Assessing the New Threat Facing the Baltic States and the NATO Alliance

Sebastiano Dina
September 2019
CYBERWARFARE AND CRITICAL INFRASTRUCTURE

Assessing the New Threat Facing the Baltic States and the NATO Alliance

Sebastiano Dina
2019 Title VIII CEE Area Studies Fellow

September 2019
The Issue

From the Editor: In Russian military thinking it is often difficult to discern a formalized doctrine of cyber warfare, but the totality of writing on the subject suggests that for Moscow, cyber is not an independent domain of operations but a subordinate part of the wider concept of information warfare. The term “cyber” as used in the West to denote computer network operations is alien to Russian thinking. For the Kremlin the key objective is information, and cyber is merely a tool to achieve that objective. In this brief, Title VIII Fellow Sebastiano Dina explores the threat of Russian CI cyberwarfare, as well as its implications for Baltic energy security and NATO’s deterrence posture.

Russia is engaging in unrelenting cyberwarfare against the critical infrastructure of the United States and its allies. As the United States moves to secure its domestic infrastructure, it must also coordinate efforts with NATO to protect vital Allied infrastructure and curtail Russian cyber-enabled influence operations. Due to their strategic position on NATO’s frontline, cooperation must begin with the three Baltic states: Estonia, Latvia, and Lithuania.
Modern states depend on reliable infrastructure to function. From roads and power stations, to oil pipelines and railways, infrastructure is inextricably tied to the economic prosperity and national security of states. Among these infrastructure assets, some are considered so vital to national interests that their destruction or incapacitation would have severe, debilitating effects on state function. These vital assets are commonly referred to as Critical Infrastructure (CI) and include the chemical, communications, energy, financial, transportation, nuclear, and wastewater sectors, among others.¹

Since at least 2013, Russia has launched a ceaseless cyberwarfare campaign to gain entry, survey, and take control of the CI of the United States and its allies.² To the Russian regime, the mere appearance of launching a cyberattack is a cost-effective, high-impact, and difficult-to-attribute tool to influence, intimidate, and blackmail its opponents. In the event of a military confrontation, Russia could use full-fledged cyberattacks to temporarily incapacitate the vital infrastructure of its adversaries.³ And left unchecked, Russia will continue to develop this capability, endangering the U.S. homeland, economy, international interests, and global military logistics network, as well as those of its allies.

With forces deployed abroad, and wide-ranging economic and strategic interests overseas, the United States relies on the CI of its allies.⁴ American logistics lines to Europe run through allied ports like Bremerhaven in Germany.⁵ U.S. military aircraft in Europe fly through airspace regulated by NATO Allies and Partners.⁶,⁷ And U.S. defense manufacturing, as in the case of the F-35, relies on parts and spares built in NATO member states.⁸,⁹ These dependencies, and others like them, highlight an inescapable fact: the CI of allies is inextricably tied to the security and prosperity of the United States.

Prime targets of Russian cyberwarfare—and U.S. allies whose critical infrastructure is of paramount importance to the United States—are the Baltic states. Due to their strategic position on or close to Russia’s border and their significant Russian-speaking minority populations, the Baltic states are a constant target of Russian influence operations and at perennial risk of Russian incursion.¹⁰¹¹ From the U.S. perspective, the Baltic states are valuable allies whose position on NATO’s
RUSSIA’S APPROACH TO CYBERWARFARE

It is often difficult to discern a formalized doctrine in Russian military writing. But an inescapable concept nonetheless emerges from analysis of government, military, and academic sources: for Moscow, cyber is not an independent domain of operations but a subordinate part of the wider concept of information warfare (informatsionaya voyna). More fundamentally, the term “cyber” as used in the West to denote computer network operations (CNO) is not a “Russian concept,” and terms like “cyber warfare” are only ever used in Russian sources to describe “foreign concepts and activities.” To Russian experts, the difference between CNO (cyber) and any other tool to collect, spread, and amplify disinformation—like bot networks or propaganda websites—is negligible and spurious. The key objective is...
information. Cyber is merely a tool to achieve that objective.

