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

BALTI ASSAMBLEE
BALTIJAS ASAMBLEJA
BALTIJOS ASAMBLĖJA

Analysis

Global Connections, Regional Implications: An Overview of the Baltic Cyber Threat Landscape

October 2015

Patrik Maldre

ISSN 2228-2076

Table of Contents

Executive Summary

This report provides a brief overview of the global and Baltic cyber threat landscape, with a particular view toward strategic threats to national and international security. The findings confirm the oft-stated view that cyber threats are becoming more numerous and sophisticated year after year and that increasing cooperation and investment are crucial to countering them. The report provides evidence for these claims primarily by examining and aggregating data from annual reports by global security companies and Baltic cyber security agencies, as well as from research papers focused on particular advanced actors and campaigns.

The aim of the report is to provide decision-makers and analysts with a more complete understanding of the cyber threats to the Baltic region in order to facilitate the development of cooperative projects and encourage effective policy development.

The global cyber threat landscape is becoming more challenging partially as a result of the continuing discovery and utilization of critical software vulnerabilities. In 2014, vulnerabilities such as Heartbleed and Shellshock caused information security experts and Internet-based service providers around the world to react rapidly in order to prevent significant breaches to their organizations and customers. More recently, the amount of critical Adobe Flash Player vulnerabilities have considerably reduced the public trust in that software, to the point that many believe the once-ubiquitous plugin will be phased out. In terms of exploits, the case of Shellshock and others demonstrated that attackers are able to incorporate vulnerabilities into attack code with increasing speed and effectiveness. On the other hand, takedowns of particular exploit kits such as Blackhole are beneficial but they will not keep attacks at bay for long. Other kits, such as the Angler kit, quickly gain market dominance. Finally, the quality and quantity of malware is also rapidly increasing, with over one million new variants reportedly created per day. There is a noticeable trend toward more advanced use of encryption, obfuscation, and “virtual-machine aware” code.

The Baltic cyber threat landscape is affected by these and other connected threat elements in a considerable way, but there are also some nuances and idiosyncrasies. Estonia reported a considerable increase in the severity of incidents, despite the overall number remaining broadly similar in comparison to the previous year. There was also a qualitative leap in the level of Estonian-language use of phishing campaigns as well as an increase in the number of defacement and denial-of-service attacks. Latvia, meanwhile, saw high-priority incidents fall and low-priority incidents rise. It also identified ransomware, Heartbleed, and Adobe and Java vulnerabilities as threats while also putting a particular emphasis on banking Trojans. Lithuania, for its part, reported a very sizable increase in the total number of incidents handled in 2014, and identified software intended to create and deploy botnets and botnet-based attacks against websites as the primary threat to civilian cyber security.

The last several years have provided an increasingly clear window into the probable development and utilization of offensive cyber capabilities by the Russian Federation. Dozens of research papers by cyber security companies have tied together different campaigns and toolkits to particular actors with connections to Russia and Russian

strategic interests. This report identifies four such “advanced, persistent threats”: Turla, the Dukes, Red October, and APT 28 (all of which are tracked with different names by different companies). The chapter on Russian cyber espionage provides details of the infection vectors, malware variants, and command-and-control infrastructure employed by these actors, as well as a consideration of targeting preferences and findings relevant to attribution. It is clear that these actors have been supporting Russia’s internal and international security policy aims since at least 2007. Perhaps most significantly, these APT groups have been acting with relative impunity; all of them are either currently active or are expected to resume activities in the near future.

Finally, the report also briefly investigates the threats to critical infrastructure cyber security in the Baltics, with a particular focus on industrial control systems whose sabotage can cause considerable destruction and loss of life. There do not appear to have been any large-scale attacks on such systems in the Baltics in recent years, but the global threat is certainly present. Although it is not widely known, there are an incredible number of Supervisory Control and Data Acquisition (SCADA) systems that can be identified, and in some cases even manipulated, through the Internet; in fact, there are roughly 6,000 of these in the Baltics alone. There are also an increasing amount of software vulnerabilities affecting industrial control systems; one report identifies a tremendous growth in the number of attacks globally. Finally, one particular APT group that accessed over 2,000 companies in over 80 countries has already been identified as possessing the capability to sabotage those systems. This is an increasing problem that has significant international security implications. Attacks against such systems not only can amount to acts of war themselves, but also trigger escalation to conventional (or, in the worst possible scenario, nuclear) war.

In the end, the nature of the threats calls for increased cooperation among the Baltics in the field of cyber security. Domestic awareness and capability development need to be advanced. At the same time, it is crucial to formalize cooperation at the regional level through the signing of a Memorandum of Understanding or analogous agreement. Furthermore, the Baltics need to be aware of the interconnectivity of their critical infrastructure and undertake projects that help to reduce the risks of a major cyber attack against it. Finally, at the global level, the Baltics can contribute to their own cyber security by helping to shape global policy debates and by providing assistance and expertise to partners and developing nations around the world.

1. Introduction

The Baltic states of Estonia, Latvia, and Lithuania emerged from under the yoke of the Russian Empire in the aftermath of the First World War and resumed exercising their sovereignty in 1991 after nearly five decades of Soviet occupation. This shared historical timeline, coupled with common geographical opportunities and constraints, has given rise to shared priorities, notably integration into Western political, military, and economic structures. Despite national idiosyncrasies, the three Baltic States have also adopted broadly analogous security policies and threat assessments. These similarities also extend to arguably the most recent major addition to the international security arena - cyber security.

Since 1991, governmental agencies and companies of most sectors in all three Baltic States have turned to information and communications technologies (ICTs) to enhance governmental effectiveness and spur economic development. This rapid rate of ICT adoption, however, has led to new national security and business risks in the form of vulnerabilities in computerized systems that can be maliciously exploited by criminals or rival nation-states for economic or strategic gain. Since the 2007 attacks on Estonian governmental, media, and banking websites that accompanied the Bronze Night, the Baltic States have all formally recognized these threats in policy documents. They have also enacted legislative changes to increase awareness and compel compliance among businesses with regard to cyber security. Since there is 'no going back to pen-and-paper,' the nature and number of these threats merit detailed examination.

The majority of threats to ICT systems are fairly global and indiscriminate as a result of the worldwide market domination of hardware and software systems by a relatively small number of producers and developers. However, the universe of potential threats can be subdivided by region, country, and sector—based on the interests and capabilities of the attackers. Factors such as prosperity, political tensions, security awareness, and language barriers, among others, can also lead to substantial differences in the threat landscape across countries and regions. This landscape, however, is in near-constant flux as a result of the rapid changes in technologies and actors that are involved as well as the practical and policy responses that are developed to achieve cyber security.

This report will provide an overview of the prevailing trends in the global cyber environment, aggregate recent national perspectives to generate a regional Baltic threat assessment, and introduce the nation-state level actors that have been implicated in malicious cyber activities against the Baltics. Additionally, the report will include an analysis of the strategic implications of these hazards and provide recommendations to strengthen public and private cyber security in the Baltics. The final product will serve to inform further Baltic cyber cooperation and contribute to the development of compatible and complementary policies and regulations in the region.

2. Global Cyber Threat Environment

The social, economic, and political benefits brought to organizations and individuals through the process of connecting computers to each other in networks and then connecting those networks to each other around the world have been truly revolutionary. However, the interconnectedness of ICT infrastructure, particularly internet-enabled devices, means that threats to the security of those devices have also become largely global in nature. The quantity of software and hardware that is created by a relatively small number of producers and developers further accentuates the worldwide character of most cyber threats. A considerable proportion of global threats also affect the Baltic States of Estonia, Latvia, and Lithuania as a result of their high connectivity and widespread use of those products. The following section will provide a brief overview of the changing threat landscape at the global level.

