Conor McDonald  
University of California, Los Angeles  

The Eastern Threat: Understanding and Counteracting Russian Cyber Activity in the Baltics

1. Introduction

From Muscovy and the Russian Empire to the Soviet Union and the Russian Federation, the leaders of the Russian state have enacted both preemptive and invasive warfare in the name of security. As Paul Stronski and Richard Sokolsky argue in *The Return of Global Russia: An Analytical Framework*, a brief prepared for the Carnegie Endowment for International Peace, Russia’s “foreign actions are often opportunistic,” aimed at creating a “a multipolar world in which it plays a more prominent role.”¹ The opportunistic and expansionist aims of Russian foreign policy are especially evident in two key regions: the Black Sea, which includes Ukraine and Georgia, and the Baltic coast, which includes Estonia, Latvia, and Lithuania.² Given Russian President Vladimir Putin’s bald revanchism in the Black Sea region, particularly the annexation of Crimea, public attention has moved away from the Baltics and toward Ukraine and the Caucasus.³ However, high strategic stressors remain in place in the Baltics, and the West must maintain its support for the region and work toward deterring Russian aggression.

The tangible threats posed by a potentially expansionist Russian Federation toward the Baltic nations of Estonia, Latvia, and Lithuania fall into two categories: conventional threats, which “[encompass] all warfare short of warfare using nuclear weapons” and involves any troops that are “not specifically labeled special operating forces,” and cyber threats, which are used more

---

¹ Stronski and Sokolsky, 1.  
² Ibid.  
³ US Department of State, “Evidence of Russian Support for Destabilization of Ukraine.”
frequently in the twenty-first century. Conventional warfare in the form of “major combat operations directed at controlling territory, inhabitants and resources” is physically and economically costly, as it requires a vast supporting military infrastructure. Cyber warfare includes assaults on social media, electronic banking attacks, and digital political strikes. This type of warfare resists definition, particularly because governments have “little incentive to embrace a definition of cyber warfare” because of the variety of ways it can appear in the international realm. This paper defines cyber warfare as any attempt by a nation (or agents working on its behalf) to carry out attacks against another nation’s technological or informational infrastructure in order to further a strategic objective. This definition is adapted from a number of expert analyses, particularly the work of Scott Applegate, an adjunct professor at Georgetown University, and members of the Institute of Electrical and Electronic Engineers. Cyberattacks are often attempts to influence public opinion—for example, the alleged Russian interference in the 2016 US presidential elections and the 2007 Russian cyber assault on Estonian financial systems were meant to undermine public faith in democracy and westernization, respectively.

Scholarly work on this topic often investigates the underlying motives for Russian expansionism. Some attribute expansion to a weakened Russian state’s economic and political insecurities, while others consider it a natural reaction to NATO expansion and subsequent American encroachment in the region. Regardless of Russia’s motive, many subject matter

---

4 Piddock, 3.
5 Ibid.
6 Applegate, 18.
7 Ibid.
8 Ibid.
9 Ibid.
10 Ibid.
11 Ehin and Berg, passim; Meyer, 67–82.
experts recognize the Russian Federation’s military superiority compared to the Baltic states’ defense industries and believe that Russia would be able to quickly annex or invade a Baltic state through conventional means with little to no military resistance.\(^1\) Despite the Russian Federation’s ability to invade Estonia, Latvia, or Lithuania using conventional means, the most tangible and realistic threats faced by these states pertain to Russian cyber warfare campaigns against them.\(^2\) This paper argues that the Estonian, Latvian, and Lithuanian governments must cooperate with each other and with NATO to advance their respective cyber defense systems and successfully defend themselves against Russian cyberattacks. If they fail to do so, the Russian Federation will continue to use cyber warfare to compromise its neighbors’ sovereignty.

