UKRAINIAN STUDIES GO GLOBAL

FRIEDRICH NAUMANN FOUNDATION For Freedom.
Ukraine

EIDOS
CENTRE FOR POLITICAL STUDIES AND ANALYSIS

CASE STUDY:

CYBERSECURITY WARFARE LANDSCAPE: UKRAINIAN EXPERIENCE

Fund of the President of Ukraine

OCTOBER
2022

TABLE OF CONTENTS

ABOUT THE AUTHOR

OLEKSII BARANOVSKYI

An experienced cybersecurity expert with a demonstrated history of working in the academic and financial industries.

He started his career as a security analyst in a software product company, proceeded with the banking and financial industry, and continued in a professional cyber security services company and academic institution. Oleksii is skilled in penetration tests, computer forensics and technical audits.

Oleksii obtained a PhD degree in Information Technology and got the position of associate professor at the National Technical University of Ukraine “Kyiv Polytechnic Institute”. Also, he holds the position of senior lecturer at Blekinge Institute of Technology, Karlskrona, Sweden. He is a certified trainer of recognised international certifications in cyber security (CISSP, CISM, CEH etc.)

Dr Baranovskyi was awarded by the National Security Council of Ukraine, Head of Cyber Police and State Service of Special Communications and Information Protection, for his impact on creating and developing national cybersecurity capabilities.

Oleksii was a subject matter expert in several international projects from OSCE, USAID and CRDF Global during 2015-2022.

ACKNOWLEDGEMENT

I would like to thank my wife Nataliia for her patience and support.

EXECUTİVE SUMMARY

On December 23rd 2015, a regional electricity distribution company (Prykarpattya Oblenergo) in Ukraine reported service outages to customers. The outages were due to a third party's illegal entry into the company's computer and Supervisory Control and Data Acquisition (SCADA) systems. Post investigations revealed that malware named BlackEnergy had infected the SCADA systems after a successful spear phishing attack. Seven 110 kV and twenty-three 35 kV substations were disconnected for three hours. Later it was revealed that three distribution companies were attacked, resulting in several outages that caused approximately 225,000 customers to lose power across various areas in Ukraine [1]. On December 17th 2016, a second power outage occurred in Ukraine and deprived part of its capital, Kyiv, of power for over an hour (Kyiv Oblenergo case). An assessment was made that a more advanced malware, Industroyer, was used in the second cyber attack against the power grid in Ukraine [2].

Critical infrastructure systems vulnerabilities under cyber security threats have also been studied previously in the engineering literature. A typical assumption in this literature is that the cyber attackers have full or partial control of the systems.

According to the popular opinion and attribution made by Eset, Mandian and other cybersecurity companies, cyber incidents of Ukrainian critical infrastructure objects were examples of Advanced Persistent Threat (APT) attacks made by Russian state-sponsored hackers related to their military intelligence and other special service related groups.

THE PREREQUISITE

RUSSIAN MILITARY DOCTRINE OVERVIEW

The following section establishes a framework for understanding how the Russian military decides to conduct cyber operations, the forms they may employ, and the objectives of these operations [4]. Specifically, this section covers the following topics:

- The specific circumstances posing a risk or threat to Russia's security requiring a military response
- The Russian military's stated responses to military risks and threats
- How Russia perceives the strategic importance of its cyber operations

Russia periodically publishes a key strategic planning document titled "The Military Doctrine of the Russian Federation" (hereafter, the "Military Doctrine"). It publicly affirms the military security concepts, concerns, and focuses expected to guide all Russian Armed Forces activities in the coming years. The current version, published in December 2014, notes that its authors considered the contents of several other long-term Russian planning documents for "up to 2020," making it highly likely that a new Military Doctrine will be published in 2020 or soon after that [5]. The 2014 doctrine contains two critical sections assessing the cyber operations of GRU's (Russia's military intelligence agency). These sections respectively identify the specific circumstances to which the Russian Armed Forces must respond and the manners in which modern armed forces act. Then by extension, these sections identify the circumstances where the Russian military is highly likely to conduct cyber operations and a spectrum of characteristics expected to be present in these operations. Understanding this framework can serve as a model for evaluating the Ukrainian case.