More broadly, information warfare is the use of “informational-technical” and “informational-psychological” means, such as electronic warfare, psychological operations, and disinformation to “dominate the information landscape” and “reduce the fighting potential of the enemy.”¹⁷¹⁸ Russian information warfare manipulates, distorts, destroys, and fabricates information which it then proliferates into the press, academia, and social media to control international narratives, foment dissent, and incapacitate an adversary’s decision-making. Contrary to Western doctrine on information warfare, the Russian approach—which harkens back to Soviet methods—is for information warfare to be conducted at all times and against any target, regardless of the state of hostilities.¹⁹

Past Russian cyberattacks have been as much about achieving the aims of information warfare through influence and intimidation as they have been about physical destruction. A telling example was the 2015 cyberattack against Ukraine’s electrical grid.²⁰ During this operation, Russian hackers infiltrated the control systems of three Ukrainian power companies and caused a six-hour blackout that affected an estimated 225,000 customers in the Ivano-Frankivsk, Chernivtsi, and Kyiv Oblasts.²¹

Three indicators point to the use of information warfare in that attack. The first is the limited physical impact. If Russia’s primary goal had been to cause kinetic destruction, the hackers could have gone much further and caused “permanent, physical damage to the grid.”²² Instead, they opted for a limited show of force which avoided long-term physical destruction.

Second, for maximum psychological effect, Russian cyberattacks are often carried out at symbolic times. For instance, cyberattacks against Ukraine—including the 2015 attack—often correspond with national holidays like Constitution Day, Independence Day, and Christmas.²³ Finally, by tauntingly repeating the attack almost exactly a year later in 2016, Russia may have sought to reinforce a disinformation narrative about the incompetence of the Ukrainian government and Ukraine as a “failed state.”²⁴,²⁵

Cyberattacks like these, which have a relatively low impact, become weaponized in the broader

“Past Russian cyberattacks have been as much about achieving the aims of information warfare through influence and intimidation as they have been about physical destruction.”
context of Russian information warfare. Rather than individual events, they are compounded by a daily campaign of disinformation, leaks, false narratives, energy warfare, corruption, and influence operations all aimed to weaken an adversary’s “will to resist.”\textsuperscript{26} Cyberattacks are a tool in the information war, not just an end.

In the future, as Russian cyber-kinetic capabilities improve, their doctrine may evolve to place greater emphasis on the physical aspect of cyberwarfare. But until then, Western observers should not discount attacks that have only limited physical effect and must instead view them in the wider context of Russia’s information strategy.

\textbf{THE ATTACK PATH OF RUSSIAN CI CYBERATTACKS}

Below the doctrinal level, basic knowledge of the technical tools being developed by Russian hackers and how attacks are carried out are prerequisites to understanding their potential strategic impact for the Baltic states and NATO. Some of the key stages and methods in Russian CI cyberattacks are apparent in four recent public cases attributed to Russia: the 2015 \textit{Sandworm} and 2016 \textit{Industroyer} attacks against Ukraine’s electrical utilities, the 2016 \textit{Dragonfly 2.0} campaign against the United States and Europe, and the 2018 \textit{Triton} malware attack against a petrochemical plant in the Middle East.\textsuperscript{27,28,29,30} Analysis of these attacks—though necessarily neither non-exhaustive nor a predictor for future methods—highlights nonetheless some of Russia’s demonstrated capabilities, and offers an opportunity to explore basic policy and technical responses.

\textit{Reconnaissance}

The common starting place for Russian cyberattacks is reconnaissance. In this phase, extensive open source research is carried out to identify targets and gather knowledge about potential vectors to infiltrate their computer networks. By parsing websites, executive interviews, public tenders, and other sources of personally identifiable information, hackers collate information about the target’s employees and organizational structure. This is later used to entice the end user by crafting highly-tailored emails that appear legitimate, but which in fact contain malicious code.\textsuperscript{31}
In complex cyberattacks like the ones against Ukraine, reconnaissance may take upwards of a year and often extends to a target’s clients and suppliers. For example, Russian hackers associated with Sandworm were already launching a phishing campaign six months in advance of the final attack in 2015. And in the Dragonfly campaign against the United States, reconnaissance identified third-party suppliers early as staging points in the final attack. Consequently, hindering Russian cyberwarfare requires that CI operators be judicious about the information they share online and watchful against adversarial reconnaissance efforts.