2. Historical Russian Interest in the Baltics

Before analyzing the potential for Russian encroachment against the Baltics in the modern era, it is crucial to understand the Russian Federation’s historical interest in the region. From a historical perspective, the Baltics have had strategic importance in Russian foreign policy since the sixteenth century. The first Russian threats to the area began with the Livonian War of 1558, when the Tsardom of Russia invaded territory comprising modern-day Estonia and Latvia.\(^3\) In 1721, the Treaty of Nystad, which concluded the Great Northern War between Russia and the Swedish Empire, officially placed the Baltics under Russian control.\(^4\) This began the first great influx of ethnic Russians into the Baltics, who filled administrative roles in major cities. The Baltic territories remained under the dominion of the Russian Empire until the 1917 revolution, at which

\(^1\) Ibid.
\(^2\) Ibid.
\(^3\) Filyushkin, 422.
\(^4\) Treaty of Nystad, art. 5.
point the autonomous Governorate of Estonia came into existence.\textsuperscript{16} The Council of Lithuania passed an act reinstating its independence in February of 1918; Latvian officials followed suit by forming a provisional government in November of that same year.\textsuperscript{17} After these states were reabsorbed by the Soviet Union after World War II, local populations were forcibly removed and ethnic Russians were encouraged to populate the Baltics. At its highest point, Estonia’s population was approximately 35\% Russian, providing the Soviet government with additional influence and regional support.\textsuperscript{18}

The Baltic region has long been considered a geographical buffer zone in culture clashes between East and West, beginning with the Great Schism of 1054, when Europe separated into two unique spheres: the West, dominated by the Holy Roman Empire and the Roman Catholic Church; and the East, dominated by the Byzantine Empire and Eastern Orthodoxy.\textsuperscript{19} The Baltic states, located between the westernmost Catholic nation of Poland and the easternmost Orthodox Slavic principalities, were subject to a cultural and religious tug-of-war.\textsuperscript{20} In the early thirteenth century, a number of battles were fought in this area as Western militaries and the Teutonic Knights sought to push the Catholic border eastward; however, Novgorodian prince Aleksandr Nevskii led the Russians to victory over the Teutonic Knights in present day Estonia, earning the region an important place in the Russian historical tradition and an accompanying cultural attachment.\textsuperscript{21}

The status of Latvia, Lithuania, and Estonia as tangible demarcations of influence between Russia and Western powers remained over the course of the next millennium, especially during

\textsuperscript{16} Huang, 65.  
\textsuperscript{17} O’Connor, 80.  
\textsuperscript{18} Chinn and Kaiser, 97.  
\textsuperscript{19} Ibid.  
\textsuperscript{20} Janušauskas, 97.  
\textsuperscript{21} Riasanovsky and Steinberg, 76.
the two World Wars.\textsuperscript{22} In the first half of the twentieth century, the Soviet Union and Nazi Germany clashed in the Baltics and eviscerated the borderlands as they fought for regional dominance.\textsuperscript{23} National borders were treated with reckless abandon, as there are very few natural terrain features that delineate the Baltics from their neighboring states.\textsuperscript{24} Additionally, political decisions by Baltic governments to assist the Germans in repelling Soviet influence led to overwhelming feelings of betrayal and scorn in the echelons of Soviet leadership.\textsuperscript{25} Despite reclamation by Soviet forces, “the devastation of the region during the two great wars […] made it politically unstable, i.e., vulnerable to influence from the outside,” and it would maintain this geopolitical vulnerability throughout the remainder of the twentieth and twenty-first centuries first as a satellite of the USSR and then an interest of Russia.\textsuperscript{26}

The Soviet Union first occupied the Baltic states in 1940 under the auspices of the 1939 Molotov-Ribbentrop Pact, then recaptured the territory in 1944 after three years of German occupation during World War II. From 1944 to 1991, the Soviet Union controlled the Baltics through puppet regimes. Lithuania, Latvia, and Estonia "all understand themselves to have been […] occupied states during the Soviet period."\textsuperscript{27} The “hostility and suspicion” that characterized Russo-Baltic relations during this period continually degraded any preexisting sense of rapport between these nations—overwhelming contempt for the Russian administration pushed Lithuania, Latvia, and Estonia to look westward as the Soviet Union collapsed, which allowed the United