The Military Doctrine identifies specific activities or circumstances that generally create conditions for armed conflict ("military risks")e or actions that may directly lead to armed conflict ("military threats"). The Russian military's explicit mission is to respond to these specific risks and threats.

The Military Doctrine enumerates 18 military risks. Most of these risks are consistent with previous Military Doctrines, indicating that core Russian security concerns are stable and remain useful for long-term prediction of future threat activities. The doctrine does not claim that these activities or conditions are presented in a prioritized order, and we assess no prioritized pattern in their order.

The Military Doctrine identifies five military threats. These threats constitute other states' diplomatic or military actions deemed deliberately hostile to Russian interests, that Russia views as direct precursors to an armed conflict. It is critical that the Russian Armed Forces take steps to neutralize or counter these actions or circumstances to prevent such a conflict.

The Russian Military Doctrine describes key ways in which states currently avoid or resolve conflicts using military force. In articulating these elements of modern military conflict, Russia has authorized its military to engage in any of these activities to identify and respond to potential and concrete military risks and threats.

İDENTİFY AND ASSESS POTENTİAL RİSKS AND THREATS

The Military Doctrine requires continuous evaluation of the global political, diplomatic, and military environment to identify emerging military risks or threats. This mission primarily manifests as espionage, including through the use of modern technical means and information technologies.

RESPOND TO CONCRETE RİSKS AND THREATS

Once a risk or threat is identified, the military must respond. Nuclear weapons and conventional military power remain the foundation of Russian national security. That backstop enables the military to support a whole-of-government fusion of hard and soft power to implement national security policy and secure strategic interests. These types of activities provide operational flexibility with a reduced risk for large-scale military confrontation or other unacceptable costs. Military engagement beneath the level of armed conflict is therefore a constant multidimensional struggle between states, with reduced emphasis on direct battlefield engagement and greater emphasis on non kinetic measures to

achieve military security goals. The Military Doctrine and other supporting documents supply an operational concept characterized as hybrid-warfare. These activities typically integrate special operations forces and non kinetic political, economic, or informational measures to shape an adversary’s social and political environment.

THE ANALYSIS FRAMEWORK

Table 1 represents the analytic framework to map detected and investigated cyber operations to Military Doctrine related tasks and responsibilities.

MILITARY ENGAGEMENT	CONCEPT	CYBER OPERATION SIGNIFICANCE
IDENTIFY AND ASSESS POTENTIAL RISKS AND THREATS		
Awareness of potential military risks and threat	The ongoing use of technical means to collect information to identify emerging military risks and threats at the regional and global level.	Cyber operations are used to conduct espionage against political and military targets.
RESPOND TO CONCRETE RISKS AND THREATS		
Widespread use of advanced weapons and technologies	The use of a broad range of weapons that employ advanced technologies such as computerisation, directed energy, robotics, and unmanned flight.	Cyber operations' tools may be advanced military technologies that provide an advantage over other states that lack the technical or financial capacity to develop, acquire, or defend against them.
Warfare impacts the entire depth of an enemy's territory simultaneously	The ability to cause widespread harm to an adversary across its physical or digital battlefield.	Cyber operations should be able to cause widespread harm to a targeted country's computerised devices.
Precise destructive attacks	The ability to selectively destroy targets rather than cause indiscriminate damage.	Cyber operations should be able to cause highly targeted destruction with precise outcomes.

Reduced time to launch military operations with preemptive activities	The time between the appearance of a cause for action and acting must be minimized.	Precise destructive cyber attacks normally have protracted timelines. Preemptive establishment of persistent access to high-value digital and computerized targets (“preparing the battlefield”) is thus necessary.
Global computerized command and control	The use of computer systems to provide unified situational awareness, enabling unified decision among dispersed military forces. Subordinate forces can take the initiative with surprise, decisiveness, and aggressiveness.	Cyber operators are empowered to take rapid, decisive action.
Creation of permanent war zones	Modern warfare creates a state of constant conflict, denying the adversary an opportunity to regroup and reassess, increasing the adversary’s stress and confusion.	Cyber operations can maintain a state of constant conflict with limited risk of escalation.
Irregular and privatized warfare	The involvement of irregular or nonstate combatants in warfare, encompassing militias, terrorists, and private military companies.	Cyber operations can use hired contractors, mercenaries, or other non-state actors to achieve military outcomes. This characteristic also includes regular military operators’ use of fake nonstate personas to accomplish military objectives.
Indirect and asymmetric warfare	The ability to neutralize threats without deploying a parity of forces.	Cyber operations typically need fewer forces and less material than kinetic warfare.
Manipulation of social or political environment	The attempt to influence, control, or instigate political and social movements, with the objective of either weakening the opponent socially or installing friendlier politicians.	Cyber operations can bolster political and social manipulation efforts, such as harming the reputation of political and social targets with provocative data leaks and disinformation.