**Weaponization**

Next, Russian hackers weaponize the information from reconnaissance to create legitimate-looking files (often PDF or Word documents) modified with malicious code or exploits. These files are later sent via email to the target company’s employees where, once opened, the embedded exploits pave the way for hackers to take control of the system.

The targeted use of compromised emails is known as “spear phishing” and is a common infiltration tool among hackers. In 2015, spear phishing was used to enable the installation of malware onto the computers of three Ukrainian energy distribution companies; in 2016, it was used to infect Ukrenergo computers; and in Dragonfly 2.0, malicious Microsoft Office files were sent from compromised legitimate email accounts to targets across the United States’ energy and critical infrastructure sectors. Guarding against phony attachments and spear phishing is therefore critical to CI cybersecurity and must start at the individual level.

**Delivery, Exploitation, and Installation**

The weaponized file is then delivered in order to obtain user credentials and other exploitable
information. Delivery can be achieved through spear phishing, as described in the weaponization phase, but there are other methods for achieving the same effect.

One such method is a “watering hole” attack. In these attacks, hackers compromise legitimate websites known to be frequented by the target to harvest their access credentials or lure them into downloading a malicious file. During Dragonfly, Russian hackers made extensive use of “watering holes” by, for example, compromising the websites of trade publications related to the CI industry.39

Another method is a supply chain attack, where hackers compromise a target’s software suppliers by using their update stream to upload malware to the target. In 2017, Russian hackers compromised the update servers of the Ukrainian accounting software M.E.Doc and used them to upload the NotPetya worm to an estimated 10% of all computers in Ukraine.40 Though NotPetya did not specifically target critical infrastructure, this attack path could be adapted to compromise power plants, gas companies, and other CI facilities through their software suppliers. To secure supply chains, more robust regulation is needed to make software providers liable for the security of their updates.

**Development, Testing, and Delivery**

In the development, testing and delivery phase, hackers develop additional malware, test its effectiveness in a simulated environment, and deliver it to the target system. Malware developed in this phase is different from the one used in previous phases. Its focus is no longer on gaining access or information, but on the physical sabotage of industrial machinery. To achieve this effect, the new malware must be able to interfere with industrial control systems (ICS) – the devices and instruments used to control an industrial process.

Since 2010, there has been an observable increase in the sophistication of Russian ICS malware. Russia’s first such malware, known as Havex, was a simple intelligence-gathering tool used to scan computer networks for connected systems and devices – but unlike other such scanners, it was tailored to detect ICS equipment and systems.41 In 2016, Russia made further progress with the development of Industroyer, which had a modular system that allowed it to interact with a wider variety of systems. Once installed, it could be used to erase data from ICS instruments and render them inoperable.42 The latest step in Russia’s malware development is known as Triton. Discovered in 2017 after an accident at a petrochemical plant in the Middle East, its advanced features allow hackers to interfere with ICS equipment by attacking its supervisory safety software.43

The increasing sophistication of Russian ICS malware is a clear indication of Moscow’s intent to target critical infrastructure. This will necessitate CI operators banning the use of all non-recognized software through blacklisting and, at the NATO level, sharing knowledge of new ICS vulnerabilities and malware as they emerge.

**Execution**

Russian hackers complete CI attacks by activating malware or exploiting existing functionality to disrupt industrial processes. Execution can take many forms, although past
cyberattacks have generally involved a high degree of coordination between concurrent Russian teams and operations.

In the 2015 Sandworm attack against Ukraine for example, execution involved four highly coordinated steps: (1) Russian hackers interrupted the power supply in central Ukraine by remotely and near-simultaneously activating the breakers of at least 27 power substations; (2) to stop Ukrainian engineers from restoring power, they “blew the bridges” by uploading malicious firmware that broke the connection between power companies and their substations; (3) they launched a coordinated telephone denial-of-service attack that flooded the power companies’ phone lines; (4) they erased data and activity logs from the target systems to render computers inoperable and destroy evidence of the attack. Such high-level coordination, coupled with the lack of a profit motive, are strong indicators of a state-sponsored cyberattack which may often be beyond the ability of CI operators to defend against.