\textsuperscript{22} Ibid.  
\textsuperscript{23} Ashmore, 13.  
\textsuperscript{24} Shlapak and Johnson, 4.  
\textsuperscript{25} Smith, 91.  
\textsuperscript{26} Janušauskas, 98.  
\textsuperscript{27} Holoboff, 112.
States to gain a foothold in the Baltics when the Soviet Union’s economy and infrastructure degraded beyond repair.\textsuperscript{28}

Unsurprisingly, the Russian government viewed this westernization as a threat. Estonian defense minister Juri Luik summarized the insecurities when he stated that “anything the Western leaders are pushing for is almost automatically something which Russia considers as alien or foreign or negative.”\textsuperscript{29} However, the cultural connections between Western Europe and the Baltics, along with rapidly developing western technological innovation, proved too insurmountable for Russia to match.\textsuperscript{30} In 2004, approximately a decade after Soviet military withdrawal from the region, the nations of Latvia, Lithuania and Estonia were accepted into NATO, officially aligning them with the foreign policy goals of the United States and its Western allies and making them the only post-Soviet nations to have membership in both the European Union and NATO.\textsuperscript{31} However, the Baltics still retain their positions as invaluable strongholds for control over the Eastern/Western balance of power, and the Russian Federation continues to pursue cultural and political imperialism against them, which prevents all three from entirely securing their freedom.\textsuperscript{32}

\textbf{3. Moving from Conventional to Cyber Warfare}

The threat to the Baltics has now expanded from physical and cultural occupation to the digital realm. Conventional invasion is uncommon in Europe today, where complex alliances discourage military intervention and the fifth article of the North Atlantic Treaty plays a crucial role in protecting its member states. For the Russian Federation, an attack on Estonia, Latvia, or

\textsuperscript{28} Ibid.
\textsuperscript{29} Mehta.
\textsuperscript{30} Janušauskas, 98.
\textsuperscript{31} Kühn, 5.
\textsuperscript{32} Ashmore, 13.
Lithuania would be indistinguishable from an attack on the United States, France, Germany, or any other powerful ally; this deterrent to conventional warfare against NATO member states has proven successful for nearly seventy years. Additionally, at the 2014 Wales Summit, in response to the Russian Federation’s military aggression in Ukraine, NATO created a task force of 5,000 troops that remains on constant rotation throughout the Baltics. Often referred to as “tripwires,” these soldiers, many of whom come from the United States, France, Germany, or the United Kingdom, signal to Russia that “an attack on one of these states would result in immediate escalation to a full-blown conflict with NATO,” thereby extending the collective defense clause and further warranting the intervention of their home nations.

For this reason, the Russian Federation began to implement alternate methods of influencing and manipulating the affairs of ex-satellite states. Cyber warfare has quickly become one of the country’s most effective attack methods, providing Russia with the ability to further its international strategic interests anonymously. This anonymity adds a layer of complexity to examinations of the Russian Federation’s execution of cyber warfare. Although it is undeniable that “there is little concrete proof of involvement of the Russian Federation government in any cyberattacks,” it remains that “the circumstantial evidence does lead to the perception that the Russian government was behind or supported […] cyberattacks” in Estonia, Lithuania, and Latvia.

---

33 Ibid.
34 NATO Review Staff.
35 Pfundstein-Chamberlain, 1.
36 Cooley, 1.
37 Ibid.
38 Ashmore, 1.
Two of the most dangerous and common forms of cyberattacks that have been utilized against the Baltics are denial of service attacks (DoS attacks) and distributed denial of service attacks (DDoS attacks). A DoS attack, the simpler of the two, inhibits an individual user’s ability to “access information systems, devices, or other network resources” by disrupting his or her internet connection.\textsuperscript{39} This prevents people from accessing banking information, communicating digitally, or conducting any form of research on the internet, often all at the same time. However devastating these attacks may be, nations and individuals with vast resources and expert ability levels (e.g., the Russian Federation and its operatives) are able to further damage a nation’s infrastructure through the execution of DDoS attacks. These allow for “exponentially more requests to be sent to the target” than in DoS attacks, which greatly expands the power and reach of the attack; they also “make the sources of the attack harder to identify,” which almost entirely eradicates any ability to blame an actor or origin with complete certainty.\textsuperscript{40} Given the relative ease with which the Russian Federation can carry out DoS or DDoS attacks on its neighbors, most experts agree that new “attack methods will continue to be developed and utilized” in order to further incapacitate the nations of Latvia, Lithuania, and Estonia.\textsuperscript{41} Presumably, the intention is that the Baltics will grow weary of Russian attacks and hence participate in fewer anti-Russian or pro-Western activities in order to avoid them.\textsuperscript{42}

