УДК 37:004:316.722.5

A.O. Lavreniuk

CYBER WARFARE IN THE MODERN WORLD

Vinnytsia National Technical University

Анотація

У статті йдеться про кібервійни сьогодення. Кібервійна сьогодні є новим і дуже важливим поняттям сучасного світу. Після суші, моря, повітря і космосу війна увійшла в п'ятий вимір: кіберпростір. Комп'ютерні збої або атаки паралізують військові системи електронної пошти, вибухають нафтопереробні заводи і трубопроводи, руйнуються системи управління повітряним рухом, потяги сходять з рейок, фінансові дані перенаправляються, пошкоджуються електромережі, супутники виходять з-під контролю. Наслідки кібервійни подібні до наслідків ядерної атаки. Це вимагає заходів захисту і безпеки інформації, яка циркулює в цих комунікаційних системах і мережах, і є одним з викликів сьогодення. Загрози комунікаційним та інформаційним системам зробили кіберзахист у сфері національної безпеки елементом, який необхідно брати до уваги.

Ключові слова: кібервійна, електронний, IT, мережа, комунікація, загроза, цифровий, кібератака, вплив.

Abstract

The article deals with today's cyber warfare. Nowadays cyber warfare is a new and very important concept of the modern world. After land, sea, air and space, the war has entered the fifth dimension: cyberspace. Some computer glitches or attacks paralyze military e-mail systems, refineries and pipelines explode, air traffic control systems collapse, trains derail, financial data gets misdirected, power grids damaged, satellites go out of control. The effects of a cyber war are similar to those of a nuclear attack. This requires protective measures and security for the information that circulates in these communication systems and networks and constitutes one of the challenges of today's time. Threats to communication and information systems have made cyber defense in the field of homeland security an element that must be taken into consideration.

Keywords: cyber warfare, electronic, IT, network, communication, threat, digital, cyber-attack, impact.

Introduction

The current risk of cyber-attacks in Western society is, arguably, as high as it has ever been. Following the initiation of Russia's attack on Ukraine in early 2022, the National Cyber Security Centre (NCSC) urged UK organisations to bolster their online defences. Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) and FBI warned of heightened threats to US organisations [1].

There is no doubt that during times of global change and unrest, cyber security becomes a battlefield of its own and both state and non-state actors have increasingly turned to cyber-attacks as a way to gain an advantage in warfare. Furthermore, with enhanced technology and an increasing number of devices connected to the internet, the scope and complexity for cyber-attacks has grown dramatically.

Cyber warfare can take many forms, including hacking into enemy state computer systems, spreading malware, and launching denial-of-service attacks. Entire towns and cities could be cut off from information, services and infrastructure that has become essential to the way we live such as electricity, online banking systems and internet, if a cyber threat is able to infiltrate the right systems [2].

Rising threats in the digital age

Cyber warfare is one of the newest elements in contemporary warfare, however, this new advancement is continuously evolving and it can be challenging, at times, to stay abreast of all the new developments. In an age when individuals voluntarily transmit and receive copious amounts of personal data, exploiting electronic devices to alter or obtain information has become a crucial new tactic of conflict known as the 'fifth dimension battlefield, after air, sea, land and outer space' and has, arguably, become vital in achieving states’ success today [3]. This information revolution is based on rapid technological advances in computer software, as such, computing ability has doubled every 18 months for the last 30 years, at a fraction of the cost it did in the 1970’s and has meant that neither mass nor mobility decide outcomes.

Main challenge with cyber-attacks is the threat actor's ability to remain anonymous, making it difficult to attribute the attack to a specific individual or group. The use of private companies and individuals as proxies in cyber-attacks only serve to further complicate matters and in the initial stages of an attack, it may be difficult

to fully appreciate the extent of the risks posed and true motivations behind it.

War and military conflicts can create a business environment that is conducive to cyber-attacks, as adversaries may seek to target businesses or sectors that are seen as important to a country's economy or infrastructure [4]. They may also go for symbolic targets such as media outlets or high-profile brands associated with a nation state. Additionally, the use of cyber-attacks in war can also create a general sense of chaos and uncertainty, which can be used to exploit vulnerabilities in businesses' cyber defences.

There is no clear set date of when cyber warfare began but a key milestone was in Kosovo in 1999. Whilst Vietnam was the world's first TV war, Kosovo became its first cyber war. NATO Kosovo operation was a major challenge in the history of the Atlantic alliance. For the first time, a defensive alliance launched a military campaign to avoid a humanitarian tragedy outside its own borders. For the first time, an alliance of sovereign nations fought not to conquer or preserve territory but to protect the values on which the alliance was founded. And despite many challenges, including the use of cyber warfare, NATO prevailed. Numerous pro-Serbian hackers attacked NATO's internet infrastructure with the goal to disrupt military operations. Whilst some states declared the cyber-attacks had no impact on their overall war effort, the U.K. admitted to having lost at least some database information, these attacks where the first sign of things to come and the potential power cyberware would have.