CYBERATTACK TO UKRAİNİAN POWER GRİD: İNDUSTROYER CASE

OVERVIEW

Table 2 represents the detailed case with the attack on Kyiv Oblenergo and its attributes.

DATE	17–18 DECEMBER 2016 [6]
Suspected actor	The cybersecurity company Dragos Inc. has attributed the cyber-attack to ELECTRUM.[7] According to Dragos, ELECTRUM is a threat activity group of high competence and sophistication in the ICS industry that is directly associated with SANDWORM.[8] In a more recent analysis, ESET has also suggested a strong link between the “Industroyer” malware and the TeleBots group that was behind the “NotPetya” and “BlackEnergy” incidents.[9]
Target	Pivnichna substation of Ukraine’s national power company (Ukrenergo), located near the Ukrainian capital Kiyv.[6]
Targeted System	Industrial control systems (ICS) of the power substation.[10]
Method	Unlike the 2015 attack on Ukraine’s power grid, in which the substation was manually switched off after access to the power grid’s networks had been gained, the Industroyer attack in 2016 was fully automated.[11] The functionality of this malware was described as a “logic bomb” that could detonate at a time of the attackers’ choice.[11] Similarly to Stuxnet, Industroyer could be programmed to run independently from its operators and function in a network that is not connected to the internet.[11] The attackers initially infiltrated the substation by exploiting a vulnerability in Siemens SIPROTEC 4 and SIPROTEC Compact devices, allowing the malware to create a backdoor after gaining access into the industrial system.[12] In addition to making a copy of the main backdoor, the malware also made one of a backup backdoor, imitated as a “Trojanized” version of Windows Notepad, that would be activated if the first version was uncovered, thus enabling the malware to remain persistent.[12]

	Then the malware aimed at the industrial hardware, namely the circuit breakers and protection relays of the substation.[12] The execution of the attack was not immediate; instead, the blackout took place later at a time and date that was pre-set and hidden within the malware's code.[12] At that pre-defined moment, the malware's payload was activated to take control over the circuit breakers and protection relays commanding them to open the circuit breaker switches.[12] In order to boost the attack and ultimately crash the system, the malware also initiated, first, a denial-of-service tool that targeted and deactivated protection relays and, second, a data wiper tool that scanned workstation hard drives for specific file extensions related to the targeted software and then removed them to prevent recovery.[12]
Result	Blackout that left a part of the Ukrainian capital, Kyiv, and its surrounding area without electricity for more than one hour.[6] The power loss at the time of the cut was estimated as one-fifth of Kyiv's consumption.[13]
Aftermath	Although it did not attract as much attention as the 2015 attack, the malware used in the 2016 attack has been described as far more dangerous for being so advanced, customizable and highly adaptable to any environment.[14] ESET has described Industroyer as the biggest threat to ICSs after Stuxnet.[14] Because Ukraine uses similar industrial technologies for its power grid to those commonly used around the world, this incident has raised serious concerns around the world, and some experts have described it as a wake-up call for reviewing and updating the cybersecurity of industrial and critical infrastructure worldwide.[15] In 2017, Ukrenergo introduced a reform aimed at reshaping its IT infrastructure and security; and a cyber incidents response centre was established to prevent threats and minimize the consequences of future cyber attacks.[16] Dragos issued an industry report specifying indicators of compromise for the malware and included guidance for security teams on how to detect malicious behaviours and set patterns associated with the ICS communications, in addition to intelligence reports containing updates on the threat actor and capability.[7]