The 2007 DDoS attack on Estonia and the 2008 DoS attack on Lithuania provide two easily identifiable case studies for what can be expected from the Russian government going forward, both from the perspective of what prompted them and from the perspective of how they were

\textsuperscript{39} US-CERT.
\textsuperscript{40} Ibid. A “request” refers to an attempt by an aggressor to overcrowd and ultimately shut down a target’s servers.
\textsuperscript{41} Harris et al., 10.
\textsuperscript{42} Ibid.
executed. In Estonia, hostilities had been mounting between ethnic Russians (a group that makes up 24.9% of the national population) and ethnic Estonians over the preservation of a Soviet World War II memorial, the Bronze Star Statue. Tensions grew steadily as the statue became “a rallying site for [pro-Russian] demonstrations and other forms of protest against the Estonian government” on the part of ethnic Russians, and they culminated in the Estonian government’s decision to relocate it, much to the dissatisfaction of the local Russian population. Following a period of riots, looting, and minor violence, “computers in the Estonian government and the Estonian national media were hacked into with significant affect [sic]” in what has now been classified as a DDoS attack, harming the nation’s economic, political, and personal infrastructures. Although the attack was limited in scope, it led to a brief period of havoc in Estonia, a nation where online voting is commonplace, most of the public follows their news digitally, and “more than 90 percent of bank transactions are done over the Internet.” Concern set in when it became clear that this had become the pattern for Russian attacks to follow.

The precursors to Lithuania’s 2008 DoS attack strongly parallel those of Estonia’s. Russo-Lithuanian relations deteriorated after Lithuania blocked talks meant to better relations between the European Union and Russia. In retaliation, the Russian government leveraged “energy resources for political gain” and refused “to compensate Lithuanian victims of Soviet labor camps.” The Lithuanian government subsequently outlawed “the display of Soviet symbols,” after which three hundred national websites, including banking, news, and social media pages,

---

43 Statistics Estonia; Davis.
44 Ashmore, 6.
45 Ibid.
46 Davis.
47 Ibid.
48 Ashmore, 13.
49 Ibid.
were disabled by DoS strikes; other sites were digitally vandalized with anti-Lithuanian and pro-Soviet imagery including hammers and sickles.\textsuperscript{50} Unlike in Estonia, where the purpose of the attack was to “completely shut down the IT structure,” the DoS attack against Lithuania was much smaller, meant perhaps as a warning of what could potentially occur should Lithuania continue its anti-Russian activities.\textsuperscript{51}

Although the Russian Federation believes that “Baltic nations fail to recognize the heroism of Soviet soldiers,” the Baltics, particularly in the case of Lithuania, are instead rejecting a revisionist Soviet history that was forced upon them after World War II.\textsuperscript{52} Lithuania, Estonia, and to a lesser extent Latvia have each been technologically attacked by the Russian Federation as a form of retaliation against acts that Russia fears threaten its soft power or influence.\textsuperscript{53} These acts include the destruction or restriction of Soviet monuments or symbols, anti-Russian political messages, and general prejudices against ethnic Russians. Recent history indicates that, as each of these acts grow more common, pro-Russian and anti-Baltic cyberattacks will continue to escalate as technology advances.\textsuperscript{54}

\textbf{4: Current Defensive Practices}

In response to the high potential for escalating cyberattacks, NATO leadership and the Baltic governments have worked together in employing several standard operating procedures as a form of response protocol. These procedures operate under the assumption that Russian cyberattacks will only be possible if an existing “threat triangle” of capability, intent and

