CYBERAGGRESSION AS A COMPONENT OF HYBRID WAR AGAINST UKRAINE

Kseniya YURTAYEVA,

PhD in Law, Associate Professor, LL.M,
Associate Professor of the Department of
Criminal Law and Criminology
of Faculty №1 of Kharkiv National
University of Internal Affairs;
visiting scholar at Weiser Diplomacy Center,
Gerald R. Ford School of Public Policy
at the University of Michigan
https://orcid.org/0000-0002-6096-2020
DOI: 10.5281/zenodo.7437734

Today the concept of hybrid war attracts increasing attention. Microsoft referring to massive destructive cyberattack against Ukrainian government, technology, and financial sector launched on the eve of the armed intrusion to Ukraine stated that the cybersecurity world entered a new age, the age of the hybrid war on February 23, 2022 [1]. Meanwhile this thesis seems to be debatable, since Ukraine has been experiencing similar cyberaggressive influence over the last several years.

The notion of hybrid war is not specifically defined in the legal provision, although articulated in governmental documents, for instance in the Strategy of Cybersecurity of Ukraine "Safe Cyberspace as a Guarantee of Successful Development of Ukraine" released in August 2021. The strategy identified hybrid aggression of the Russian Federation on Ukraine in cyberspace as the main threat to the national cybersecurity. Efficient cyberdefense capable for conducting armed counteraction in cyberspace was recognized among main strategic objectives of Ukraine [2].

Analyzing manifestations of the hybrid war we can clearly track escalation of cyberaggressive actions of the Russian Federation against Ukraine starting from 2013-2014. This aggravation is associated with vigorous flows of disinformation in Ukrainian social media that was later followed by the most destructive cyberattacks on governmental and public institutions.

Notorious cyberattacks against Ukrainian energy system took place in 2015 and 2016. It was one of the first cyberattacks

specifically targeting objects of critical infrastructure. As a result of the use of malware known as Blackenergy, 30 electricity substations in the Western Ukraine were disconnected and as many as 230,000 customers which amounts the population about 1.4 million lost power supply for several hours [3].

The second cyberattack against Ukrainian energy system took place one year later in December 2016. This time hackers used a specifically designed malware for manipulating the physical components of industrial control networks called Industroyer. As a result of the cyberattack on Ukraine's power grid one fifth of Kyiv was off power for one hour and cybersecurity specialist rightfully considered it to have been a large-scale test [4].

The third large-scale cyberattack this time on the Ukrainian governmental services was conducted in 2017 just before the Day of the Constitution of Ukraine with the use of the virus NotPetya which disrupted the work of thousands of state enterprises. Cybercriminals used the method of targeted supply chain attack conducted through the accounting firm MeDoc whose services were widely used by Ukrainian businesses for tax reporting injecting malicious code into their software. NotPetya infiltrated computer systems via software update from MeDoc and enabled it to infect networks of thousands of Ukrainian governmental institutions [5]. Unlike Wannacry, a ransomware cryptoworm used in cyberattack in May of 2017, Notpetya was a malware wiper which encrypted the systems, making it impossible to decrypt and recover the data. Notpetya was a cyberattack specifically targeted at Ukraine but it also spread far beyond the borders of Ukraine, causing $10 billion of damage globally.

Presented cyberattacks on the Ukrainian governmental institutions and power grid are still considered one of the worst cyberintrusions ever. Ukrainian governmental officials and international experts squarely placed the blame outages and disruption of the work of governmental institutions on cybercriminal groups associated with Russian security services, namely the Russian Main Intelligence Directorate.

Despite of the different modes of attacks and miscellaneous cybermalware sited cyberattacks had common features:

- they were all specifically aimed at the targets inside Ukraine;
- these attacks were large in scale and had devastating impact on the functioning on the Ukrainian public sector;

- cyberattacks lacked mercenary motivation. Their technical characteristic was designed for destruction or obtaining the right to manipulate computer systems.

- cyberattacks were attributed to cybercriminal groups associated with Russian security services.

Analyzing current cybersecurity situation, the Deputy Director of the State Service of Special Communications and Information Protection of Ukraine Victor Zhora admitted that massive cyberattacks took place recently before the start of Russian large-scale attack on Ukrainian territory. At night on the 14th of January a number of Ukrainian governmental sites suffered a massive cyberattack, which were defaced and partially destroyed by the use of special wiper. The next one took place just before the actual intrusion on the 22 of February of 2022 [6].

During the first days of the armed intrusion hackers associated with the Russian Federation also made an attempt to destroy Ukrainian cybersecurity system. Cyberattacks were specifically aimed at destructing communication among the Ukrainian military units. For example, during the first hours of war on the 24th of February Ukrainian military and law enforcement were deprived of the support of satellite connection from American company Viasat [6]. The nature of this attack is not publicized. Although the cyberattacks succeed, they haven't reached their ultimate goal, because Ukrainian state communication services managed to recover with support of satellite Internet connection provided by Elon Musk's Starlink.

In the late March Ukrainian law enforcement managed to stop another attack on Ukrainian power grid. Hackers tried to use modified version on logical bomb ransomware Industroyer2 as was previously used in the attack in 2016, but it was timely detected and stopped [4].

All these explicitly demonstrates that the roots of the Russian undeclared cyberwar on Ukraine can be traced several years before the actual military intrusion to Ukrainian territory and it an additional argument for attributing the start of the Russian cyberaggression on Ukraine to 2014.

Today Ukraine faces unprecedented cybersecurity challenges. Despite of the numerous targeted cyberattacks Ukrainian cyberdefense demonstrates strong resilience to malicious cyberinteractions. To a considerable extent it can be attributed to

timely recognition of hybrid war threats, appropriate strategic planning and creation of specialized law enforcement and military units countering cyberaggressive actions conducted by state and non-state actors. Armed aggression of the Russian Federation triggered novel threats to Ukrainian cyberdefense posed by combination of aggressive activities in cybersphere with kinetic warfare, which greatly increases social dangerousness of the mentioned actions. In this regard lowering the threshold for criminal liability for unauthorized access to informational telecommunication systems and providing aggravated liability for committing such actions during martial law (amendments to the Art. 361 of the Criminal Code of Ukraine) looks clearly logical. At the same time further research is required to explore the possibilities for applications of international law, including provisions of International Humanitarian Law, to criminal activities in cyberspace during martial law. This proposal goes in line with the p. 32 of the Plan for realization of the current Cybersecurity strategy of Ukraine [7].

References:

1. Microsoft Digital Defense Report 2022. URL: https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.
2. Про Стратегію кібербезпеки України: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. Miller C. Throwback Attack: BlackEnergy attacks the Ukrainian power grid. URL: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/ (date of access: 05.11.2022).
4. Industroyer 2: the Russian Cyberattack on Ukraine Infrastructure. URL: https://www.headmind.com/fr/industroyer-2/ (date of access: 05.11.2022).
5. Greenberg A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (date of access: 05.11.2022).
6. Бурдіна Е. «Агресор повинен потрапити до кам'яного віку». Заступник голови Держспецзв'язку Віктор Жора — про кібертероризм росії та опір України хакерським атакам. URL: https://dou.ua/lenta/interviews/russian-cyberwar-against-ukraine/ (дата звернення 05.11.2022).
7. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30.12.2021 р. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text