УДК 004.056:355

A.Hulevata
L.Magas

PROTECTION OF CYBER SPACE OF UKRAINE DURING WAR

Vinnytsia National Technical University

Abstract
The work considers the main aspects of the protection of the cyberspace of Ukraine in the conditions of war. Starting with a description of the threats facing the country, as well as the detection and classification of cyberattack.
Keywords: *cyberspace, war, Ukraine, attacks, hackers, IT army, protection.*

Анотація
У роботі розглядаються основні аспекти захисту кіберпростору України в умовах війни. Починаючи з опису загроз, з якими стикається країна, а також виявлення та класифікації кібератак.
Ключові слова: *кіберпростір, війна, Україна, атаки, хакери, IT-армія, захист.*

Introduction

Russia's open military attack on Ukraine began on February 24, 22 and continues to this day. During the war, it is necessary not only to protect the country's borders, but also the information space, as the enemy is trying to harm from all sides. Starting on February 24, isolated Russian cyberattacks have complicated the distribution of medicines, food and emergency aid. These attacks have had a variety of effects, from blocking access to essential services to stealing data and spreading disinformation. Other malicious cyber activity includes phishing emails, data-destroying malware, surveillance software, and information theft [1].

Basics

From the beginning of the war, from February 24, 2022, 4,500 cyberattacks were carried out on Ukraine, compared to 2021, there were about 2,000 attacks, and in 2020 there were only 800.[2]

Hackers typically distribute malware that steals data or destroys information systems, the most common tactic used by Russian military hackers in Ukraine. Such attacks account for more than a quarter of their total number and can be part of more complex and powerful operations.

Russia's main attacks on Ukrainian cyberspace are: espionage, i.e. obtaining intelligence on logistics, weapons, plans and operations of the Security and Defense Forces; spreading fake information and maximizing destructive impact, i.e. disabling critical infrastructure, depriving citizens of access to banking services, etc [3].

Russian hackers target the following sectors the most: the public sector, which traditionally ranks first in terms of the number of cyberattacks, accounting for about a quarter of all cases; the energy sector, commercial, telecom, and logistics sectors; and cyberattacks on the logistics sector are a natural next step to disrupt the supply chain and affect the logistics capabilities of critical equipment and supplies for the civilian and military sectors [3].

In the early days of the war, the IT army consisted of 175,000 volunteers from all over the world: from white hackers and hacktivists to representatives of such technology companies as Elon Musk's SpaceX. Even the world-famous Anonymous Collective sided with Ukraine, promising to act against Russia in cyberspace.

At the same time, Ukrainians in underground forums called for help in protecting Ukrainian cyberspace.

Foreign experts say the process of creating a state-funded cyber army is unprecedented. Never before has any government managed to recruit independent candidates for a global volunteer organization.

During the war, Anonymous launched DDoS attacks on corporate, news and government websites, compromised more than 90 databases of telecommunications, retail and government organizations in Russia [4].

Ukraine's defense in late February 2022 was bolstered by a £6 million package of IT support and assistance in identifying Russian cyber threats provided by the United Kingdom. This support was announced only on November 1, almost 250 days into the war. In addition, the protection included transferring data to the cloud,

partnering with Western companies, and using Starlink mobile terminals. This proved to be an extremely important and effective method of countering cyberattacks [5].

In February, Ukraine backed up as much data as possible. After the intrusion began, Liam Maxwell, director of transformation at Amazon Web Services, met with a Ukrainian official in London "and literally wrote on a piece of paper" which of Ukraine's digital assets she needed help saving. The priorities included property, citizen and criminal registries, Maxwell says. "It's like Maslow's hierarchy of needs"[5].

AWS cybersecurity experts and IT professionals also trained Ukrainians on cybersecurity and how to move data from local IT systems to the cloud, where it can be better protected. In particular, they shared intelligence on cyber threats [5].

Currently, Ukraine has limited capabilities to counter cyberattacks, but it is trying to strengthen its cyber defense with external assistance. The government has attracted volunteers from around the world to form an IT army. In response to the Russian attacks, an IT team created by the Minister of Digital Transformation has launched several DDoS and wiper attacks. The former disrupt servers by artificially creating a large amount of traffic, while the latter result in the deletion of data. The targets of the attacks include the Russian government, media systems, financial institutions, defense facilities, power grids, and railroads. As part of the cyberattacks, independent hackers from around the world have stolen and released Russian government and financial data, including emails, information on banking, energy production, and propaganda campaigns, as well as data on military personnel and Federal Security Service (FSB) agents. This sensitive information is reportedly then passed on to international activists to punish Russia for its crimes in Ukraine. The secondary effect of the latest hacking efforts is their success in creating chaos in Russian cyber systems and destroying the belief that Russia's cyber defenses are impregnable [6].

Conclusion

Thus, the protection of Ukraine's cyberspace in time of war is an extremely important task that requires constant attention and effort. Cyberattacks can cause serious damage not only to infrastructure and communication systems, but also to national security, the economy, and public confidence in the state.

The importance of protecting cyberspace in times of war is heightened by the fact that cyberattacks can be used as a weapon to launch large-scale attacks on strategic facilities and critical infrastructure. The protection of cyberspace becomes essential to ensure the functioning of government agencies, defense systems, energy networks, financial institutions and other important sectors of the economy.

Successful protection of cyberspace requires a comprehensive approach that includes the development and implementation of effective cybersecurity strategies, enhancing the skills of specialists, developing cooperation with international partners, and developing modern protection technologies.

In times of war, it is important to ensure reliable cyber defense, identify, analyze and respond to potential threats, protect critical systems and infrastructure, and strengthen the culture of cybersecurity among citizens.

REFERENCES

1.Attacks and their consequences URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf

2. Number of cyberattacks in Ukraine in recent years URL: https://lb.ua/society/2023/02/28/547362_rosiya_shchodenno_zdiysnyuie_blizko_10.html

3. War in Ukraine: Pulse of Cyber Defense URL: https://techukraine.org/2023/01/09/war-in-ukraine-pulse-of-cyber-defense-september-december-2022/

4. How Russia and Ukraine are fighting on the cyber front URL: https://www.epravda.com.ua/columns/2022/09/28/691925/

5. What were the tactics of cyber defense in Ukraine at the beginning of the invasion URL: https://ain.ua/2022/11/12/yakoyu-bula-taktyka-kiberzahystu-v-ukrayina-na-pochatku-vtorgnennya/

6. Countering cyber attacks URL: https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline

https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf

Liudmyla Mykolaivna Magas – Lecturer of English, FL department of Vinnytsia National Technical University, Vinnytsia, , e-mail: magas@vntu.edu.ua

Hulevata Anzhelika Andriivna - student of group УБ-21б, Faculty of Management and Information Security , Vinnytsia National Technical University, Vinnytsia, e-mail: gulevataanzhelika@gmail.com

Магас Людмила Миколаївна – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: magas@vntu.edu.ua

Гулевата Анжеліка Андріївна **–** студент групи УБ-21б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: gulevataanzhelika@gmail.com