ENC
ENCouncil.org
European Neighbourhood Council

ENC ANALYSIS

Russian Cyberwarfare Capabilities: Assessing the Threat for Ukraine's Critical Infrastructure

September 2018

Authors: Andreas Marazis, Robert Kothe

ABOUT THE AUTHORS

Andreas Marazis

Head of Research for Eastern Europe and Central Asia
European Neighbourhood Council (ENC)

Robert Kothe

Research Assistant at European Neighbourhood Council (ENC)

"We face a dangerous, unpredictable, and fluid security environment, with enduring challenges and threats from all strategic directions; from state and non-state actors; from military forces; and from terrorist, cyber, and hybrid attacks."

Brussels Summit Declaration, 11 July 2018

The latter non-conventional way of warfare has become the norm and a daily headache for post-Soviet conflict-affected countries as well as for several EU member states. Among them, Ukraine is considered by many experts to be the testing ground for Russia's 'subversion war'[1], to borrow Messner's concept. Cyber warfare is a long-term psychological strategy aiming to wane the adversary by demoralising the spirit of citizens and thus undermining the legitimacy of the authorities.

For many post-Soviet states, including Ukraine, the choice lies between looking either to the West at possible Euro-Atlantic integration into the European Union (EU) and the North Atlantic Treaty Organization (NATO) or moving back into the Eurasian sphere dominated by the Russian-led Eurasian Economic Union (EEU) project. Just like Estonia, Georgia, and Kyrgyzstan fell victim to sophisticated and damaging cyber-attacks after acting against the wishes of Russia from 2007 to 2009[2], similarly Ukraine provoked Moscow's wrath in the form of an invasion by conventional and cyberspace forces similar to the ones we saw in Georgia.[3] Since March 2014, Russia has deployed cyber proxies equipped with sophisticated malicious software (malware), who have and are willing to cripple critical infrastructure that is vital to the Ukrainian state and population.

Critical infrastructure sustains the vital function of society, protection of basic needs, and gives its people the feeling of safety and security. Acts to undermine critical infrastructure are destabilizing and create chaos within a state's society. After such an attack, society cannot trust that the state can protect its basic needs. It is a maximum show of covert force in the cyberspace in peacetime, and therefore cyber sabotage has become so useful for Russia in Ukraine. It destabilizes the country, sends a political message, and gives Russian hackers the chance to test and prove their capabilities.[4]

There is compelling evidence that suggest that Russia conducted its first major cyber sabotage attack on Ukraine to cut power in Yuzivska region (Easter Ukraine) where Kyiv had hoped it would begin fracking operations. Shell had signed a production sharing agreement[5] to invest in Ukrainian fracking in Yuzivska prior to the Russian invasion, which would have seen self-sufficiency for half of Ukraine's energy consumption. Chevron did the same in the Olesska region (Western Ukraine) that was supplied by the electrical distribution companies that were targeted in the December 2015 attack. Both companies froze their activities in March 2014, and Russian has remained the energy hegemon of the

[1] Ofer Fridman (2018) "Russian 'Hybrid Warfare': Resurgence and Politicisation", Hurst & Co., London, pg. 66-70
[2] http://www.eujournal.org/index.php/esj/article/viewFile/2941/2770
[3] https://geostrategy.org.ua/images/blok_XXI-engl-last.pdf pg. 8-14
[4] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
[5] https://www.euractiv.com/section/energy/opinion/russia-s-silent-shale-gas-victory-in-ukraine/

region.[6] Critical infrastructure serves as a dynamic target in Russian hybrid warfare as it ensures geopolitical and economic damage, while also causing social instability and distrust in the target's government.

Ukrainian critical infrastructure has been targeted on ten reported occasions from May 2014 to July 2018. The Ukrainian critical infrastructure sectors targeted in Russian attacks include: **energy distribution**, **transport**, **banking**, **financial market**, and **drinking water supply**. Eight of the attacks reported relied on the use of malware. The latter follow a pattern consistent with the Russian **Advanced Persistent Threats (APT) 28**, also known as *Tsar Team*[7]. They begin infiltrating networks through spear-phishing email campaigns, which either mimic the domains of real state institutions or link to infected domains of actual state institutions.[8] Once an employee or user clicks on the link, the system is infiltrated, and malware is installed with a backdoor for later use called *zero-day vulnerability*. When the threat agent has conducted enough reconnaissance on the network and its target (e.g. passwords) they are ready to begin their assault. They launch persistent Distributed Denial-of-Service (*DDoS)* attacks to overwhelm the network, which lock out access for the hacker's target and gives them time to exfiltrate data and commit cyber espionage. The assault ends with the use of a *KillDisk*, to rewrite the infected systems files with random data, making the system unusable after and erasing evidence of the hacker infiltration.[9] [10]