	On May 11th 2017, President Trump signed an executive order to strengthen the cyber security defenses of federal networks and critical infrastructure. In the executive order, there is a section specifically addressing the threats from "electricity disruption and prolonged power outages resulting from cyber security incidents". Incident responses have been carefully studied and a substantial set of cyber requirements has been placed on all U.S. grid operators of bulk power grid for several years [17]. On October 19th 2017, the Federal Energy Regulatory Commission (FERC) proposed new mandatory cybersecurity controls to address the risk posed by, for example, smaller grid control centers that are typically less critical than major control centers, but which are nonetheless vulnerable to intrusion software [18].
Purpose	The real purpose of the attack remains unclear. There are concerning scenarios regarding the potential capabilities of the Industroyer, which are not limited to electricity blackouts that could last for up to several days but could even extend to causing physical damage.[12] According to Dragos, such potential capabilities of the malware and its functionalities which were not fully exploited could be a good reason to believe that the 2016 power grid attack may have been just a proof of concept attack.[7]

THE CHALLENGE

1. Investigate the case.
2. Map the known attributes and consequences of Industroyer attack to Military Engagement Activities according to the Military Doctrine. Explain the possible benefits of each outcome.
3. Propose a solid policy-based solution to prevent/respond to similar attacks to critical infrastructure objects in your country. Which positive/negative consequences might be obtained after implementing your solution?

OUTCOMES

The military's use of hybrid warfare reflects a popular Russian strategic paradigm known as "information confrontation." Within this paradigm, international relations is a constant struggle for dominance of what is known, perceived, believed, or emotionally felt. More granularly, states conflict over information itself (known as informational-psychological effects) or the means by which it is held, transmitted, or processed (known as informational-technical effects).

This context of this information confrontation concept illuminates our understanding of Russia and its cyber operations. Beyond traditional espionage, cyber operations should be considered as part of Russia's vision of a long-term confrontation over beliefs, understanding, and emotions that impact Russia's ability to advance its policy vision and secure its strategic interests. Short-term effects, such as how long an attack disrupts power distribution, are of secondary importance to their ability to signal, penalize, and emotionally influence target populations.

Public sources generally track most Russian's cyber activities as two mission-focused activity clusters that mirror the dual aspects of informational confrontation, with the division covering informational-psychological effects and the division covering informational-technical effects. Though their infrastructure and toolsets are usually separate and distinct, their occasional overlaps serve as one publicly observable indicator of their bureaucratic interconnection.

CONCLUSIONS

Russia is a prolific, capable, and determined threat actor. Its operations blend technical prowess with strategic vision, taking deliberate steps to target data and systems in ways that advance long-term national military security objectives. Fortunately for defenders of democratic world (Ukraine, EU, USA) the Rissias's process for selecting targets and methods is consistent and therefore predictable. By understanding threat actor motivations, defenders can anticipate when, where, and how attacks will unfold—enabling defenders to take deliberate steps to improve their security posture.

The Russian military seeks to maintain high-combat readiness and improve nonnuclear deterrence by creating "threats of inflicting unacceptable damage." Russia will therefore seek to establish cyber-based deterrence, signaling that it possesses the access and ability to disrupt critical sectors, as happened with conventional weapons during the war in 2022. To this end, we expect attempted intrusions will likely occur in Western critical sectors such as energy, utilities, and transportation, and attacks are more likely in non-NATO countries, where they are less likely to draw an allied military response.

The Russian military aspires to better coordinate with economic, political, and other nonmilitary elements of state power. In contrast to trends in the previous decade, this coordination could plausibly lead to military cyber operations occurring in collaboration with Russian civilian security services. Such coordination could undermine attribution efforts going forward.

APPENDİX 1. GENERAL PROTECTİON APPROACHES FROM CYBER THREATS

Understanding adversaries' motives is critical to proactive, efficient threat mitigation and risk management. A narrow, inflexible focus on compliance and recovery coupled with a lack of awareness of relevant threats can lead to persistently mounting costs to defend against a vague constant threat of attack. A deep understanding of threat actors can lift this haze, allowing pointed, deliberate, and informed decisions about managing risk from the c-suite to hands-on-keyboards network defenders. This agile, threat-centric security paradigm ultimately aims to drive efficiencies by continuously anticipating, mitigating, detecting, responding, and recovering from rapidly evolving threats.