At the most general level, the aim of cyber security practitioners is to safeguard the confidentiality, integrity, and availability (CIA) of systems and information. Those objects of defense can become threatened as a result of the discovery of vulnerabilities, i.e. weaknesses in the code allow an attacker to compromise the CIA of that system or piece of software. After the discovery or disclosure of a 'vulnerability', malicious actors can develop specific types of code, known as 'exploits', to take advantage of that vulnerability in order to gain access to information, execute remote commands, conduct a denial of service, or pose as another entity on the network.[1] Remote commands given by the attacker can include instructions to the computer to download additional pieces of malicious software, known as 'malware', without the user being aware of the download or the activities of the malware once it is on the computer. Malware can also be distributed in other ways, such as by visiting compromised websites or through removable media storage devices such as USB drives. These vulnerabilities, exploits, malware and their delivery mechanisms, and the actors that are behind all of those developments collectively constitute much of what can be referred to as the cyber threat landscape. Since the threat landscape is almost always in a state of flux—new vulnerabilities are constantly being discovered, new exploits are regularly created to take advantage of those vulnerabilities, and new types of malware and increasingly clever delivery mechanisms are being compiled – practitioners and policymakers alike have a continuous need for new information on the latest threats and trends.[2]

[1] "Terminology." *CVE – Common Vulnerabilities and Exposures.* Mitre Corporation, 27 Feb. 2013. Web.
[2] The following sections compile information from the annual reports of a variety of computer security companies. The assessments and statistics of each are based upon the sources of information available to them, which are primarily their own customers. For this reason, the individual facts presented below should not be seen as different aspects of the same data set, but rather as pieces of different data sets that can be assembled to identify trends and draw out insights into the bigger picture of the global cyber threat landscape.

2.1 Vulnerabilities

New types of software and updated versions of older ones are continually found to be lacking from a security standpoint. Vendor employees, security researchers, governmental agencies, and others reported a total of 9,400 new vulnerabilities that were subsequently added to the standardized Common Vulnerabilities and Exposures (CVE)[3] database in 2014.[4] 24 of these vulnerabilities were so-called "zero-day" vulnerabilities[5], software weaknesses that were not discovered by researchers, disclosed to the vendor, and fixed, but rather which emerge during the course of an attack that is identified, usually by a computer security company. Furthermore, attackers exploited the top five zero-days for a combined 295 days before the companies whose software had been vulnerable made patches available to their customers.[6] However, a total of ten CVEs accounted for almost 97% of the exploits observed in 2014; moreover, only one was from that year, with a majority being more than a decade old.[7] Finally, 2014 did bring to light several highly critical vulnerabilities in widely used open-source software, namely "Heartbleed", "Shellshock", and "Poodle." By one estimate, the Heartbleed vulnerability potentially affected 17% of the Internet's secure web servers.[8] Additionally, worldwide responses have been far from ideal; 56% of all versions of the protocol affected by it are still vulnerable because they are more than 50 months old.[9] The Shellshock case, on the other hand, became an example of how quickly attackers begin to exploit such vulnerabilities; exploits were used within hours of the disclosure, and after a week millions of attacks were observed per day.[10] All in all, it is safe to assert that defenders and vendors continue to have their hands full, as new and complex vulnerabilities are discovered and old ones continue to be commonly leveraged.

2.2 Exploits

It is virtually impossible for software developers to create products that are completely secure, and legitimate researchers are constantly working to discover flaws. However, both before and after the public discovery of these vulnerabilities, various types of threat actors also work to create code to exploit those security oversights in order to achieve a degree of control over computers to: carry out credential theft; steal, change, or delete information; use the computer to send out spam; utilize it as part of a robot network, or "botnet," to carry out large-scale denial-of-service attacks, or numerous other types of nefarious activities. In order to do so, the threat actor needs to create a piece of exploit code or purchase what is known as an "exploit kit." The most common targets of exploitation, both historically and in 2014, are the most widely spread software categories, especially operating systems (e.g. Windows, Mac

[3] "Terminology." *CVE – Common Vulnerabilities and Exposures.* Mitre Corporation, 27 Feb. 2013. Web.
[4] "2015 Internet Security Threat Report." *Symantec* 20 (2015):. Web.
[5] "Magnified Losses, Amplified Need for Cyber-Attack Preparedness: TrendLabs 2014 Annual Security Roundup." *Trend Micro* (2015):.Web.
[6] "2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.
[7] "2015 Data Breach Investigations Report." *Verizon* (2015): Web.
[8] "2015 Dell Security Annual Threat Report." *Dell* (2015): Web.
[9] "2015 Annual Security Report." *Cisco* (2015): Web.
[10] "2015 Dell Security Annual Threat Report." *Dell* (2015): Web.

OS, Linux), web browsers (e.g. Internet Explorer, Mozilla Firefox, Google Chrome), third-party plugins (Adobe Flash Player, Oracle Java, Microsoft Silverlight), and document processors (Adobe Reader, Microsoft Word).[11] Specific exploit kits that leverage both recent and older vulnerabilities are perhaps the most serious threat, as these kits often contain code to take advantage of multiple types of software.

The year 2014 saw a major shift in the cyber threat landscape with regard to exploit kits, with the late 2013 takedown of the actor(s) behind the "Blackhole" exploit kit which was previously responsible for roughly 20% of exploit kit usage in 2013 and 40% in 2012.[12] This led to a significant decrease in overall kit detection in the early months of 2014[13], but numbers soon picked up with the attacker community shifting increasingly to the Angler, Nuclear, Sweet Orange, and Goon kits.[14] The Angler kit, with its use of Flash, Java, Microsoft Internet Explorer, and Silverlight vulnerabilities, accounts for 60% of kit usage.[15] It has been particularly highlighted as the most effective and sophisticated exploit kit, and has achieved a reported 40% compromise rate in 2015.[16] With regard to the type of software that is being exploited, there have also been recent trends that are worth highlighting. For one, the quantity of Java exploits has decreased markedly according to a variety of security reports, while those for Silverlight have seen a dramatic upturn.[17] Furthermore, the number of vulnerabilities found in Adobe Flash Player (and the associated development of exploits and inclusion into exploit kits) has more than doubled[18]. Finally, 2014 and 2015 have also featured an increasing amount of demonstrated exploits of software that are used in products such as cars[19], medical devices[20], and, perhaps most controversially, in planes.[21] Finally, there is an established consensus among security firms that patches for vulnerabilities are taking longer to roll out, while threat actors are conversely gaining speed in terms of the time it takes them to create and independently use an exploit as well as incorporate it into exploit kits.