In 2007, eight years after Kosovo, McAfee LLC stipulated that over 120 countries had developed cyber means to use the internet to target other states through financial markets, computer systems, and national infrastructure. This new warfare realm, referred to as "cyberspace", has become the key to the future for contemporary conflict.

Examples of cyberattacks have demonstrated the extent to which sophisticated techniques can be used to target and disrupt critical infrastructure [5]. For instance, the Stuxnet computer worm, renowned for its complexity, was specifically aimed at Iran's nuclear facilities in 2010, with a particular focus on its uranium enrichment programme. By exploiting vulnerabilities within control systems, Stuxnet successfully inflicted serious damage upon centrifuges and effectively crippled Iran's nuclear programme.

In another notable incident in 2017, numerous companies were subjected to an extensive global hack that severely impacted vital infrastructure providers. The NotPetya ransomware attack caused immense financial losses by encrypting the systems of affected businesses [6].

Preceding this event was yet another ransomware outbreak known as WannaCry. This widespread infection reached millions of computers worldwide and had a significant impact on essential infrastructure such as hospitals, transportation networks, and telecommunications businesses. The attack exploited weaknesses present within the Windows operating system, leading to substantial disruptions across various sectors.

These attacks can have disastrous results, causing widespread power outages, transportation disruptions, and economic collapse. As cyber criminality develops, governments and organisations face an increasing urgency to strengthen their cybersecurity safeguards to defend against future acts of cyber warfare.

Russia, Ukraine, and the global implications

Karim Khan, the lead prosecutor of the International Criminal Court, unveiled the ICC's new commitment: to investigate cybercrimes that may be in violation of the Rome Statute [3]. This treaty outlines the court's authority to prosecute unlawful acts, including war crimes, crimes against humanity, and genocide. In a statement to the quarterly publication Foreign PolicyAnalytics, Khan reiterated the importance of adapting to the evolving nature of conflict, emphasising the potential for digital front lines to yield damage and suffering comparable to traditional battlefields.

Karim Khan, the lead prosecutor of the International Criminal Court, unveiled the ICC's new commitment: to investigate cybercrimes that may be in violation of the Rome Statute. This treaty outlines the court's authority to prosecute unlawful acts, including war crimes, crimes against humanity, and genocide. In a statement to the quarterly publication Foreign PolicyAnalytics, Khan reiterated the importance of adapting to the evolving nature of conflict, emphasising the potential for digital front lines to yield damage and suffering comparable to traditional battlefields.

The ICC's official stance, as provided by a representative of the Office of the Prosecutor (OTP), is that "conduct in cyberspace may potentially amount to war crimes, crimes against humanity, genocide, and/or the crime of aggression, and that such conduct may potentially be prosecuted before the Court where the case is sufficiently grave.".

While the ICC prosecutor did not expressly reference Russia's and Ukraine's ongoing cyber battle, it appears to have piqued his interest. Ukraine has been the subject of an increasing number of cyberattacks by

Russia, as hostilities have escalated significantly. These attacks go beyond infrastructure targets and include cyber operations aimed at disseminating disinformation and propaganda that can affect public opinion both at home and abroad. These attacks have the ability to destabilise governments and cause public unrest.

Victor Zhora, the deputy chairman and chief digital transformation officer at Ukraine's State Service of Special Communication and Information Protection (SSSCIP), anticipates that Russia will continue its online attacks, potentially constituting "cyber war crimes," even after the physical conflict subsides. This underscores the urgent need for international pressure to address these ongoing cyber threats.

Since the beginning of this war, Russian hackers have targeted Ukrainian military, financial, and governmental targets. These assaults have had far-reaching implications, such as the 2015 attack on the power infrastructure in western Ukraine, which knocked off electricity for an estimated 230,000 Ukrainians [7]. Furthermore, the second-biggest bank in Russia, state-owned VTB, suffered the largest cyberattack in its history in December 2022, though the perpetrator remains unknown. Notably, the number of malware coming from Russian IP addresses has increased significantly since February 2022.

Concerns about the possibility of another significant attack are increased by the uptick in malware activity and cyberattacks in the area. The international community is closely monitoring the situation, urging nations to reinforce their cyber defences. Effective resistance to this growing digital threat necessitates international cooperation and information sharing among governments.

Cyber warfare as a new battleground

The United Nations has highlighted cyber-attacks as a modern-day hazard, with data showing a doubling of cyber-attacks in the first half of 2019 compared to the second half of 2018. These attacks mostly target factories, oil and gas companies, and educational institutions, putting vital infrastructure owners at risk. More than a hundred cyber incidents with the potential to disrupt international peace and security have been identified in the last year. These strikes have the potential to cause significant damage and casualties [8].