\textsuperscript{50} Rhodin.
\textsuperscript{51} Ashmore, 7.
\textsuperscript{52} Rhodin. Quote from an interview with Russian premier, Dmitri Medvedev.
\textsuperscript{53} Ashmore, 13.
\textsuperscript{54} Ibid.
opportunity remains uninfringed upon. According to this theory, if “an adversary’s capability, intent, or opportunity is neutralized or removed, the adversary is incapable of causing large-scale harm to operations” through the use of a DoS or DDoS strike.\(^5^5\)

In the Baltics, Russian intent to inflict technological harm on its neighbors may be impossible to neutralize as long as Russian leaders feel threatened by anti-Russian sentiments from ethnically Baltic citizens.\(^5^6\) Unless the Baltic nations leave NATO and submit to Russian influence, this obstacle will remain insurmountable.\(^5^7\) In like fashion, the only way for the Baltics or the West to lessen the Russian state’s capability of carrying out cyberattacks would be through “kinetic strikes on infrastructure”—e.g., efforts by the West to destroy Russian-based attack centers with missiles or bombs—or other preemptive, conspicuous engagements that would “potentially [be] perceived as hostile.”\(^5^8\) Given the meager size of their military forces, it would be wrong to argue that Estonia, Latvia, or Lithuania would be willing to wage any form of conventional warfare against the Russian Federation. Likewise, leaders from the United States and NATO have made it clear that they wish to repair relations with Russia, not exacerbate them by destroying Russian infrastructure.\(^5^9\)

Consequently, the most effective way for the Baltics to protect themselves against cyberattacks would be to mitigate opportunities for the Russian Federation to engage in a cyberattack, thus collapsing the “threat triangle.”\(^6^0\) A combination of preventive measures could “eliminate the possibility of DDoS attacks altogether” before they begin.\(^6^1\) One of the most

\(^{55}\) Harris et. al., 3.
\(^{56}\) Ibid.
\(^{57}\) Ibid.
\(^{58}\) Ibid.
\(^{59}\) Taylor.
\(^{60}\) Harris et. al., 3.
\(^{61}\) Mirkovic and Reiher, 48–49.
effective, common-sense ways that the Baltic states could weaken outside opportunities for cyberattacks would be to eradicate the anonymity associated with them. Continuing to fund and utilize revolutionary software like Pi, which “gives the victim of a DDoS attack the ability to filter” any incoming attack against “known attacker” histories, thus identifying with relative certainty the source of an attack, can lift the curtain on Russian anonymity and force attackers to face international consequences.\(^6^2\) Another method that must become a standard in order to reduce opportunities for threat is for the Baltic governments to adopt artificial intelligence early warning systems, such as Random Early Detection (RED), and implement them within their most critical and susceptible infrastructures (banking, defense, etc.).\(^6^3\) RED systems can indicate when site traffic “exceeds a specified number,” at which point the host can “throttle back the flow rate” or reduce threatening quantities of distributed internet traffic, which might then be associated with a DDoS attack.\(^6^4\) The only reason that this system has not been implemented on a wide scale in the Baltics is because it would require those nations “to add additional software and functionality” to their systems, a task that could be accomplished with proper assistance from NATO but is difficult for their governments to accomplish on their own.\(^6^5\)

Should the Baltic nations fail to install these preventive measures, there will be a resultant failure to diminish Russian attacks. Since Russian capability and intent are not realistically reducible, attacks will carry on over time. For this reason, reactive measures, or measures that “strive to alleviate the impact of an attack on the victim” following the successful execution of an attack, are emphasized in allied training.\(^6^6\) The NATO-organized Cooperative Cyber Defense

\(^6^2\) Yaar et. al., 13  
\(^6^3\) Harris et. al., 12.  
\(^6^4\) Ibid.  
\(^6^5\) Ibid.  
\(^6^6\) Mirkovic and Reiher, 48-49.
Center of Excellence (CCDCOE), based in Tallinn, Estonia, annually conducts an exercise known as Locked Shields, during which over “1,000 experts from nearly 30 nations” (many of whom come from Estonia, Latvia, and Lithuania) “play the role of national rapid reaction teams that are deployed to assist a fictional country in handling a large-scale cyber incident and all its multiple implications.” These joint exercises between allies are absolutely crucial to the defense of the region as a whole because, at the height of a cyberattack, the nation being attacked at the point of its critical infrastructure will have the most difficulty defending itself. According to some scholars, this idea of collective defense “implies an unusual economic model,” since “parties that will sustain the deployment cost are not the parties that directly benefit from the system,” a fundamental flaw that can only be mitigated through continual membership in NATO and the enforcement of its treaty’s fifth article. The parties sustaining “the deployment cost” of these defense mechanisms are also benefiting from this system, since the safety and operability of a nation’s allies leads to the safety and operability of the nation itself.

