO naval forces and capabilities that the Baltic States are relying on in the case of Russian state-on-state aggression.

Mine warfare and other constabulary maritime security enforcement missions can only be executed by B3 sailors at sea on capable, affordable vessels. Sharing the development, production and maintenance costs of these expensive vessels, whether they are patrol boats or mine warfare ships, and other armaments is the best way to ensure affordability.

Lastly, there is a need to change the understanding of the purpose of coastal navies. Coastal navies need to identify and document their requirements and build their forces to meet these specific requirements. This discussion needs to be a "maritime security" discussion and not a "naval" one. This includes how we talk about coastal navies in both the NATO and EU maritime strategies. At the moment, neither are specific enough with respect to small navies and impel these navies to focus too much thought and money on high-end naval capabilities that take away from what they need to successfully secure their maritime spaces.

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.

Due to the Baltic States' limited naval and air force capabilities, it may make sense to create common services (e.g., a naval squadron). But such a joint structure would need to be underpinned by a visible will and ability of Estonia, Latvia and Lithuania act in such a united fashion.

Air Defense: Building Proper Denial Capabilities for the Baltics

Presently, the Baltic States possess only very limited air-defense capabilities against major airborne attack. Their command-and-control networks provide only for peacetime operations, but are insufficiently robust to support a NATO air-defense posture in times of crisis.

As a priority, the Baltic States should enhance the air surveillance, command-and-control network they have developed under BALTNET, both to improve their own abilities to conduct air-defense operations prior to and during a crisis, as well as to ensure that Allied air-defense assets deployed to or exercising in the region can integrate smoothly into local air command and control.

Anthony Lawrence emphasizes in this report that action is needed in two broad areas. First, redundancy is required in the communication networks that connect Baltic C2 nodes, both within Baltic territory and to the outside world. Where single links exist, they should be duplicated, while additional routes should be created to ensure that the network can continue to function even if some links are non-functional (e.g., through technical failure or deliberate attack by an adversary).

Second, C2 needs to be enhanced, both through the introduction of technical upgrades and through the recruitment and training of personnel. The goal of these measures should be to create Command and Reporting Centers in the three states, each capable of assuming battle management roles on a continuous (but rotational) basis. Thus, ensuring the functioning of Baltic air C2, even if some locations were unavailable. The necessary technical upgrades essentially amount to the provision of Link 16 capability at Lielvārde and the acquisition of a number of Link 16 terminals to accommodate Allied air-defense assets deployed to the region. The Baltic States may wish to consider unconventional staffing solutions, perhaps using civilian personnel, or building on Estonia's experience of creating a voluntary Cyber Defense Unit.

As the Baltic States decentralize their air command-and-control operations, it will be important that they work together to develop a common training plan and conduct common training events, since Baltic airspace would continue to be treated as a single volume.

With measures to enhance air surveillance and command and control either programmed or implemented, it will make sense for the Baltic States to invest in additional air-defense weapons systems. As an immediate priority, existing short-range ground-based systems need to be fully integrated into the Baltic air C2 network—otherwise, friendly aircraft operations will be constrained by a need to keep away from areas in which Baltic air-defense assets might be operating.

In order to maximize the chances of success, the three states should consider building upon the BALTNET framework to develop a new cooperation mechanism, reminiscent of those successfully established and operated with Nordic support in the 1990s, to manage cooperation across the board in air defense.

The Baltic States, then, should be able to strengthen their air surveillance, command and control and, in the slightly longer term, field a number of short- and medium-range ground-based weapon systems. But this will still fall short of the layered, integrated air-and-missile-defense system they will need to confidently defend their airspace.

While not members of NATO, it is inevitable that Finnish and Swedish air defenses will be activated in the event of a Baltic crisis. To maximize the chances of success, Estonia, Latvia and Lithuania will also need to improve cooperation among themselves—both to achieve material benefits and to demonstrate to the rest of the Alliance that their efforts should be supported. Baltic solutions, in conjunction with active backing from NATO and other Allies, can substantially increase deterrence and air defense in the Baltic region.

Cyber Security: Boosting Cooperation and Public Cyber Hygiene

Cooperation between the public and private sectors as well as civilian-military domains should be enhanced and strengthened in the future. Currently, B3 cooperation is lacking both institutionally and practically. Cooperation among think tanks, tech startups, and other related groups should be considered and utilized to improve this structure. More intensive cooperation on cyber security awareness, training and exercise initiatives is one of the main tasks for upcoming years within the cyber security domain.