Further, this case shows that Russian cyberattacks are often accompanied by additional measures to frustrate CI recovery efforts, lengthen operational downtime, and remove evidence that could be used to attribute the attack. A Russian cyberattack is therefore not necessarily a standalone operation, but can involve multiple simultaneous efforts. Sabotage of an industrial process is not the sole objective, but could also involve incapacitating the enemy’s response and securing plausible deniability for the Kremlin. Building on this knowledge, NATO member states should mandate off-site backups of all CI access and activity log data and be weary when responding to a cyberattack that concurrent attacks could occur elsewhere.

“Russian cyberattacks are often accompanied by additional measures to frustrate CI recovery efforts, lengthen operational downtime, and remove evidence that could be used to attribute the attack.”

So far, this brief has explored the doctrine and practice of Russian CI cyberwarfare by assessing past operations. In the process, it has highlighted three key takeaways: (1) Russia has a permissive cyber doctrine with a high tolerance for CI attacks, even during peacetime; (2) Russia is actively developing technical capabilities to sabotage CI; and (3) Russian cyberattacks, even against physical targets, can be part of a larger information...
Cyberwarfare and Critical Infrastructure, 9

Cyberwarfare strategy. Coupled with the growing volume and boldness of Russian cyberwarfare, this is a clear indication that Moscow intends to continue CI cyberattacks in the future. Moreover, they also signal a growing need to assess the exposure of vulnerable U.S. allies to cyberattacks, as well as the potential implications for NATO’s deterrence posture and U.S. foreign policy.

In the following section, the brief will outline just such an assessment with a focus on the Baltic states and the implications for local energy security. The first section starts with Russia’s key interest in the Baltic states. It then explores how the history of energy in the region has perversely increased the Baltic states’ vulnerability to CI cyberwarfare and highlights key infrastructure assets that may be targeted in the future. The section concludes with an assessment of the potential impact on U.S. and Baltic state interests.

Among Russian interests in the Baltic states, perhaps none is more important than reestablishing “strategic depth.” For more than a decade, this has been a driver of Russian influence operations in the region, and could be furthered through future CI attacks. This apparent need for strategic depth comes from the belief that Russia is under “permanent siege” by the West. In this world view, Moscow perceives that the United States has abused its post-Cold War unipolar hegemony by expanding NATO and using democracy promotion to undermine its authority. This sense of vulnerability is compounded by Russia’s geography, which lacks significant natural defenses. Therefore, to ensure its security under these conditions,
The Kremlin believes that it must re-establish strategic depth by expanding outwards and increasing the distance between its heartlands and the enemy — a distance which decreased significantly when Estonia, Latvia, and Lithuania joined NATO in 2004.49

Russia will be unlikely to coerce the Baltic states back into its sphere of influence through military force.50 Instead, Russia relies on a variety of tools including corruption and disinformation to undermine faith in NATO, erode Baltic national cohesion, and influence elections. But a particularly effective tool—which stands to gain from Russia’s increased cyber proficiency—is pipeline politics. Here, Russia has exploited its dominant position as the primary regional energy exporter by threatening dramatic energy price increases or stopping supply. Examples of energy blackmail span from the beginning of Baltic independence through today: in 1990, Russia interrupted oil supplies to the Baltic states in an effort to crush calls for independence;51 in 1992-1993, Russia again cut off oil exports to pressure the Baltic states into rescinding their demand for the withdrawal of Russian troops from the region;52 and on various occasions in 1998, 2003, and 2006, Russia curtailed energy supplies to influence negotiations for the sale of the Latvian port of Ventspils and the Mažeikiai oil refinery in Lithuania – the only such refinery in the region.53,54

Recognizing Russia’s chokehold on their energy supply, the Baltic states have started ambitious infrastructure projects in recent years to secure energy independence. Though largely successful, Baltic energy has been concentrated into a few infrastructure assets, increasing the potential damage of a cyberattack. Two assets are particularly concerning: the Lithuanian liquified natural gas (LNG) terminal in Klaipėda, and the Inčukalns Gas Reservoir in Latvia.