2.3 Malware

The software vulnerabilities and the code needed to exploit those flaws lead to perhaps the most crucial piece of the threat landscape puzzle: malware. There are various types of malware, including but not limited to viruses, Trojans, worms, bots, adware, rootkits, and spyware. These different categories also have considerable

[11] "Microsoft Security Intelligence Report." *Microsoft* 18 (2015): Web.
[12] "2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.
[13] "2015 Annual Security Report." *Cisco* (2015): Web.
[14] "2015 Annual Security Report." *Cisco* (2015): Web.
[15] "2015 Dell Security Annual Threat Report." *Dell* (2015): Web.
[16] "2015 Midyear Security Report." *Cisco* (2015): Web.
[17] "Microsoft Security Intelligence Report." *Microsoft* 18 (2015): Web.
[18] "2015 Midyear Security Report." *Cisco* (2015): Web.
[19] Menn, Joseph. "Security Experts Hack into Moving Car and Seize Control." *Markets*. Reuters, 21 July 2015. Web.
[20] Welch, Ashley. "U.S. Officials Warn Medical Devices Are Vulnerable to Hacking." CBS News, 4 Aug. 2015. Web.
[21] Zetter, Kim. "Is It Possible for Passengers To Hack Commercial Aircraft?" *Security*. Wired Magazine, 26 May 2015. Web.

internal variety in terms of complexity and functionality. Exploit code is not malicious by definition. For example, exploits are used as part of the Metasploit framework to test the security of software products.[22] However, much of the time malware will include exploit code as part of its broader code base in order to enable the implementation of various different malicious activities, such as logging keystrokes or sending out spam messages. Furthermore, exploitation is often the step that precedes malware infection, as it enables malware to be downloaded onto a victim's computer—often without the user's permission or knowledge. The way that malware is downloaded onto the machine depends on the type of vulnerability that is exploited, such as whether a Java flaw is used to remotely execute controls to download it or whether an exploit requires privilege escalation on the system to do so manually by the attacker. Regardless, there is a continuing consensus among the cyber security community that the quantity and sophistication of malware is steadily increasing year-over-year. In other words, the cyber threat landscape continues to become more complex and dynamic, thereby requiring constant attention.

There are several trends in the world of malware that are significantly changing the cyber threat environment. First and foremost, the quantity of malware is increasing as the financial benefits of cybercrime continue to grow. According to one estimate, a total of 317,000,000 new pieces of malware created in 2014 (compared to 253,000,000 in 2013[23]), which translates into nearly one million new pieces per day.[24] This rather large number is partially due to the increasing ability of malware writers to produce small, automated changes in their code with every infection in order to avoid antivirus signatures, but it is astounding nonetheless. One particular category of malware that has been prodigiously increasing in the last years is ransomware, which either holds, or pretends to hold, a computer's data for ransom by encrypting it and charging money for the key that is necessary to decrypt it.[25] Ransomware has even become a serious threat for mobile devices as well.[26] One industry player reported 8,800,000 ransomware cases in 2014, up 113% from 2013 and constituting 24,000 attacks per day.[27] Furthermore, ransomware's rise to prominence reflects some wider developments in the malware world, specifically with the use of the Tor network as well as more sophisticated encryption for command-and-control communications.[28] Malware strands are also increasingly adapting to the techniques of security researchers, such as the use of virtual environments to analyze them. In fact, estimates indicate that 28% of malware is now "virtual sandbox aware"[29] and 30% use custom encryption to hide communication of stolen data.[30] Additionally, computers infected with malware continue to be able to be remotely controlled as parts of increasingly stealthy and sophisticated botnets; according to one estimate, such networks

[22] "M-Trends 2015: A View from the Front Lines." *Mandiant* (2015): Web.
[23] "2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.
[24] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.
[25] "2015 Midyear Security Report." *Cisco* (2015): Web.
[26] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.
[27] "2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.
[28] "2015 Midyear Security Report." *Cisco* (2015): Web.
[29] "2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.
[30] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.

constitute 34% of attacks.[31] However, there has also been good news for the threat landscape in 2014, with the GameOver Zeus[32], ZeroAccess[33], and Ramnit[34] botnet takedowns contributing to a significant reduction in the reported number of infected computers worldwide in 2014, from 3,500,000 to 2,300,000.[35] These statistics and trends form part of what computer security experts refer to as the "arms race"[36] between security providers and threat actors. This arms race primarily shows signs up speeding up rather than slowing down, with plenty of victories and defeats for both sides.

2.4 Connected Threat Elements

The brief overview of the cyber threat landscape presented above has focused on statistics and trends regarding vulnerabilities, exploits, and malware. However, there are numerous other elements of the environment which merit consideration in order to attain a fuller picture of the global state of affairs. These include delivery mechanisms such as spam and websites, techniques of exploitation such as social engineering that don't require vulnerabilities, as well as a consideration of the threat actors that are behind the means and methods of compromise. However, an overview of these complementary elements as they relate to Baltic cyber security will also emerge from the following two sections.

[31] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.
[32] "Global Threat Intel Report 2014." *Crowdstrike* (2015): Web.
[33] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.
[34] "Microsoft Security Intelligence Report." *Microsoft* 18 (2015): Web.
[35] Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.
[36] "M-Trends 2015: A View from the Front Lines." *Mandiant* (2015): Web.

3. Baltic Cyber Threat Environment

The global cyber threat environment considerably affects the cyber security of the Baltic States of Estonia, Latvia, and Lithuania. For example, the vulnerabilities found in the software of operating systems, document processors, and web browsers constitute hazards to Estonian users, companies, and governmental agencies as well because of their usage of these programs. Furthermore, web-based attacks and phishing attempts also threaten users in the Baltic States since the global infrastructure of the Internet allows them to connect or be redirected to compromised or fake websites. However, in addition to global threats, individuals and organizations in the Baltics also face more local and targeted threats as well. These include specialized phishing campaigns, targeted intrusion attempts against state institutions, and denial-of-service attacks, among others. The following section will elaborate on the available information regarding national threat landscapes and analyze the degree to which they connect or overlap with each other.

3.1 Estonia[37]

The most relevant source of information regarding the state of cyber security in Estonia comes from the Estonian Information Systems Authority's (EISA) annual report, which has been published since 2012 and has consistently advanced in terms of detail, depth, and utility. As the agency responsible for handling security incidents in Estonia's top-level domain (.ee), EISA has the most comprehensive and authoritative view of the changing national threat landscape[38].

In 2014, EISA reported a similar number of incidents as the year before (1,151 in 2014, 1,164 in 2013), but the severity of incidents increased considerably. The number of security incidents reported by state institutions nearly quadrupled (from 135 in 2013 to 436 in 2014), partially as a result of new reporting requirements that came into force in 2014. EISA noted several features of the global cyber threat environment that strongly affected Estonia as well, namely the Heartbleed and Shellshock vulnerabilities, the appearance of ransomware, and campaigns connected to global events. The Heartbleed vulnerability, whose exploitation is impossible to detect after-the-fact, reportedly affected 5% of servers in Estonia, which included approximately 100 vulnerable servers on the government network. Additionally, the dreaded Cryptolocker and other ransomware strands were encountered in Estonia as well in 2014. These posed a particular danger to institutional hard drives that processed sensitive or personal data and that were not regularly backed up. Finally, EISA also drew attention to the fact that security incidents increasingly involved malware that behaved less maliciously in a virtual environment, mirroring the worldwide trend of sandbox-aware malware development mentioned above.

[37] "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." *Estonian Information System Authority* (2015): Web.
[38] "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." *Estonian Information System Authority* (2015): Web.

The cyber threat environment in Estonia, however, also included various distinctive elements connected specifically to its domain. First, the number of denial-of-service attacks on organizations in Estonia increased considerably (13 in 2013, 22 in 2014) and the quantity of defacements of websites also rose (240 in 2013, 295 in 2014). EISA also reported a leap in the quality of Estonian-language usage in phishing campaigns, meaning that the complexity of Estonian grammar and syntax is no longer a high enough barrier to prevent the effectiveness of this category of cyber threat. Finally, EISA also drew specific attention to the spread of malware by web-based attacks. According to the EISA assessment, a large proportion of websites use common software such as Wordpress or Joomla during initial setup and owners then don't continue to download necessary security updates in the months and years that follow. This leaves them open to defacement while also allowing for the possibility of compromising them to spread malware to site visitors. This proved to be the case with high-profile cases such as the nationwide transportation provider Elron as well as less-publicized incidents. To make matters worse, the complexity of the malware found on compromised websites has also shown signs of advancement, such as by using the IP address range of connections to infect users with slightly different malware strands that depended on their location.