States are employing non-state actors in the digital realm, which appears to be classified as a novel domain of military strategy due to the risks it poses to global peace and security if mishandled.

The rise of cyberspace as a new battleground has prompted significant ethical and legal problems about how warfare should be conducted [5]. Notably, the International Committee of the Red Cross (ICRC) has made tremendous progress by publishing the first-ever rules of engagement for civilian hackers active in wars. This endeavour is a direct response to the worrisome increase of nationalistic cyber-gangs since the invasion of Ukraine, which has blurred the distinction between civilian and military hacking.

The International Committee of the Red Cross' rules of engagement for civilian hackers are based on international humanitarian law, with the primary goal of minimising collateral damage caused by cyberattacks during conflicts. These principles forbid the targeting of civilian objects, the deployment of uncontrollable viruses, and the threat of terrorising citizens. They emphasise the importance of protecting medical and humanitarian facilities, which are critical for civilian survival, as well as preventing the instigation of crimes under international humanitarian law. Importantly, these standards encourage compliance even if the opponent does not, reflecting the ethical ideals that guide the ICRC's operations.

While the ICRC's regulations are an important step towards regulating cyber warfare, they confront significant hurdles [2]. Due to the anonymity and decentralised nature of cyber activity, enforcement remains a serious concern. Some hacktivist groups have stated their intention to flout these guidelines, raising worries about their effectiveness. Furthermore, distinguishing between independent hacktivists and those indirectly funded by states can be difficult, complicating enforcement operations.

In a rapidly changing cyber warfare battlefield, the ICRC effort stands as a light of hope. These criteria, which accord with the concepts of proportionality and distinction that underlie traditional combat, can help limit the harm done to civilians and critical infrastructure during conflicts. The voluntary commitment of certain hacktivist groups to adopt these standards is an encouraging sign that the rules can reduce cyberattacks on civilian targets.

However, it is critical to recognise that not all hacktivist groups will voluntarily follow these standards. International collaboration and robust legal frameworks will be required to hold individuals who continue to operate without restraint accountable for their activities [3].

Conclusion

The designation of cyberspace as a new strategic military domain emphasises the growing relevance of cyberwarfare in deciding conflict outcomes. As state-sponsored cyberattacks become more widespread, states

must prioritise the development of effective defences and the formation of close multilateral alliances to combat this growing threat. Continuous research into novel cybersecurity solutions is required to limit the possible effects of cyber activities on global peace and security. Nations may better protect their interests and build a more stable and secure world by grasping the particular difficulties provided by cyberspace and taking proactive actions to guard against cyber warfare.

Cyber practitioners have at their disposal a wide variety of effective cyberware and its resonating power means that future successes in the virtual world can turn into successes in the real world. Cyber warfare represents a fundamental transformation in the very nature of the concept of conflict itself and all conflicts in the future will have a cyber dimension. Efforts must be made to incorporate cyber warfare in international law to attempt to mitigate effects caused, prevent attacks in the future and hold attackers accountable.

REFERENCES

1. Rise of cyber warfare: The growing threat of cyber-attacks in modern conflicts and the impact on businesses. URL: https://www.techuk.org/resource/natsec2023-wbd-20jan23.html
2. Cyber Warfare: Evolving the Modern Battlefield. URL: https://www.atlanticcounciluk.org/single-post/cyber-warfare-evolving-the-modern-battlefield
3. Cyber Warfare in Modern Conflict: Rulebook Redux. URL: https://internationallaw.blog/2023/11/20/cyber-warfare-in-modern-conflict-rulebook-redux/
4. Cyber Warfare: Types, Examples, and How to Stay Safe. URL: https://www.avast.com/c-cyber-warfare
5. Modern Warfare in the Digital World. URL: https://globaledge.msu.edu/blog/post/57128/modern-warfare-in-the-digital-world
6. Cyber Warfare. URL: https://www.imperva.com/learn/application-security/cyber-warfare/
7. Attacks in cyberspace. URL: https://www.britannica.com/topic/scalping
8. Cyber Warfare: The New Front. URL: https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware

Лавренюк Арсен Олександрович – студент 2 курсу Вінницького національного технічного університету, факультету інформаційних технологій та комп'ютерної інженерії, групи 1ПІ-22б, Вінниця, e-mail: arsenlavreniuk@gmail.com.

Науковий керівник: ***Кухарчук Галина Вікторівна*** — викладач кафедри іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: galinakuh07@gmail.com.

Lavreniuk Arsen Oleksandrovich — second year student of Vinnytsia National Technical University, Faculty of Information Technology and Computer Engineering, Group 1PI-22b, Vinnytsia, e-mail: arsenlavreniuk@gmail.com.

Supervisor: ***Kukharchuk Galyna Viktorivna*** – an Assistant Professor of Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: galinakuh07@gmail.com.