CYBER RISK MANAGEMENT

Adopt a threat-centric risk management approach to better understand threats, attack vectors, and critical assets, and to prioritize efforts and optimize your investment. Focus on strong asset management and surface area reduction and adopt best practices and settings for configuration management.

Threat Landscape Assessment: Evaluate relevant adversaries' motives,methods, and intentions related to your organization, its sectors, its geographic areas of operation, and its critical assets to increase your awareness of your attack surface and to inform organizational resource optimization and risk management strategies. The results of a threat landscape assessment, paired with the high-value asset identification described in the next recommendation, are central to selecting impactful security controls.

High-Value Asset Identification: Identify the information or resources whose confidentiality, integrity, or availability are most critical to your organization's. Next, determine if this critical information or resources are similar to assets known threat groups have previously compromised. You will then need to evaluate whether your top adversaries would consider the abuse of these assets to be useful or unique for advancing their goals. Understanding the vulnerabilities and security control gaps previously leveraged to exploit these assets is a critical step.

This allows you to prioritize vulnerability management and security gap mitigations on high-value assets based on impact on mission and business. Applying appropriate mitigation plans will reduce your overall attack surface and ensure your most valuable assets are optimally protected.

Threat, Control, and Risk Modeling and Simulation: Assessthe alignment of your security controls and risk management strategy to your top adversaries' capabilities and intentions.This can be accomplished by developing hypothetical scenarios that explore possible future adversary tradecraft to develop a proactive security stance, ahead of adversary capability developments. Then use analytics, modeling, and simulation techniques to run what-if scenarios and gather insights that optimize risk management in the context of your specific threat landscape.

CYBER DEFENSE

Harness insights gained through continuous threat intelligence analysis to predict and defend against evolving attack patterns. Keep your networks secure with a strong vulnerability management program that actively searches for unpatched systems and unauthorized activity. Build, test, andfund incident response plans that can be implemented to thwart data loss or downtime at a moment's notice. Leverage Any security incidents to strengthen the program by systematically capturing and integrating lessons learned.

Continuous Risk Management: Adjust your security posture based on anticipated future threat activity. Your adversaries' perspectives on your organization may change due to your business decisions, such as starting new lines of business or entering new markets, or due to broader geopolitical circumstances.

Logging: Maximize network visibility and centralize logs to the greatest extent reasonable. Historic NetFlow traffic andEndpoint Detection and Response (EDR) data can be extremely useful for understanding what happened in incidents.For example, log analysis showed115 that the disruptive attack on a Ukrainian power distribution station in 2016 plausibly had a far smaller impact than attackers may have intended. Logging can also provide data to test analytics, train advanced analytics-based detection models,and update organizational threat modeling.

Threat Intelligence: Identify, contextualize, and track campaigns and threats, and integrate these insights into security planning and operations. Actively seek out new sources of threat intelligence that improve situational awareness of political and economic events and interests that trigger adversary response or retaliation. Tracking and analysis of the string of faux-ransomware attacks in Ukraine prior to the NotPetya event might have informed useful defense strategies, such as global companies reducing connectivity with their Ukraine units around national holidays and anniversaries related to Ukrainian Identity and independence.

Advanced Detection: Inform analytic development from threat modeling, prioritizing the most likely attack vectors.Analytics-based detection is key to hunting advanced adversaries that do not use commoditized attack tactics and cannot be detected using commoditized cyber defense. Investing in an analytics platform is the best way to combat these highly capable threats.

Threat Hunting: Optimize hunt efforts by focusing on the resources likely adversaries tend to target or abuse. Organize Around purple team capabilities to develop a deep understanding of offensive and defensive capabilities to better inform threat hunting in your environment. Targeted disruption attacks frequently involve long dwell times, increasing defenders' opportunities to expel or isolate hackers before they act. For example, the faketivist “Mr. Robot”-themed attacks on Ukrainian financial organizations in December 2016 relied on at least nine months of effort, like escalating privileges and lateral movement, before the hackers disrupted their victims.