3.2 Latvia[39]

An overview of the state of cyber security in Latvia in 2014 reveals both similarities and differences with Estonia and Lithuania. The primary Latvian body responsible for supporting governmental and private institutions in the field of information security, CERT-LV, outlines the key issues faced by the country in its 2014 report. During the reporting period, CERT-LV processed 3,034 high-priority and 487,055 low-priority incidents, compared to 4,964 and 247,815 in 2013, respectively. Like Estonia, CERT-LV also mentioned the relatively new scourge of ransomware, which first began appearing in November 2014 in the form of a strain called "CTB Locker." Latvia was also severely affected by Heartbleed, which left at least 1,300 Latvian websites in a vulnerable and exposed condition. Furthermore, Latvian citizens' computers were also infected via common Adobe and Java as well as other web browser vulnerabilities. However, unlike the Estonian report, the Latvian document specifically mentions malware known as "banking Trojans" that infect users with the intention of stealing their online banking credentials. Hundreds of computers were affected by this threat, with an unknown Latvian grouping carrying out at least three related attack campaigns during the reporting period. Finally, Latvia was also significantly affected by an e-mail phishing campaign which involved sending spam to a user's entire contact list about the sender being in trouble abroad and needing financial transfers for travel assistance. All in all, clearly there are global cyber threats that were also prevalent in Latvia, but there are also homegrown threats that attempt to subvert Latvian users' Internet usage for financial gain.

[39] "Publiskais Pārskats Par CERT.LV Uzdevumu Izpildi 2014.Gadā." (n.d.): n. pag. Latvijas Universitātes Mātematikas Un Informatikās Instituts; CERT-LV; Aiszardzibas Ministrija, 2014. Web.

3.3 Lithuania[40]

The Communications Regulatory Authority (CRA) of Lithuania is the institution that includes the country's national CERT and that is responsible for the network and information security of Lithuania's cyberspace. CRA provides an annual report of its activities to the Lithuanian government as well as to the public. While it does not go into great detail, this report, is the most accessible and authoritative English-language source of information on the cyber threat landscape in Lithuania.

The number of incident reports that CERT-LT receives on a yearly basis is dramatically higher than Estonia, and has been growing significantly in the last years alone. In 2014, the number of reported incidents totaled 36,136, which is a 43% increase from the 25,337 that were reported in 2013. According to CERT-LT, 11,376 of these, or 315 of the total, are ascribed to malicious software whose primary purpose was to take control of a computer in order to include in it a botnet. CERT-LT also investigated 165 denial-of-service attacks (representing a 27% increase over 2013), most of which were conducted with automated means using botnet resources. CERT-LT also analyzed 4,853 cases of information system compromise (compared to 10,924 in 2013), most of which were also ascribed to botnets attacking poorly secured websites. Finally, CERT-LT reported 13, 827 cases of "security gaps."

The information presented by CRA and its component organization, CERT-LT, does not lend itself to a detailed analysis of the difference between the national and global cyber threat environment. It is clear, however, that several overarching problems connect the two. The worldwide scourge of botnets is clearly a high priority for Lithuania, with CERT-LT even providing tools on its website to combat them. For CERT-LT, botnets also constitute the foundation for a significant proportion of the other cyber threats that it has identified. Web-based attacks, specifically related to unpatched websites, also constitute a significant characteristic of the Lithuania cyber threat landscape, just as they do on a global level. Given the specific focus on botnets in the Lithuanian report, however, it appears that this aspect of the environment in Lithuania is relatively more problematic than it is in the world as a whole.

[40] Lithuania. Communications and Regulatory Authority. *Annual Report 2014*. 2015. Print.

4. Russian Cyber Espionage

While the previous sections have dealt with a variety of different aspects of the global and regional cyber threat landscapes, they have focused on the generally more pedestrian varieties of malware that are primarily used by cybercriminals and other types of malicious actors. However, an understanding of the nature of the Baltic cyber threat environment would not be complete without a consideration of the much more sophisticated and determined campaigns of presumably nation-state sponsored groups known as "advanced, persistent threats" (APTs). These actors and the malware they deploy are of the greatest significance to the foreign relations and security policies of the Baltic States and deserve special consideration. Furthermore, while there have been cases of cyber threats emanating allegedly from actors based in China and Iran, this section of the report will focus on the much more overwhelming quantity of threats that are connected to the actor that each of the Baltic States considers to be the primary threat to their national security – Russia.

The campaigns that Russian APT groups launch are characterized by a focus on stealing information that is relevant for political and strategic decision-making by a state actor, rather than information that can be used for economic gain (such as intellectual property or banking credentials). Generally, these operations are multi-year in duration, characterized by a formal malware development environment, constitute activities that require immense human and financial resources, and are presumably wildly successful in terms of compromises and information stolen. The targets include government ministries, militaries, political think tanks, advanced research institutes, energy companies, and even individual politicians, activists, and journalists in NATO and EU countries as well as in the former Soviet space more generally. Overall, the campaigns are characterized by some combination of the following qualities that can be used for attribution: they target organizations that are directly relevant to Russian strategic interests; they contain Russian-language preference in coding and communications; compilation times of malware variants are almost exclusively during workdays between 8 a.m. and 6 p.m. in the Moscow time zone, and; overlaps in terms of encryption keys or command-and-control infrastructure that is registered in Russia or by Russians. This is the world of Russian cyber espionage, which casts a wide net but has a particularly identifiable focus on the former Soviet Union, including the Baltics.

While many of the following campaigns have been active since at least 2010, Russian cyber espionage has become even more prolific in the last several years. This is at least partially explained by the fact that the security situation in the Europe and the world has deteriorated significantly in the last two years due to the Russia-Ukraine conflict and the resulting tensions between Russia and the West. These frictions have clearly translated into increased cyber activity as well, with the Estonian Information Systems Authority stating publicly that "the number of incidents related to foreign special services has increased significantly" in 2014.[41] The Lithuanian Ministry of National Defence has also attributed a rise in Russian cyber espionage partially to the crisis in Ukraine even before the illegal occupation and annexation of Crimea.[42] Indeed, it

[41] "2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." *Estonian Information System Authority* (2015): Web.

[42] Lithuania. Ministry of National Defence. Second Investigation Department. *Assessment of Threats to National Security*. Vilnius: 2014. Print.

appears that the pace and effectiveness of Russian cyber operations has also led to a greater number of discoveries and analyses of their activities by computer security companies such as F-Secure, Kaspersky Labs, FireEye, GData, Symantec, and others. The following sections provide a brief overview of the largest and most notorious actors and campaigns.

4.1 Snake[43] / Turla[44] / Uroburos[45]

One major cyberespionage campaign was revealed in 2014, when the German information security firm GData published a research paper on an actor that they referred to as Uroburos. As is often the case, several other security companies were tracking or began to track the actor as well, leading to several high-profile follow-up publications by BAE Systems (who called it Snake) and Kaspersky Labs (whose designation was Turla). The latter asserts that hundreds of computers belonging to government, industry, and research institutes in at least 45 countries were compromised with Uroburos. According to BAE Systems' data, Lithuanian organizations were among the most targeted by this actor. For this reason, the APT actor is among the most strategically relevant aspects of the threat environment in the Baltics.