Klaipėda is a floating LNG storage and regassification unit that allows Lithuania to import natural gas through maritime shipping. Since starting operations in 2014, it has successfully broken Gazprom’s monopoly in the Lithuanian gas market and allowed energy supply diversification.55 Between 2014 and 2016, greater diversity and market competition led to a 55% decrease in Lithuanian gas prices.56 In 2015, its first full year of operation, the terminal imported 90% of Lithuania’s natural gas demand and has the capacity to import Lithuania’s annual gas needs twice over.57,58 With this spare capacity, it can also partly fulfill...
Latvian and Estonian natural gas demand, further weakening Russia's regional energy monopoly. But its outsized role in Lithuanian and regional energy independence also means that the Klaipėda terminal could become a prime target for Russian cyberattacks.

Similarly, the Inčukalns Gas Reservoir in Latvia is the only significant gas storage facility in the Baltic states. It has a capacity of 2.3 billion cubic meters, with the potential for further expansion to 2.8 billion cubic meters. This capacity enables it to function as a safety reserve, increasing the reliability of regional gas stocks from 100% to 145.94%. It also operates in synergy with Klaipėda: when gas demand is low during the summer, the reservoir fills with excess gas from Klaipėda and is then released back into the system when demand increases; and in the event of a sudden shortfall in supply, it provides a cushion, buying time for the Baltic states to address the shortfall or find emergency suppliers. As the only significant Baltic reservoir, Inčukalns is critical to regional gas supply and, like Klaipėda, is therefore a potential cyberattack target.

A successful Russian cyberattack against either asset would significantly impact Baltic security, NATO's Eastern Flank defense posture, and regional U.S. foreign policy interests. In the region, Russia could use cyber-enabled energy disruptions, coupled with more traditional subversion methods, as a tactic to intimidate and sow chaos. A well-timed cyberattack during an election period could be used to sway voters in a direction more favorable to Russian interests. And a concerted cyber campaign against CI could be used to slow construction of Baltic energy infrastructure, extending the lifespan of Russia's remaining energy influence.
At the NATO level, because cyberattacks are difficult to attribute and their destructiveness can be highly tailored, Russia could manipulate the intensity of the attack to inflict significant damage while remaining below NATO’s Article 5 threshold. Such cyberattacks could also damage NATO cohesion by straining the confidence of Allies that NATO is capable of defending them. Disruptions to the Baltic energy system could also hinder the reinforcement and sustainment of NATO Enhanced Forward Presence troops stationed in the region. And attacks against the military gas supply chain could impede the refueling of Allied air patrol missions.

Finally, for the United States, leaving Russian CI cyberattacks in the region unchallenged would weaken confidence in American security guarantees, endanger U.S. personnel stationed in the region, and allow Russia to field test and develop new CI attack methods which could more intensely threaten U.S. interests in the future. The United States should thus seek to support Baltic cybersecurity efforts through greater information-sharing and technical assistance.

POLICY RECOMMENDATIONS

Support Lithuanian Sensor Development

One area which could benefit from U.S. technical assistance in the Baltic region is the development of cybersecurity intrusion sensors, which scan for suspicious activity like unrecognized IP addresses, known malware code, and irregularities in packet exchange. As future cyberattacks could become increasingly automated, these sensors will play a critical role in independently detecting and blocking intrusions. In Lithuania, the National Cyber Security Center is developing new sensors for its domestic CI assets. Once completed, they will be deployed across Lithuania and protect important regional facilities like Klaipėda. To increase their effectiveness, NATO states should standardize the type of data collected and how it is recorded, and then share it. This will allow for comparison of intrusion trends, detection of patterns of network reconnaissance, simplification of the communication of technical data, and identification of the spread of new malware, exploits, and attack methods.

Invite Baltic CI Operators to DHS Initiatives

The United States can also support Baltic CI operators by extending an invitation to existing Department of Homeland Security (DHS) CI initiatives. A first such initiative is the Cyber Information Sharing and Collaboration Program (CISCP). CISCP is a collaborative program that allows CI operators in the United States to share knowledge about vulnerabilities and grants them access to DHS threat analysis databases. Through CISCP, when CI engineers discover a new vulnerability, they can rapidly notify the rest of the industry and request DHS support. As members of CISCP, Baltic CI operators would be able to check their systems against the existing vulnerabilities database, respond more rapidly to new vulnerabilities, and contribute knowledge of any vulnerabilities they discover. A second initiative prime for United States-Baltic collaboration is the DHS’s Automated Indicator Sharing (AIS) system. AIS is a software that automatically checks incoming IP and email addresses against a CI community-generated blacklist. When AIS detects a blacklisted address, it
automatically blocks it and issues a report to the DHS. Participation in AIS would give Baltic CI operators an added layer of protection against spear phishing and contribute their own knowledge of suspect addresses to the database. Should Baltic membership of these initiatives prove successful, DHS could consider granting limited access for vetted individuals to sensitive but unclassified platforms like the Homeland Security Information Network (HSIN).67