Whether through NATO-led training or independent domestic defense, a firm balance between preventive and reactive measures is paramount to securing the safety of each Baltic nation’s cyber realm. The Estonian government has chosen to integrate their public cyber defense sectors with local private sector technological companies in order to conduct “security tests of information systems” and gain “a better overview of where [these companies’] vulnerabilities and risks might lie,” which greatly helps to fine-tune any existing security problems. Additionally,

---

67 NATO CCDCOE.
68 Mirkovic and Reiher, 49.
69 Ibid; The North Atlantic Treaty.
70 Mirkovic and Reiher, 49.
71 Ibid.
72 Annual Cyber Security Assessment 2017 (Republic of Estonia), 43.
as of 2018, “Estonia is creating a division to combat cyberattacks, the number of personnel in which is set to increase by 20% each year.”73 Lithuania has followed suit, with a recent government act in 2018 offering private sector companies the opportunity to “participate in the implementation of the National Cyber Security Strategy,” at which point they will be able to work toward strengthening the “cyber security of the country and the development of cyber defense capabilities.”74 Although its defense ministry is moving more slowly than Estonia’s or Lithuania’s, the Latvian government is beginning to acknowledge experts' requests to redirect its national defense focus from strictly countering foreign propaganda to also speaking “on clear actions on internet infrastructure issues,” including what “the action plan [would be] if the state loses internet approach, etc.”75 As these nations continue to build independent steps toward security in conjunction with internationally accepted preventive and reactive measures, they will be able to strengthen their infrastructure and minimize Russian cyber aggression.76

5: Further Defensive Development

Despite the strong potential for developing Baltic cybersecurity, such steps are still marred by unique difficulties. Three major obstacles must be overcome within the upcoming decade if the Baltics wish to properly protect themselves from an increasingly advanced onslaught of Russian threats. First, each of these three nations must mandate that both public agencies and private companies report each cyberattack they fall victim to.77 Second, defenses against distributed denial
of service attacks need to undergo realistic testing.\footnote{Ibid.} Third, the Baltics must add additional functionality to their government’s internet systems alongside their global allies.\footnote{Harris et. al., 12.} These steps will be technologically complicated and politically charged, but their implementation would put Latvia, Lithuania, and Estonia at the forefront of international cyber safety.\footnote{Ibid.}

Mandating reports of cyberattacks within both public and private sector companies is an essential component to expanding a government's understanding of the specific threats posed against them. Because of the perception that “reporting occurrences of attacks damages the business reputation of the victim,” attacks are often reported only to government organizations when the secrecy of details can be guaranteed.\footnote{Mirkovic and Reiher, 47.} This is not an unreasonable position; a recent report from accounting firm PricewaterhouseCoopers illustrated that “87 percent of consumers are […] willing to walk away and take their business elsewhere if, or when, a data breach occurs” in a company.\footnote{Neveux.} However, if Estonian, Lithuanian, and Latvian companies and public sector organizations hide their problems in order to maintain consumer support, it will be nearly impossible for their governments to refine and adjust their security measures.\footnote{Mirkovic and Reiher, 47.}