The actors behind Uroburos have created one of the most sophisticated cyber espionage tools that the public has ever seen, and they used it to breach the systems of high-profile targets around the world, with a special emphasis on the regions bordering Russia. The initial infection vectors that were used to compromise these organizations included spear-phishing e-mails with malicious attachments, and several types of watering hole attacks from compromised websites. The exploit code that was used also contained two zero-day vulnerabilities that enabled escalation of privileges on the target system and the ability to execute remote code. These initial breaches led to the victims unwittingly downloading the Trojan backdoor, which proceeded to communicate system information back to the actors over the Internet. If the target was deemed interesting, then additional malware based on target characteristics was delivered. The subsequent Uroburos toolkit itself contains rootkit capabilities, meaning that it establishes a very low-profile and deep foothold in the victim's machine. It contains two file libraries, and the main function of one is simply to open the other. This functionality made it difficult to discover and understand in its entirety. Furthermore, the malware is able to spread in a network, gain access to devices that are not connected to the Internet, and exfiltrate data using a peer-to-peer architecture. This setup also hinders the work of incident response teams, because it is difficult to identify and isolate all the infected nodes. Also, rather than registering domains and servers themselves, the actors behind Uroburos also compromised a number of each in order to use them for command-and-control and data exfiltration.

---

[43] "Snake Campaign: Cyber Espionage Toolkit." *BAE Systems Applied Intelligence* (2014): Web.

[44] "The Epic Turla Operation: Solving Some of the Mysteries of Snake/Uroburos." *Https://securelist.com/analysis/publications/65545/the-epic-turla-operation/*. Kaspersky Labs, 7 Aug. 2014. Web.

[45] "Uroborus: Highly Complex Espionage Software with Russian Roots." *G Data Security Labs* (2014): Web.

The actors then used a network of proxies and VPNs to access those resources, thereby going to great lengths to retain anonymity.

Despite substantial skills and resources directed toward resisting analysis, there are still numerous pieces of evidence pointing to Russian origin in the Uroburos case. First, the command-and-control motherships set the language codepage to 1251, which is used for rendering Cyrillic characters. Second, the compilation code of the backdoor version sent to various victims set the language to Russian. Third, BAE systems analyzed the compilation times and days of the various variants, and found that almost all of them were created between Monday and Friday during working hours in Moscow time. Furthermore, the actor checked for the presence of a virus labeled Agent.BTZ, which had been used in a suspected high-profile Russian attack against the United States Department of Defense in 2008, and didn't infect computers where Agent.BTZ presence was detected. Finally, the choice of attachment names and targeted institutions also reflects Russian strategic interests. Altogether, there is considerable evidence in the public domain to indicate that this is a well-resourced and highly skilled operation that is conducted or at least sponsored and funded by the Russian Federation. Recent reports also indicate that the actors behind Uroburos are still active and advancing, with Kaspersky publishing new information about how the campaign is abusing satellite-based traffic to hide its own command-and-control communication[46].

4.2 The Dukes[47]

Since 2012, numerous computer security firms have been shedding light on an allegedly Russian cyber espionage campaign that utilizes a number of different Trojan backdoors and other types of malware to steal information and credentials from ministries, militaries, parliaments, and other governmental organizations around the world. This group, known as the Dukes, constitutes one of the most extensive and bold examples of Russian cyber espionage to date. One member of the Duke "family," CosmicDuke, had the dubious honor of being named in the annual report of the Estonian Internal Security Service as one of the advanced, persistent threats that successfully breached government systems and considerably affected Estonia's national security in 2014[48]. This disclosure, coupled with what is known about the targeting aims of the rest of the Dukes, makes this threat group an unavoidable and important element of the Baltic cyber threat landscape.

To date, security researchers have discovered nine distinct malware toolsets that are considered to be members of the Duke family: MiniDuke, CosmicDuke, CloudDuke, SeaDuke, OnionDuke, CozyDuke, HammerDuke, PinchDuke, and GeminiDuke. Most of them have been the subjects of extensive research papers in their own right and, while they may merit individual consideration, the format of this report does not allow it. Overall, there is a considerable variety among the Dukes in terms of objectives,

[46] Tanase, Stefan. "Satellite Turla: APT Command and Control in the Sky." *Securelist*. Kaspersky Labs, 9 Sept. 2015. Web.

[47] Lehtiö, Artturi. "The Dukes: 7 Years of Russian Cyber Espionage." *F-Secure Labs Threat Intelligence* (2015): Web.

[48] Estonia. Estonian Internal Security Service. *Annual Review 2014*. By Harrys Puusepp: 2015. Print.

capabilities, and infrastructure. For example, members of the family such as CozyDuke are rather used for massive infection campaigns, while the more recently discovered SeaDuke is much more low-profile and difficult to discover. Most of the campaigns that have been ascribed to the Dukes have had spear-phishing e-mails as their infection vector, but there have also been cases where OnionDuke has been spread using a Tor exit node based in Russia and legitimate websites such as "diplomacy[dot]pl" have been compromised and used to spread CozyDuke. In terms of functionality, the Dukes are toolsets that mostly include first and second-stage Trojans, downloaders, droppers, infostealers, and keyloggers. Analogously, the command-and-control infrastructure is shared or overlapping in some cases and completely distinct in others. For example, CloudDuke is named after the use of cloud-based C2 infrastructure while HammerDuke (or Hammertoss as FireEye has named it) employs stealthy Twitter-based communication protocols with its operators. Furthermore, this group has also leveraged zero-day vulnerabilities such as one in Adobe Acrobat Reader in 2013 to achieve their aims. Finally, most of the members of the Dukes have relatively advanced encryption mechanisms in their communications and also employ anti-detection and anti-analysis elements such as obfuscation and anti-sandboxing.

Researchers at security companies such as F-Secure, Symantec, Kaspersky Labs, BitDefender, and others have been tracking the Duke family since 2013 They point to similarities in the malware strands' functionality, infection vectors, working hours (Monday-Friday Moscow time), command-and-control infrastructure, and (Russian) language patterns evident in coding, which serve as indications that either one actor is behind the family's operation or, at the very least, that the various actors are working together closely. The choice of high-profile strategic targets in NATO and EU countries, as well as the discovery in 2014 of a Tor exit node, further indicate that the malware has been deploy by a Russian group in support of Russia's strategic interests. Furthermore, the complexity and duration of the campaigns highlight the extensive amount of resources, both in terms of technical skill and hours worked, that has been necessary to conduct this level of espionage. The accrued evidence leads to the tentative conclusion that the most plausible theory of the group's identity is that it is either a state-sponsored Russian cybercriminal syndicate or even a branch of the Russian security services. The actors behind the Dukes, whoever they may be, are still very active. The most recent analysis detailing new aspects of two early versions and linking all members of the Dukes together over a seven-year period emerged only days before the publication of this report.

4.3 APT 28[49] / Pawn Storm[50]

2014 was a prominent year for discoveries of purportedly Russian cyber espionage campaigns. During the year, computer security firms FireEye and Trend Micro both published research papers detailing different but overlapping aspects of the operations of an actor that they refer to as APT 28 and Pawn Storm, respectively. As with many of the other cases of Russian cyber espionage, the targets of this group include, *inter alia*, governmental institutions in Eastern European countries, Euro-Atlantic security institutions such as NATO and the OSCE, and the ministries and militaries of Caucasus states. One particular domain that was used for phishing attempts by this threat actor attempted to use a military exercise called Baltic Host, which is conducted annually in the Baltics with the participation of the United States, as a compromised domain (baltichost [dot] org) to target involved individuals. This indicates that Baltic governments are targeted and means that the actor has taken its place in the Baltic cyber threat landscape.