As it is currently difficult to share intelligence within the B3 and with other countries, communication along these avenues needs to be improved. There should be concentrated development to create a common information platform for cyber defense and improving public/military cooperation in cyber security.

There is room for improvement with regard to institutional and operational cooperation/coordination. Gaps exist between national Computer Emergency Response Teams (CERT) on the exchange of information relating to recommendations on best practices, threat assessments, cooperation and coordination of cyber security exercises, as well as the coordination of B3 interdependencies on mapping and assessing. This coordination should be improved through the framework of NATO COEs on cross-sector issues and by finding ways to combat propaganda/fake news. Taking a more rigorous approach toward cooperation/coordination between national CERTs and private-sector cyber response teams is necessary. For example, this could be establishing cooperation on penetration (PEN) testing of critical infrastructure and incident response.

Lithuania has proposed to create a Rapid Reaction Team (RRT) within the EU's Permanent Structured Cooperation (PESCO) mechanism. Further analysis is necessary to determine wither such a regional RRT would add value. The use of regional cyber security forums should be developed, perhaps following Lithuania's current PESCO project that builds a common approach to handling the issues of cyber security. The PESCO projects could be used to first advance a regional B3 approach to cyber security and later as the basis of a broader EU model.

Creating a common annual Baltic Cyber Security Threat Assessment Report in the future could allow for more intense cooperation on information exchange. Furthermore, the creation of a regional task force can better develop ways for countries to exchange information, best practices, methodologies, common tools, assessments, etc.

Cooperation can also help develop an understanding of what kinds of initiatives do or do not work to improve cross-sector activities within the broader framework of NATO COEs. RRTs should be considered in order to ensure reciprocity of action. This will need to be thoroughly thought through as limited resources make coordinated threat assessments more challenging. A task force able to assess interdependencies and that can create/evaluate methodologies is worth exploring. NORDEFCO is a good example, but again the Lithuanian PESCO project could further help in developing a Baltic cyber security plan.

Better coordination of exercise activities should be achieved in the years to come to avoid situations in which two important cyber security activities are happening at the same time. For example, the Locked Shields 2018 Exercise was happening at the same time as the main planning conference of the multinational, Lithuanian-led Amber Mist Exercise. Activities should be better coordinated to avoid overlap of highly similar activities of different countries.

The creation of regional task-forces for assessing service interdependence should be considered regarding the exchange of information, discussions over methodologies, common assessment tools, etc. Exchange of experiences and lessons learned to improve basic cyber-hygiene skills should be shared across central governments and at regional and local levels of state administration (municipal governmental authorities). Lessons learned should be shared regarding national initiatives to improve cyber security awareness in society because cyber-security threats and vulnerabilities are very similar across the B3.

In telecommunications, financial, energy and transport sectors, a number of B3 joint ventures already operate in all three countries, and there are interdependencies of cross-border vital services and infrastructures. These interdependencies and vulnerabilities need to be better mapped. Moreover, various national-level prevention and resilience approaches and measures need to be coordinated.

Cyber-security baseline requirements for vital services are not harmonized among the Baltic States. There may be added value 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, potential research should suggest specific areas and measures to support cross-border resilience of critical information infrastructure. When an agreement on the synchronization of the B3 electricity networks with continental Europe is achieved, there will be a need to cooperate on enhancing cyber security aspects of electricity networks[3]

Ways to foster B3 cooperation in crisis response to a large-scale cyber incident that affects more than one country should be explored. For example, cooperation is necessary between the Cyber Defense

[3] 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.

Units of the Estonian, Latvian and Lithuanian National Guard forces with regard to PEN testing of critical infrastructure and incident response.

Baltic countries each have their own national-level initiatives to curb disinformation in social media, but there is little cooperation between them in this field, which should be developed within the next few years. Possibilities to exchange best practices and to develop common approaches should be explored.

For purpose of education, training, and exercises, there is a need to develop a strong cyber-security curriculum at the Baltic Defense College. Also, it should be considered whether regional defense academies, universities and think tanks could jointly seek funding earmarked for cyber security research projects. There is an initiative at the EU to create a European Cyber Security Research and Competence Center, which would include funding prospects, so B3 educational institutions may be able to propose joint research projects.