Cyber Wargames and Exercises: Evaluate your ability to respond to plausible threat scenarios involving your most likely, dangerous adversaries. A holistic understanding of adversaries—encompassing technical and nontechnical attributes—is necessary to craft realistic, anticipatory scenarios. Most wargames and exercises should simulate failure to prevent adversaries from acting on their objectives,thereby testing crisis management, business continuity, and service restoration capabilities.

Information Sharing: Share information with peers, governments, and other companies to increase community awareness of current adversary activity and improve visibility of your threat landscape. Greater threat visibility increases the likelihood that early indications and warnings of future threat activity will become apparent.

REFERENCES

1. R. M. Lee and M.J. Assante, "Analysis of the Cyber Attack on the Ukraine Power Grid" in E-ISAC and SANS., Washington, DC, TLP:White, Mar. 2016.
2. A. Cherepanov, "Win32/Industroyer A New Threat for Industry Control Systems", ESET, Jun. 2017, [online] Available: https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
3. C. W. Ten, C. C. Liu and G. Maninaran, "Vulnerability assessment of cybersecurity for SCADA systems", IEEE Trans. Power Syst., vol. 23, no. 4, pp. 1836-1846, Nov. 2008.
4. Bearing witness: Uncovering the logic behind Russian military cyber operations. 2020 Booz Allen Hamilton Inc., C.09.036.19.
5. “The Military Doctrine of the Russian Federation,” Approved by the President of the Russian Federation on December 25, 2014, The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, June 29, 2015, https://rusemb.org.uk/press/2029.
6. НЕК "Укренерго" - NPC Ukrenergo, official statement (18 December 2016). See also BBC News, ”Ukraine power cut 'was cyber-attack” (11 January 2017); The National Radio Company of Ukraine, “Ukraine power cut 'was cyber-attack”(11 January 2017).
7. Robert M. Lee, “CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids” (Blog 12 June 2017).
8. Dragos Inc., ‘Electrum’ (2017).
9. Anton Cherepanov and Robert Lipovsky, “New TeleBots backdoor: First evidence linking Industroyer to NotPetya”(11 October 2018).
10. Dragos Inc., “CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations” (13 June 2017).
11. Andy Greenberg, “Crash Override': The Malware That Took Down a Power Grid” (12 June 2017).
12. Charlie Osborne, ”Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout” (30 April 2018).
13. BBC News, ”Ukraine power cut 'was cyber-attack” (11 January 2017); The National Radio Company of Ukraine, ”Ukraine power cut 'was cyber-attack” (11 January 2017).
14. Anton Cherepanov and Robert Lipovsky, “Industroyer: Biggest threat to industrial control systems since Stuxnet” (12 Jun 2017).

15. Anton Cherepanov and Robert Lipovsky, “Industroyer: Biggest threat to industrial control systems since Stuxnet” (12 Jun 2017). See also: Kim Zetter, “The Ukrainian Power Grid Was Hacked Again” (10 January 2017); John E Dunn, “Ukraine power outages ‘the work of cyberattackers’, warn experts” (16 January 2017).
16. Ukrenergo, “UKRENERGO-2017: results of the first reforms” (2018).
17. "Cyber Risk Preparedness Assessment Table-Top Exercise 2012 Report", NERC, May. 2013.
18. John Siciliano, "FERC Sets Rules to Protect Grid from Malware Spread Through Laptops", Washington Examiner, [online] Available: http://www.washingtonexaminer.com/ferc-sets-rules-to-protect-grid-from-malware-spread-through-laptops/article/2638081.

Fund of the President of Ukraine

for Education, Science, and Sports

Projest initiated by the Fund of the President of Ukraine for Education, Science, and Sports, implemented by Eidos and supported by the Friedrich Naumann Foundation for Freedom in Ukraine

UKRAINIAN STUDIES GO GLOBAL

FRIEDRICH NAUMANN FOUNDATION For Freedom. Ukraine

EIDOS CENTRE FOR POLITICAL STUDIES AND ANALYSIS

4 Luteranska Street, Kyiv, Ukraine
presidentfund.gov.ua