The actors behind APT 28 and Pawn Storm utilize a variety of techniques, tools, and procedures to compromise their targets. The unifying factor behind the various campaigns that this actor has conducted appears to be the use of a Trojan called Sofacy, which acts as the backdoor that enables further infection with second-stage downloaders that eventually lead to a set of modular implants that FireEye refers to as Chopstick. These tools enable the entire range of espionage activities, from credential theft and keylogging to file exfiltration. As with other campaigns, this one employs malicious e-mail attachments that exploit known vulnerabilities to gain system access. It has also demonstrated that it possess “zero-day” vulnerabilities such as one Java weakness that it employed in 2015. However, this threat actor has displayed an advanced degree of social engineering and “next-level” phishing capability, which it uses both as initial infection mechanisms as well as for credential and data theft that does not involve infection. While APT 28 has shown that it is particularly adept at faking Outlook Web Access sites to harvest credentials and compromise accounts, it also regularly employs faked websites of security conferences and international organizations in order to do so as well. The actor has also been known for breaching several legitimate Polish websites, including that of a power exchange, which delivered Sofacy to addresses of a certain preconfigured IP address range. APT 28 has also added iOS and Linux targeting ability since it started its activities in 2007. Interestingly, neither company provides much detail regarding the command-and-control infrastructure employed by this group.

The two reports about APT 28 or Pawn Storm also provide different accounts of targets as well. Interestingly, while FireEye focuses on institutions such as ministries of defense and internal affairs, Trend Micro has continued to analyze the activities of Pawn Storm in relation to individuals. Using almost 12,000 unique credential phishing attempts, it has discovered that the group behind the malware tools and phishing attempts is also targeting quite a variety of media figures and activists in Russia and elsewhere, including the likes of Pussy Riot and journalists in various Russian media

[49] "APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye* (2014): Web.

[50] Loucif Kharouni, Feike Hacquebord, Numaan Huq, Jim Gogolinski, Fernando Merces, Alfred Remorin, and Douglas Otis. “Operation Pawn Storm: Using Decoys to Evade Detection.” *Trend Micro Forward-Looking Threat Research Team* (2014): Web

outlets. This observation adds depth to the objectives of the group; clearly, it is interested in not just foreign military and diplomatic threats to the regime but also domestic dissidents and relatively independent media organizations. This type of intelligence is necessary if the consumer is worried about regime preservation.

As with the other cyber espionage operations, a variety of indicators point to the Russian origin of the actors behind the technology. Of course, the choice of targets, including domestic ones, provides one line of reasoning. The targeting preferences are once again supported by Russian language usage in code compilation as well. FireEye also analyzed the compilation dates and times and, predictably enough, they lined up almost perfectly with weekday working hours in the Moscow time zone. Finally, Trend Micro has identified a substantial rise in the targeting of Ukrainian elites since the start of the Russian invasion. The actor has continued to operate since 2007 and is seemingly unhindered by publications about its activities by security companies, with Trend Micro uncovering its use of a Java zero-day in July 2015.[51]

4.4 Red October[52] / Cloud Atlas[53]

In October 2012, a particularly hot month, security specialists from Kaspersky Labs launched an investigation into a series of cyber attacks against various types of governmental institutions primarily in Eastern Europe and the former USSR. They uncovered a unique and sophisticated cyber espionage network that had been active since 2007 and was in operation at the time they published their research. Embassies of unnamed countries in Latvia and Lithuania were among the publicly identified organizations that had been breached by these actors, marking Red October as one of the most dangerous aspects of the Baltic cyber threat landscape.

The actors behind Red October used spear phishing emails that contained a malicious attachment to their targets to achieve an initial foothold in their target systems. The document contained code that exploited vulnerabilities in Microsoft Word and Excel programs to launch a custom Trojan on victim workstations. The dropper then established command-and-control communications with various servers and websites in order to provide system information and load further spying software if the target was deemed interesting. Kaspersky identified 30 modules containing approximately 1,000 different files that were used to analyze the victim's system, identify files of interest, and pack, encrypt, and exfiltrate troves of confidential information via the Internet.

The modules consisted of two different types of malware, differentiated by whether they worked only in online mode and stayed purely in system memory or whether they also saved files to disk. There were also specific modules that were capable of compromising mobile devices as well as network equipment. Additionally, there was

[51] "Operation Pawn Storm: Fast Facts and the Latest Developments." *Security News*. Trend Micro, 18 Aug. 2015. Web.
[52] "“Red October” Diplomatic Cyber Attacks Investigation." *SecureList*. Kaspersky Global Research and Analysis Team, 14 Jan. 2013. Web.
[53] "Cloud Atlas: RedOctober APT Is Back in Style." *SecureList*. Kaspersky Global Research and Analysis Team, 10 Dec. 2014. Web.

one particularly noteworthy module that introduced an almost foolproof way to get back into the system if the actor was caught and expelled. The command-and-control infrastructure was also quite advanced, consisting of a variety of websites hosted on numerous levels of compromised servers based primarily in Germany and Russia that served as proxies ensuring the anonymity of the actors behind the campaign.

The actors behind the Red October threat also attempted to avoid attribution by using exploit code that had been developed and used outside of their campaign. However, Kaspersky identified numerous artifacts in the kit that pointed to Russian-speaking authors. Additionally, the location of the C2 infrastructure (in the case of servers) and registering parties (in the case of domains) constitutes evidence pointing to Russian actors. The sophistication and timeframe of the campaign indicates substantial resources, both human and financial, were at the actors' disposal. Finally, the choice of targets betrays no cybercrime attempts for monetary gain and almost completely matches the strategic interests of the Russian Federation. Evidence points to Russian state-sponsored cyber espionage in this case.

Interestingly, after initial public identification, the actors behind Red October went quiet for nearly two years. However, Kaspersky reports that they re-emerged at the end of 2014 with new methods that included cloud-based C2 infrastructure. The new designation for the APT actor is Cloud Atlas, and the actor is still believed to be active at the time of publication.

5. Industrial Control Systems Cyber Security

Thus far, the report has concentrated on the global and Baltic cyber threat landscape by focusing on threats that are primarily directed at workstations, servers, and websites that possess information that can be stolen or held for ransom by the attackers for financial or political gain. However, this report would not be complete if it did not at least consider cyber threats to critical infrastructure, particularly those "supercritical" sectors that deal with energy, water, and raw material creation/processing/distribution as well as telecommunications and banking. These are the sectors that, if attacked, would cause massive physical damage and potentially even loss of life. Such attacks would constitute strategic-level threats to international security that could escalate into conventional crises and wars. These types of threats are enabled by the increasing adoption of ICT-based industrial control systems, which have already been the targets of attacks like the notorious Stuxnet attack on Iran's nuclear infrastructure in 2008. Most recently, in 2014 a German steel plant was compromised and attacked, with subsequent failures preventing the shutdown of two large furnaces, resulting in "massive" damage to the facility.[54] Fortunately, no lives were lost in that incident. However, events such as these prove that attacks on such systems are taking place today, and could potentially happen in the Baltics as well.