Hybrid Warfare: Challenges and Tasks for the Future

Russia could easily exploit political and social tensions in the Baltic countries to try to draw them away from the Euro-Atlantic partnership and back into Russia's sphere of influence. According to Villiar Veebel, two types of measures must be adopted to avoid this. First, political resilience should be increased in all Baltic countries individually as well as in the Baltic region as a whole.[4] This would allow the Baltic States to rapidly adopt countermeasures in case of Russian aggression, while simultaneously not allowing Russia to use the strategy of low-level aggression. Under these circumstances, the main hope for the Baltic countries would be that Russia gives up on aggression during the conflict after seeing that the model of "a peaceful liberator" would not work in the Baltics. Second, it is necessary to avoid social discontent in the Baltic countries, which would work in Russia's favor in a potential conflict. Thus, attention should be paid to social inclusion and social welfare in Estonia, Latvia and Lithuania. This applies particularly to some regions of the Baltic countries with a high share of the Russian-speaking population.

The most active area for Baltic cooperation is in strategic communication (StratCom). Currently, StratCom representatives hold annual or biannual meetings to exchange information and coordinate positions. This helps develop initiatives that focus on developing approaches to ensuring there is societal resilience in the area of media and societal support for intra-regional understanding. However, while the Baltic States face some of the same issues, they will have to be addressed differently due to the nuances of their scope, manifestation, etc. Nevertheless, cooperation within this domain should be sustained and enhanced in the future.

The three nations actually know relatively little about each other and are not primarily interested in

[4] Baltic Security Strategy Project, *Defense and Deterrence workshop materials,* May 10, 2018 (unpublished).

one another's affairs. The Baltic States reflect a very low neighborhood index, and domestic media reports of one another's affairs tends to be scarce. Lack of interest also extends to promoting outside actors and organizations.

In order to foster this understanding, some thought must be put in to how the three Baltic States can become more committed to promoting and elevating one another. Public diplomacy techniques could easily reflect a distinct cultural or historical dimension.

The promotion of media literacy and critical thinking is obligatory in any established democratic society. Experts should use media literacy materials that can be shared across the Baltic States and altered to meet the nuanced needs of each specific population.

It is important to develop a system where all three states could work together to resist the common threat to their continued independence. This coordination is especially important in the region, as it is often treated as a testing ground for political instruments used by Russia to gain influence, power and resources.

Coordination is needed across different political sectors and dimensions. This should include the promotion of people-to-people contacts and central themes of communication focused on the operational picture, analysis of risk and vulnerability, as well as interaction and joint crisis management. For example, there is currently no shared media channel across the Baltic States, which also discourages interest in each other's affairs. Establishing a media channel that features all three countries could be a remedy, but such a channel should also reach out to minority populations. A B3 channel could draw in Russian speakers, signaling a more inclusive society. This could also improve communication and cooperation among journalists from across the Baltic States. Investigative and objective journalism practices and training could be shared across the region.

The unique nature of disinformation campaigns currently prevents the B3 from benefiting from intra-regional cooperation in this area. Disinformation is often tailored to local contexts and incidents familiar to the specific target audience. Campaigns bombard target societies with biased or false stories until they are recirculated by more reputable media outlets. Thus, intra-regional cooperation faces a significant obstacle.

In recent years, the most important fields of cooperation have been foreign policy and security policy. However, more cooperation in the field of media and societal resilience is needed. More guidance and instruction to the public must be delivered by official authorities like the ministries of culture to teach and inform the public regarding issues of disinformation and other forms of hybrid offensives, while at the same time underscoring the need for multi-stakeholder collaboration on media literacy and resilience coming from a bottom-up approach. Combined initiatives of Baltic leaders are forming more public awareness around the problem, but Baltic populations need to become more analytically critical as media consumers.

In the future, the three countries need to focus on developing and implementing projects that offer comprehensive and effective strategies in which they can counter Kremlin disinformation spread across the region. This could include an analytical toolkit that can effectively deal with disinformation at the institutional, strategic, and conceptual levels.

Author Biographies

Mr. Glen Grant works as a defense and reform expert in Ukraine working for the Ukrainian Institute for the Future. He is also a Senior Fellow at 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, Glen 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 the UK's Ministry of Defense (MOD). This work involved him supporting many operations, including both Gulf Wars, Bosnia and Kosovo. He was also 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 *Kiev Post*. He is a skilled change manager with a Master's degree in the Leadership of Innovation and Change from York St. John University, in the UK. Glen 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. 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, Anthony 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. Anthony 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.

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, Olevs 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). Olevs was a recipient of the Transatlantic Fellowship Program from The World Affairs Institute in 2018. He is Director of the Baltic Security Strategy Project and a PhD student at Riga Stradins University.

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.

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. Otto 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.