The pro-Russian hacktivist groups **CyberBerkut** and **GreenDragon** both accessed the system of a Ukrainian bank in July 2014. CyberBerkut mimicked the tactics of Green Dragon, who had used a *DDoS* attack to take down PrivatBank's website days earlier, and disclosed confidential information including passport data, account information, and phone numbers.[11]

Yet the danger to Ukrainian critical infrastructure comes from APT 28, a cyber proxy with reported ties to the Russian Main Intelligence Directorate (GRU). According to FireEye[12], they have conducted attacks on targets that would benefit the Russian government since 2007 and not for economic benefit like most cyber criminals.[13] APT 28 deployed *BlackEnergy* in December 2015, an updated version of the malware that was used on Georgian critical infrastructure in 2008, after being six months inside the systems. They accessed the control centres of three Ukrenergo electricity distribution companies that

[6] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn91
[7] https://www.fireeye.com/current-threats/apt-groups.html
[8] https://www.scmagazine.com/report-russia-may-be-readying-cyberattack-against-ukraine/article/776676/
[9] https://www.scmagazine.com/blackenergy-back-telebots-launch-malicious-toolset-reminiscent-of-earlier-attacks/article/579319/
[10] https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html
[11] https://themoscowtimes.com/articles/cyber-berkut-hackers-target-major-ukrainian-bank-37033
[12] FireEye is a publicly listed enterprise cybersecurity company that provides products and services to protect against advanced cyber threats, such as advanced persistent threats and spear phishing.
[13] https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html

provided power for Kyiv and the Ivano-Frankivsk oblast. They simultaneously and remotely opened 30 distribution substations at once through the control centres of Supervisory Control and Data Acquisition (SCADA)[14] systems. This caused more than 700,000 people to lose power and subsequently heat for six hours, which cybersecurity experts have said was more than what the cyber proxy expected to do in terms of damage. [15] [16]

BlackEnergy's use on Ukrainian critical infrastructure is not limited to the December 2015 attack. A month after, *BlackEnergy* was found in the networks of Boryspil International Airport in Kyiv, but was disabled before its zero-threat vulnerability was exploited. Ukrainian military officials traced the origins of the malware back to Moscow, where FireEye believes APT 28 is based.[17] [18]

APT 28 is also believed to be behind the attack on another power facility in Northern Ukraine in December 2016, but only targeted a single transmission substation. Instead of using *BlackEnergy*, the cyber proxy deployed a new malware, *Industroyer*, specifically designed for manipulating industrial control systems while also providing more stealth.[19]

Researchers have also found parallels between much smaller attacks conducted on Ukrainian mining organizations and railway systems in November and December 2015 due to the presence of *KillDisk* and a similar malware to *BlackEnergy*.[20] In July 2018, Ukrainian Secret Services (SBU) were able to stop an attempted cyber sabotage attack on a Ukrainian drinking and critical water supply station. The network equipment of the Aul Chlorotransfer Station in the Dnipropetrovsk province was targeted by a malware that is very similar to *BlackEnergy* called *VPN Filter*, which has been reported to have been created by APT 28.[21] The chlorine distillation station is Ukraine's only active station; therefore the attack would have had a severe impact on the Ukrainian state and society.

The 2017 *NotPetya* attacks were specially aimed at Ukraine, despite infecting businesses worldwide, and affected five different critical infrastructure sectors, the Ukrainian government, the Chernobyl monitoring station, and businesses across the country. Ukrenergo was again targeted, but the malware was unable to affect power supplies. Both the banking and financial service sectors were targeted. The National Bank of Ukraine and

---

[14] Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to control industrial processes locally or at remote locations, monitor, gather, and process real-time data, directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software and record events into a log file.

[15] https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA

[16] https://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/

[17] https://www.independent.co.uk/news/world/europe/ukraine-cyberattack-boryspil-airport-kiev-russia-hack-a6818991.html

[18] https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html

[19] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[20] https://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/

[21] https://www.threatshub.org/blog/ukraine-blocks-vpnfilter-attack-against-core-country-water-system/

the largest state-owned lender, Oschadbank, systems were both disrupted, as well as many ATMs across the country. Disruption also occurred in Kyiv's subways electronic payment systems and the country's largest airport, Boryspil International Airport.