5.1 Threats, Exposures, and Attacks

There are a variety of threats that exist to critical infrastructure providers around the world that rely on industrial control systems. First, like other types of software, the code base for industrial control systems software is also often imperfect in security terms. New vulnerabilities are identified and disclosed on a regular basis. In fact, several new vulnerabilities have been made public within the month preceding the publication of this report[55]. Second, the systems in use are often very old so-called "legacy" systems that in many cases have not been upgraded for years or even decades. In these cases, their primary protection is considered to be that they are disconnected from other computer systems and from the Internet more broadly. However, this is manifestly not the case worldwide. Project Shine, a research effort conducted on their own time by two IT professionals, used a specialized search engine tool called Shodan to reveal that over 2,000,000 Supervisory Control and Data Acquisition (SCADA) systems are connected and openly accessible from the Internet.[56] While these also include more pedestrian devices such as traffic and security cameras, a large proportion of them still belonged to critical infrastructure providers. Only a small percentage of those identified systems are in the Baltics. However, this still comes out to 1,571 systems in Estonia, 2,093 in Latvia, and 1,951 in Lithuania.[57] Third, while there have only been a few recorded cases of physical damage, attacks against SCADA systems are growing dramatically year-over-year. One report by Dell asserts

[54] Zetter, Kim. "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever." *Security*. Wired Magazine, 8 Jan. 2015. Web.
[55] Paganini, Pierluigi. "ICS-CERT Warns of Zero-Day Vulnerabilities in SCADA Systems." *Security Affairs* (2015): Web.
[56] "Project Shine Findings Report." *Infracritical* (2014): Web.
[57] "Project Shine Findings Report." *Infracritical* (2014): Web.

that it saw 92,676 attacks on SCADA systems in 2012, with that number increasing to 163,228 in 2013 and a whopping 675,186 in 2014.[58] The report specifically states that 202,322 of the attacks against SCADA systems took place in Finland[59], which is an important partner to the Baltic States in terms of energy provision. This alone should give the Baltics cause for concern and provide impetus for information sharing and cooperation.

5.2 Energetic Bear / Dragonfly[60]

In late 2013 and early 2014, several security companies published reports on an actor that was conducting breaches of systems belonging to companies in the oil, gas, defense, and other critical infrastructure sectors. In total, the actor was confirmed to have compromised over 2,000 companies in 84 countries around the world. The actor, referred to as Energetic Bear by Crowdstrike and as Dragonfly by Symantec, appeared to be most interested in strategic plans and intellectual property related to oil and gas projects. It employed kits that are known as Havex and SYSMain remote access tools. Initially it was thought that the primary infection vectors were, predictably enough, malicious e-mails and compromised websites. However, further research that followed the initial disclosures indicated that the actor had also breached the systems of three companies that provided software for industrial control systems. They inserted Trojans into the products offered by the ICS providers, whose customers used automatic updates downloaded from their website to make sure they had the newest versions. When those customers downloaded the updates, they were automatically infected. While this activity was noticed on average roughly 24 hours after in each case, it resulted in at least 250 companies being breached. Most disturbingly, the attackers were able to do more than just steal information; Symantec reports that they also possessed the capability to "sabotage" the control systems of compromised companies. So, while this actor showed restraint by not doing so, the possibility existed and may have depended on the political context. Massive economic damage or loss of life may have been the result. Interestingly, after its activities were publicly illuminated, the actor retreated from the use of its command-and-control infrastructure and kept a low-profile for several months.[61] As is usually the case with such attackers, however, they resurfaced with different targets, including financial ones, and a new C2 infrastructure.[62] This case could be a harbinger of what is to come in the future of the Baltic and global cyber threat landscape.

---

[58] "2015 Dell Security Annual Threat Report." *Dell* (2015): Web.
[59] "2015 Dell Security Annual Threat Report." *Dell* (2015): Web.
[60] "Dragonfly: Cyberespionage Attacks Against Energy Suppliers." *Symantec Security Response (*2014): Web.
[61] Ilyin, Yuri. "Still Around: Energetic Bear / Crouching Yeti APT Is Not Going Away." *Kaspersky Lab Business* (2015): Web.
[62] Ilyin, Yuri. "Still Around: Energetic Bear / Crouching Yeti APT Is Not Going Away." *Kaspersky Lab Business* (2015): Web.

6. Analysis and Recommendations

The preceding sections make clear that cyber threats are continuing to become faster, more complex, and more numerous. Cybercrime pays, and individuals as well as groups will continue to be drawn to the relatively easy money that can be made using social engineering and malicious code. However, the Baltics—perhaps as a result of their relative lack of affluence—do not rank among the countries with the highest levels of cybercrime, especially compared to other Western European and North American states[63]. This may appear fortunate, but the Baltics face a much more serious cyber threat in the form of Russian cyber espionage.

In light of increased tensions due to the Russian invasion of Ukraine, Russian cyber espionage has grown to become a very significant danger to the Baltics. There is now significant evidence that Russia has invested heavily into offensive cyber capabilities over the last decade. These capabilities include developing and deploying malware, taking over websites and servers for command-and-control communication, and creating phishing websites or social engineering schemes in order to gain access to data and systems of foreign governments and companies (or contracting proxies to do so). Furthermore, given their success rate, it is likely that these capabilities are now an integral part of the toolset that the Russian Federation uses to develop its foreign and security policy postures and advance its own strategic interests. Cyber capabilities fit neatly into the framework of the Gerasimov Doctrine of asymmetrical warfare that has been influential in Russia since 2013, and that can be used as part of broader campaigns of information warfare. The ultimate aim of the Russian Federation is political and economic domination of the former Soviet space. Offensive cyber capabilities, including breaching networks for the purpose of espionage, enable Russia to achieve an information advantage over those that it considers to be its enemies or its rightful client states. The type of information that could be exfiltrated through such cyber espionage includes, but is not limited to, details about: military procurement plans, ongoing (counter)intelligence operations, sensitive diplomatic negotiations, future macroeconomic plans, strategic exercises of all kinds, and much more. Furthermore, actors that are working in Russia's strategic interests in cyberspace are continuing to operate with impunity, and new dimensions of the threat have continued to emerge over the course of the last few years. This report has endeavored to review part of the progression of several such actors, and their behavior has continued to become more aggressive as time has passed. Based on available evidence, this threat will not go away any time soon.

Taken together, the cyber threats identified and described in this report constitute a serious problem for the internal and international security of Estonia, Latvia, and Lithuania. Today, the economic functioning and even political stability of any of the three countries could be significantly undermined by a determined and well-resourced set of actors. The Baltics should consider themselves fortunate that they have not had to manage any large-scale cyber crises in the last eight years. However, it is crucial that the Baltic States do not rest on their laurels and good fortune, but continue to move

[63] "Net Losses: Estimating the Global Cost of Cybercrime." *Economic Impact of Cybercrime II*. McAfee and Center for Strategic and International Studies, June 2014. Web.

forward with their domestic, regional, and global cyber cooperation in order to counter these threats.

Domestically, each country must continue to improve their resilience to cyber threats by, among other things, educating individuals, establishing baselines and standards for industries, enhancing public-private partnerships, and increasing cyber capabilities in governmental institutions. Importantly, all three countries have national cyber security laws or strategies that are relatively high-quality and that outline the most important ways forward at the national levels. However, for Latvia and Lithuania, there is currently considerable political momentum for increasing defense budgets for the next several years (unlike Estonia, which is one of the few NATO countries that already contributes 2% of GDP to defense). While most of these resources will understandably be devoted toward conventional arms, some of it should be devoted to improve their national cyber security capabilities. For Estonia, on the other hand, it is critical that there continues to be a substantial investment of human resources in clarifying and improving domestic crisis response procedures, including by simplifying the legal situation.