Additionally, the need for the “realistic testing” of potential responses to DoS and DDoS attacks cannot be understated.\footnote{Ibid.} Unfortunately, the lack of large-scale testing environments makes this currently impossible due to the lack of “safe ways to perform live distributed experiments across the Internet, or detailed and realistic simulation tools,” since live internet-wide experiments

\begin{thebibliography}{99}
\bibitem{78} Ibid.
\bibitem{79} Harris et. al., 12.
\bibitem{80} Ibid.
\bibitem{81} Mirkovic and Reiher, 47.
\bibitem{82} Neveux.
\bibitem{83} Mirkovic and Reiher, 47.
\bibitem{84} Ibid.
\end{thebibliography}
would pose great technical risks to the cities and nations in which they occur. As a result, data regarding defense system performance is almost always taken from the findings of “small-scale experiments and simulations,” and is therefore “not credible.” The National Science Foundation in the United States is currently developing a large-scale testing environment for what is referred to as “heavy vehicle cyber security experimentation,” but there must be continuous dialogue and support between America and the Baltics in order for Estonia, Latvia, and Lithuania to get the most out of this research project. Until this dialogue leads to an appropriate testing environment and productive experiments, it will be difficult to determine with absolute precision how prepared the Baltics are to recover from and prevent cyberattacks.

Lastly, the Baltics must add additional software and functionality to their internet systems. In order to fully implement software like the artificially-intelligent random early detection program, significant changes must be made to the internet’s core both in the Baltics and globally, which in and of itself supposes great political problems. This will be the most difficult of the three steps, and acquiring “international agreement upon the integration of the required changes into the network layer will be one of the biggest challenges” in its implementation. Despite involving years of debate, collaboration, and political resistance from global cyber attackers such as the Russian Federation, NATO members must remain unified in their desire to update the functionality of their internet in order to accommodate these programs and determine

---

85 Ibid.
86 Ibid.
87 Amla.
88 “Functionality” here refers to a uniform, global ability to monitor and potentially restrict excessive internet traffic.
89 Harris et. al., 12.
90 Ibid.
where they “stand in the cyber security arena.” Ultimately, given their small international influence, the Baltics should intend to follow future US-led efforts to implement these changes.

VI: Conclusion

The realm of cyber warfare is a new, daunting field with a number of unprecedented challenges that distinguish it from twentieth-century conventional warfare. What remains unchanged, however, is the Russian state’s efforts to assert influence and control in the Baltics. The effectiveness of recent Russian cyberattacks and concomitant shortcomings in establishing cyber defense systems in all three of the Baltic nations reveal that there is more to be done in the region to protect against Russian aggression. DoS and DDoS attacks will continue to play a major role in the Russian Federation’s attempts to “discipline” anti-Russian sentiment across its border. The Baltics must continue to implement defensive actions to guarantee their security. These actions include reducing attacker's anonymity and instituting artificially intelligent systems to reduce site traffic during DDoS attacks. Research has begun on these actions in Estonia and Lithuania, but they must eventually implement them. Additionally, continued collaboration on the part of the Baltics with NATO’s Cooperative Cyber Defense Center of Excellence and the United States’ National Science Foundation will ensure the free exchange of updated information regarding cyber defense. Each of these courses of action will reduce the overall threat faced by the Baltic countries. It is only upon their implementation that each nations’ sovereignty can be protected from the Russian threat.

91 Ibid.
92 Filyushkin, 422.
93 Ashmore, 1.
94 Mirkovic and Reiher.
95 Harris et. al., 3; Amla.
Although an anonymous strike on a computer network may not provide the same sense of tangible, material loss as a conventional attack on public infrastructure, its effects can be similarly damaging to the security of a victim. The Baltics face this threat today. Despite the fact that Vladimir Putin’s “flexing behavior is [little more than] a flimsy facade to cover for economic feebleness,” his nation’s strength will continue to grow should it maintain coercive influence over its Baltic neighbors. The continued success of Russian cyberattacks in the Baltics could establish a precedent: other neighboring nations who seek to align against the Russian Federation might face these attacks. Given that Estonia, Latvia, and Lithuania, protected as they are from military intervention by their NATO membership, face the most cyberattacks of Russia's neighboring countries, the region must emplace strong defenses against them. The threat from Russia may be mitigated through technological improvements and sustained alliances, but the negative and potentially dangerous effects of slow-moving change still remain a likely reality.

Works Cited


---

96 Neveux.
97 Painter.
98 Radu.
99 Jewkes and Vukmanovic.