The *NotPetya* attack was not meant to financially exploit its target, but instead to disrupt and cause financial damage. The malware disguised itself as a *ransomware*[22], but it was in fact a form of malware called a wiper which is specifically designed to destroy and disrupt data. 75.2% of the infected computers worldwide were found in Ukraine, which displays the pronounced geographical targeting of the virus. The attack reportedly cost Ukraine 0.4% of its yearly GDP within thirty minutes. [23]

The virus fits the pattern of Russian attacks on critical infrastructure due to the extensive economic damage; therefore it was no surprise that the United States' CIA recently indicted three Russians and blamed the GRU for the attack.[24] European intelligence services blamed Russia for the attack as well.[25] This means that it is likely that APT 28 was behind this massive assault on Ukrainian critical infrastructure as well. Three months later, a malware sharing much of the same code as *NotPetya*, called *BadRabbit*, affected flights at the international airport in Odessa and the electronic payment systems in the Kyiv metro.[26]

Attacks on critical infrastructure are also supplemented by cyber espionage campaigns that search for potential targets for cyber sabotage and seek out the staff members of critical infrastructure. In February 2017, a cybersecurity firm found evidence of a Russian cyber espionage campaign that compromised more than 60 Ukrainian targets, which included critical infrastructure sectors like the energy ministry and a firm that designs remote monitoring systems for oil & gas pipelines.[27]

Russian threat agents are targeting the specific systems that control and monitor critical infrastructure in cyber espionage campaigns, and then conducting cyber sabotage with perfected tools to conduct cyberwarfare on critical infrastructure like *Industroyer*. APT 28 waited six months before it carried out its attack in December 2015; therefore no one knows when the next attack will be or if the malware and *zero-day vulnerability* are already there. *Zero-day vulnerabilities* are rarely discovered right away and can even take years to be found.[28]

---

[22] Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
[23] http://euromaidanpress.com/2017/07/25/money-is-not-always-the-answer-what-do-we-know-about-latest-cyber-attack-on-ukraine/
[24] https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html
[25] http://www.atlanticcouncil.org/blogs/ukrainealert/it-s-the-holiday-season-again-will-ukraine-be-ready-for-the-next-cyberattack
[26] https://www.reuters.com/article/us-cyber-summit-ukraine/ukraine-says-notpetya-hackers-likely-behind-badrabbit-malware-idUSKBN1D02D1
[27] https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-charges-russia-with-new-cyber-attacks-on-infrastructure-idUSKBN15U2CN
[28] https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

It should also be noted that CyberBerkut conducted attacks on the Ukrainian Electoral Commission hours prior to the 2014 Ukrainian Presidential Election and infected the election networks with malware that would have deleted the election's results. The Ukrainian Security Service was able to remove the malware just in time for the election to go on smoothly, but things could have gone differently.[29] The United States is currently discussing whether or not to make its election infrastructure part of its critical infrastructure. [30]

Regardless of the various reports and evidence provided to show their responsibility in these attacks, Kremlin has always denied its offensive cyberspace capabilities claiming plausible deniability through their use of cyber proxies and tacit support of hacktivist groups.[31]

For the EU, attacks on Ukrainian critical infrastructure have resulted in serious implications for cybersecurity policy. Numerous EU member states have been targeted by Russian cyber espionage campaigns that infiltrated the networks of their critical infrastructure, and the same malware that was used in Ukraine was found in Swedish industrial control system networks.[32] Hybrid and cyberwarfare measures like state sponsored cyber sabotage are increasing year by year and could become a common occurrence in the future. The EU should therefore take the time to learn the lessons that it can from Ukraine, before Russia, or any other state actor, tries to test their capabilities.[33]

Policy Recommendations

Ukraine's experience with Russian state-sponsored attacks on its critical infrastructure has been comprehensive and has targeted every sector that European Union Agency for Network and Information Security (ENISA)[34] considers mandatory for member states and

[29] https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Weedon_08.pdf
[30] https://epic.org/foia/dhs/cybersecurity/russian-interference/EPIC-17-03-31-DHS-FOIA-20180315-Production.PDF
[31] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
[32] United Kingdom warning of Russian state actors infiltrating critical infrastructure through supply chains. Accessed at https://tech.newstatesman.com/business/russia-uk-critical-infrastructure and BlackEnergy 2 found on the industrial control system networks in Sweden. Accessed at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf
[33] http://securityaffairs.co/wordpress/33448/cyber-warfare-2/cyber-warfare-balance-of-power.html
[34] The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Heraklion Crete. The Agency works closely together with Members States and private sector to deliver advice and solutions. This includes, the pan-European Cyber Security Exercises, the development of National Cyber Security Strategies, CSIRTs cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, and identifying the cyber threat landscape, and others. ENISA also supports the development and implementation of the European Union's policy and law on matters relating to NIS.