At the regional level, cooperation needs to continue to be more formalized. The Baltic States have been negotiating a memorandum of understanding (MoU) for years, but have yet to sign it, despite rhetorical support at the highest political levels.[64] This agreement would provide the basis for additional development of capabilities such as channels to rapidly exchange classified information relevant to threats against national security. It would also undoubtedly improve day-to-day information sharing, which is today mostly reliant on connections and trust at the personal level. Furthermore, the Baltic States need to work toward an understanding of the interconnectedness of critical infrastructure among the three states and their neighbors. As it stands, an extensive attack on the energy, transportation, telecommunications, or banking systems of one of the Baltics could exert serious negative effects in the other two or even more widely in the region. Considering that the Baltics share Alliance ties and broadly similar strategic threat assessments, cyber attacks against interconnected infrastructure would undoubtedly be tempting targets for those who would threaten them. For this reason, the countries need to move toward greater preparedness for such events by formalizing cooperation and undertaking networking, policy-level, and technical-level projects.

At the global level, the Baltics can strengthen their cyber security by continuing to be good partners for other nations and companies with respect to sharing information, providing assistance when resources permit, and engaging proactively and cooperatively in global cyber security policy debates. These kinds of activities will generate political capital and inspire reciprocity, which can in turn be used to advance the skills and resources of domestic actors. By all estimates, the global usage of ICTs will continue to grow and the Baltics should pursue capacity-building at home as well as around the world in order to promote an open, free, and secure cyberspace for generations to come.

[64] "Joint Statement." Prime Ministers' Council of the Baltic Council of Ministers. December 5, 2014.

7. Conclusion

This report has endeavored to shed light on the state of the global cyber problem, provide an overview of the experience of the Baltics in this context during the last year, and identify the most relevant cyber threats to the regional security of the Baltics. It has become clear that cybercriminals and nation-state sponsored actors alike are becoming increasingly adept, numerous, and sophisticated. The threat to critical infrastructure through the use of computers is real and growing. Decision-makers and analysts should not ignore any of these threats; if anything, their attention to them should continue to grow and advance in pace with the increase in threats. The ways to counter these threats, however, are not changing but require more human and financial resources. Adversaries of various kinds are continuing to do so; governments and businesses in the Baltics cannot afford to fall behind. Rather, they should take the initiative and attempt to get ahead of the threats whenever and wherever possible. There is no doubt that cyber security will only continue its ascent to prominence in domestic and international affairs, both in the Baltics and beyond.

Works Cited

"2014 Annual Report Cyber Security Branch Of the Estonian Information System Authority." *Estonian Information System Authority* (2015): Web.

"2015 Annual Security Report." *Cisco* (2015): Web.

"2015 Midyear Security Report." *Cisco* (2015): Web.

"2015 Data Breach Investigations Report." *Verizon* (2015): Web.

"2015 Dell Security Annual Threat Report." *Dell* (2015): Web.

"2015 Internet Security Threat Report." *Symantec* 20 (2015): Web.

"APT28: A Window into Russia's Cyber Espionage Operations?" *FireEye* (2014): Web.

"Cloud Atlas: RedOctober APT Is Back in Style." *SecureList*. Kaspersky Global Research and Analysis Team, 10 Dec. 2014. Web.

"Dragonfly: Cyberespionage Attacks Against Energy Suppliers." *Symantec Security Response (*2014): Web.

"The Epic Turla Operation: Solving Some of the Mysteries of Snake/Uroburos." *Https://securelist.com/analysis/publications/65545/the-epic-turla-operation/*. Kaspersky Labs, 7 Aug. 2014. Web.

Estonia. Estonian Internal Security Service. *Annual Review 2014*. Compiled by Harrys Puusepp: 2015. Print.

"Global Threat Intel Report 2014." *Crowdstrike* (2015): Web.

"HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group." *FireEye Threat Intelligence* (2015): Web.

"Joint Statement." Prime Ministers' Council of the Baltic Council of Ministers. December 5, 2014.

Lehtiö, Artturi. "The Dukes: 7 Years of Russian Cyber Espionage." *F-Secure Labs Threat Intelligence* (2015): Web.

Lithuania. Communications and Regulatory Authority. *Annual Report 2014*. N.p.: n.p., 2015. Print.

Lithuania. Ministry of National Defence. Second Investigation Department. *Assessment of Threats to National Security*. Vilnius: 2014. Print.

Loucif Kharouni, Feike Hacquebord, Numaan Huq, Jim Gogolinski, Fernando Merces, Alfred Remorin, and Douglas Otis. "Operation Pawn Storm: Using Decoys to Evade Detection." *Trend Micro Forward-Looking Threat Research Team* (2014): Web

Ilyin, Yuri. "Still Around: Energetic Bear / Crouching Yeti APT Is Not Going Away." *Kaspersky Lab Business* (2015): Web.

"Magnified Losses, Amplified Need for Cyber-Attack Preparedness: TrendLabs 2014 Annual Security Roundup." *Trend Micro* (2015): Web.

Marinos, Louis. "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber-threats." *European Network and Information Security Agency* (2014): Web.

"Microsoft Security Intelligence Report." *Microsoft* 18 (2015): Web.

Menn, Joseph. "Security Experts Hack into Moving Car and Seize Control." *Markets*. Reuters, 21 July 2015. Web.

"M-Trends 2015: A View from the Front Lines." *Mandiant* (2015): Web.

"Net Losses: Estimating the Global Cost of Cybercrime." *Economic Impact of Cybercrime II*. McAfee and Center for Strategic and International Studies, June 2014. Web.

"Operation Pawn Storm: Fast Facts and the Latest Developments." *Security News*. Trend Micro, 18 Aug. 2015. Web.

Paganini, Pierluigi. "ICS-CERT Warns of Zero-Day Vulnerabilities in SCADA Systems." *Security Affairs* (2015): Web.

"Project Shine Findings Report." *Infracritical* (2014): Web.

"Publiskais Pārskats Par CERT.LV Uzdevumu Izpildi 2014.Gadā." (n.d.): n. pag. Latvijas Universitātes Mātematikas Un Informatikās Instituts; CERT-LV; Aiszardzibas Ministrija, 2014. Web.

""Red October" Diplomatic Cyber Attacks Investigation." *SecureList*. Kaspersky Global Research and Analysis Team, 14 Jan. 2013. Web.

"Snake Campaign: Cyber Espionage Toolkit." *BAE Systems Applied Intelligence* (2014): Web.

Tanase, Stefan. "Satellite Turla: APT Command and Control in the Sky." *Securelist*.

Kaspersky Labs, 9 Sept. 2015. Web.

"Terminology." *CVE – Common Vulnerabilities and Exposures.* Mitre Corporation, 27 Feb. 2013. Web.

"Uroborus: Highly Complex Espionage Software with Russian Roots." *G Data Security Labs* (2014): Web.

Welch, Ashley. "U.S. Officials Warn Medical Devices Are Vulnerable to Hacking." CBS News, 4 Aug. 2015. Web.

Zetter, Kim. "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever." *Security*. Wired Magazine, 8 Jan. 2015. Web.

Zetter, Kim. "Is It Possible for Passengers To Hack Commercial Aircraft?" *Security*. Wired Magazine, 26 May 2015. Web.

International Centre for Defence and Security
Narva mnt 63/4 East Building, Tallinn 10152, Estonia
info@icds.ee, www.icds.ee
Tel.: +372 6949 340