Rethink the Airgap

A common feature of all CI vulnerabilities is the insufficient separation of systems from the open web. Before the introduction of internet of things (IoT) industrial management technologies, CI systems were entirely self-contained and separate from the internet. But the digitalization of control systems that has taken place over the past two decades has resulted in a breach of this separation (known as the “air gap”). Today, engineers operate machinery remotely from their home or office computers, field technicians receive live sensor data through apps on their personal phones, and CI software is updated through the open internet.68 These devices and processes, which are connected to the web, are potential entry points for hackers. Because cybersecurity engineers do not have the resources available to secure every new phone, computer, and piece of IoT equipment that is added to company networks, there is a growing need to rethink the importance and implementation of the airgap. A potential solution, is to identify the vital controls needed
for the baseline operations of CI facilities, and then segment those controls into a network completely separated from the internet. Once segmented, they could no longer be accessed remotely, and would require engineers be physically present at a facility to operate them. In turn, hackers would hindered in accessing these most vital systems, effectively limiting their potential to cause damage. In addition to segmentation, CI operators should run security checks on their staff’s personal devices, increase awareness about the airgap, and hard-lock personal devices out of the segmented network.

Create Honeypots

A final technical measure for securing Baltic CI are “honeypots.” In cybersecurity, honeypots are computers, websites, servers, and emails disguised to appear as alluring targets to hackers. Honeypots are usually disguised as high-value targets like banks, utility companies, and government agencies that promise to hold lucrative financial information or sensitive government documents. In reality, honeypots hold only phony data and an array of intrusion sensors. In the past, they have been used to great effect to safely gather information about the wider threat landscape. Though widely used in many countries, it is possible that there are no government-run CI honeypots in either Lithuania or Latvia. To increase knowledge of the cyber threat to Baltic CI, the United States should offer its assistance and prior expertise in setting up honeypots to the Baltic governments. Once operational, data from the honeypots should be corroborated with sensor data from CI facilities to paint a detailed picture of the number and frequency of cyberattacks, the most common attack vectors, and the origin of attacks – insofar as this can be ascertained.

Increase Bilateral Training

As part of existing efforts to strengthen allied CI, the U.S. Department of Energy has run cybersecurity trainings and exchanges with the Baltic states. Lithuanian officials have testified to the usefulness of these trainings and suggested they could be extended. Future trainings and exchanges could begin in two areas: forensics and emergent technologies. With improved forensics, the Baltic states will be better-able to protect their CI by detecting existing breaches and tracing the origin of attacks. Finally, by running new trainings on emergent technologies, the United States can contribute to future-proofing Baltic CI against the threats of tomorrow.
Endnotes


15 Ibid.

16 Ibid.


26 Connell and Vogler, “Russia’s Approach to Cyber Warfare.”


Greenberg, “How an Entire Nation Became Russia’s Test Lab for Cyberwar.”


“Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.”


“Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.”

Ibid.


Blank, “Cyber War and Information War a la Russe.”


Center for European Policy Analysis


57 Chivvis, et al., “NATO’s Northeastern Flank.”

58 Collins, “Russia’s Use of the ‘Energy Weapon’ in Europe.”


63 Melchiorre, “Recommendations on the Importance of Critical Energy Infrastructure (CEI) Stakeholder Engagement, Coordination and Understanding of Responsibilities in Order to Improve Security.”


66 “Interview with Lithuanian government officials” July 2019.


“Interview with Lithuanian government officials,” July 2019.

“Interview with NATO officials,” June 2019.

“Interview with Lithuanian government officials,” July 2019.


“Interview with Lithuanian government officials,” July 2019.