their Computer Security Incident Response Teams (CSIRTs)[35] to protect.[36] Despite ENISA's efforts to prioritize critical infrastructure protection, the ongoing pilot projects analysing critical European infrastructures[37] and the implementation of contractual Public Private Partnership (cPPP) projects funded under the Horizon 2020 Research and Innovation Framework Programme (H2020) in cybersecurity[38], the EU's response is still largely focused on raising awareness and identifying threats. The following recommendations aim to increase the EU's critical infrastructure cyber resilience, as well as Ukraine's through cooperation including lessons learnt from each other:

- Facilitate the sharing of knowledge through a plethora of agencies and groups (e.g. ENISA and the Network and Information Security (NIS) cooperation group[39]) focusing on: increasing protection and cyber resilience of critical infrastructure; research and training specific to countering the threat of advanced persistent malware threats designed for cyber sabotage of critical infrastructure; implementation of critical infrastructure cybersecurity procedures and plans in member states between the public-private sectors.
- Ensure enhanced cooperation between cybersecurity authorities in the EU, national CSIRTs, and the private sector.
- Transform ENISA into a comprehensive European Cybersecurity Coordination Platform which will manage not just CSIRTs but also 1) the EU member states' response to cyber attacks with increased resources for efficiency and speed; 2) the detection, prevention, cooperation, protection, and prosecution of the cyberspace; 3) its own agency focusing on critical infrastructure; and 4) will ultimately transform from a safety to a security-oriented agency.
- Increase focus on finding and patching *zero-day vulnerabilities* through ENISA and CSIRTs, and encouraging research in relevant Centres of Excellency, such as the European Centre of Excellence for Countering Hybrid Threats in Helsinki.
- Designate election infrastructure as a part of the NIS[40] directive's mandatory sectors in which ENISA and CSIRTs must protect, to further protect EU democracies from hybrid threats, including Russian disinformation and cyber attacks.

---

[35] Computer security incident response teams (CSIRTs) respond to a computer security incident when the need arises. Failure of these teams can have far-reaching effects for the economy and national security.

[36] http://ec.europa.eu/epsc/publications/strategic-notes/building-effective-european-cyber-shield_en

[37] In 2013, the European Commission evaluated the progress made by EPCIP and suggested that the programme enter a new, more practical phase. This phase involves launching a pilot project analysing four critical European infrastructures that could be vulnerable to threats. These are: 1) the EU's electricity transmission grid, 2) the EU's gas transmission network, 3) EUROCONTROL and 4) GALILEO – the European programme for global satellite navigation.

[38] https://ecs-org.eu/cppp

[39] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

[40] The Directive on security of network and information systems (NIS Directive) aims to achieve a high common level of network and information systems security across the EU. The Directive applies to two groups. The first, operators of essential services (OES), includes the health, energy, water and transportation sectors. The second, digital service providers (DSPs), covers online search engines, Cloud computing services and online marketplaces.

- Increase EU cyber diplomacy, research, events and participation of think tanks to foster international dialogue and cooperation on critical infrastructure cybersecurity with the purpose of an agreement prohibiting state sponsored sabotage of other states critical infrastructure.
- Increase EU-NATO Enhanced Cooperation on developing responses and cyber defence on critical infrastructure with increased focus on researching and training against advanced persistent threats, malware, and *zero-day vulnerabilities*.
- Ensure Ukraine's collaboration at multiple levels on cybersecurity and cyber defence between national authorities, operators of essential services, agencies attaining to cybersecurity, and the public by cooperating with the nation on establishing a single point of authority and its own dedicated cybersecurity agency.
- Facilitate the cooperation between public and private actors in Ukraine at early stages of the research and innovation process in order to stimulate the cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).
- Invite Ukraine in Permanent Structured Cooperation (PESCO) projects as third state participant[41], especially in two (out of 17) projects linked to Cyber Threats and Incident Response Information Sharing Platform and the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security.[42]
- Increase funding for cybersecurity training and research projects between EU and Eastern Partnership-based think tanks through the new all-encompassing Neighbourhood, Development and International Cooperation Instrument (NDICI) and the Instrument contributing to Stability and Peace (IcSP).

[41] https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_22-06-2018_2.pdf
[42] http://data.consilium.europa.eu/doc/document/ST-6393-2018-INIT/en/pdf