Acta of Turin Polytechnic University in Tashkent, 2023, 30, 47-50
Published Online September 2023 in Acta TTPU (http://www.acta.polito.uz/)

THE INTERNATIONAL CONSEQUENCES OF CYBER WARFARE: A STUDY OF THE “STUXNET” CASE

Musakhanov D.
Turin Polytechnic University in Tashkent
Email: diyor.musakhanovv@gmail.com

Abstract– This article attempts to analyse the international consequences of cyber warfare. As an example, the author considered an episode of joint operation of the U.S. and Israel against a nuclear facility located in Natanz, Iran with the aim to destabilise it using the “Stuxnet” computer worm. The study aims to define the concept of cyber warfare and its characteristics, briefly analyse the principle of the virus, understand the impact and consequences of the virus on the international community, and determine further prospects and threats that await us with the development of cyberwars.

Key words– Stuxnet, cyber warfare, cybersecurity.

I Introduction

Cyber warfare is one of the most pressing challenges for international relations at present. With the development of technology and the increase in the number of people who use the Internet and digital technologies, cybercriminals, and government hackers can use cyberattacks to carry out large-scale operations against other states, corporations, or individual users [2].

Cyber warfare can have serious implications for international security, economics, and politics. Cyber attacks can damage critical information infrastructure, and disrupt the functioning of the banking system, energy supply, water supply, transport, and other important sectors of the economy [5]. Cyber warfare can also be used to interfere in the elections and political processes of other states. In this regard, the study of the impact of cyber war on international relations is a relevant and important topic that can help understand how cyber war affects the political map of the world and the role of cyber security in ensuring international security.

The purpose of the study is to create a general picture of the impact of cyber warfare on international relations and an understanding of what global threats are possible due to the high potential of the use of cyber weapons. The results of the study can be used by politicians, cybersecurity specialists, and the scientific community to gain an understanding of the consequences of cyber warfare.

II THEORETICAL BACKGROUND

1. Cyberspace - the complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form [1;9;10].

2. Cyber warfare is the use of cyber-attacks against an enemy state, causing damage comparable to real war and/or disrupting vital computer systems. Some intended outcomes could be espionage, sabotage, propaganda, manipulation, or economic warfare [1;9;10].

3. Cybersecurity - measures and practices aimed at protecting computer systems, networks, and data from threats such as cyber-attacks, viruses, hacker attacks, and cyber espionage [1;9;10].

4. Cyber-attack - malicious activity in cyberspace aimed at violating the confidentiality, integrity, or availability of information systems, networks, or data [1;9;10].

5. Information warfare is a form of conflict in which the parties use information technology, communication tools, and media to achieve their political, military, or informational goals by manipulating information, spreading disinformation, conducting cyber-attacks, and other similar actions [10]. The purpose of the information war is to influence public opinion, weaken the enemy, create chaos, and strengthen one’s position. It is necessary to take into account that one of the features of cyber warfare is the possibility of anonymity and elusiveness of attackers, which makes it even more dangerous. Cyber warfare has both short-

term and long-term consequences, including confidential information, critical loss business interruption, disruption of public order, and others. Cyber warfare can be waged by both state and non-state actors such as cybercriminals, terrorists, and hackers.

III LITERATURE REVIEW

Relatively recently, the world is faced with a completely new principle of warfare, which is completely different from any of the others. Over the years, cyberspace has become one of the key places for the use of military weapons, becoming one of the most important phenomena arising from the development of information and computing technologies. In this literature review, the author attempts to provide brief data regarding existing literature on the theme of cybersecurity and cyber warfare.

To begin with, the book Fundamentals of Cybersecurity. Standards, search, methods, and media (Belous A.I. & Solodukha V.A., 2021) [10] introduces us to the basic concepts of cyberspace, cyber attack, cyberterrorism, cybersecurity, cyber and information warfare. This book is the starting point for understanding the basic principles and terminology in the field of cybersecurity.

In the article (Singer P. & Friedman A., 2014) [9] Cybersecurity and Cyberwar: What everyone needs to know, the authors offer an overview of the general concepts of cyber warfare and cyber security, and discuss possible trends that may affect the field of cybersecurity in the future. In addition, in the article, Cyber Attacks as a Means of Political (Volkova E. 2020) [5], specific cases of cyberattacks and their use as a tool of political influence are considered. The author analyses these cases in detail and provides insight to better strengthen cybersecurity.

Moreover, there is interesting research regarding Stuxnet, particularly by Marie; Robin, Patrice (2017): Hotspot Analysis: Stuxnet. In this study many aspects have been considered, however, some of them were considered quite briefly. For instance, there is not enough information to find out a real international effect. There is a book by (F. Kaplan, 2016) Dark Territory: The Secret History of Cyber War [11], that sheds light on the main events of cyber warfare, such as sabotage, espionage, and attacks on critical infrastructure. Furthermore, this book provides an overview of the challenges which governments and military organisations face in the process of repelling cyber attacks.

Overall, the presented literature review provides us with information on a general overview of the field of cyber warfare and cybersecurity. However, the lack of information in the literature regarding possible consequences is noticed. Probably, it is because of the rapid development of technology and cyberspace in general. In order to raise awareness, expand horizons and provide adequate security in this area, it is important to constantly update the knowledge base, conduct new research in the field of cybersecurity and set international standards in this field.

IV ANALYSIS OF THE IMPACT OF CYBER WARFARE ON INTERNATIONAL RELATIONS

Let us consider the example of the use of cyber warfare tools, in particular the computer worm "Stuxnet" designed by U.S. and Israeli intelligence against the Iranian nuclear facility in Natanz. It is a well-known fact that the most pressing problem of the world community is the unresolved issue of Iran’s nuclear program. This problem was actively discussed at the meetings of the International Atomic Energy Agency (IAEA) in the period from 2006 to 2008 [12]. Several resolutions demanding that Iran stop further development of its own nuclear program did not lead to significant shifts in the resolution of the Iranian crisis [8]. The government of the country announced its intention to continue to develop its own nuclear program for meeting the internal needs of the state and in the interests of the Iranian people. Iran’s refusal to comply with IAEA requirements to stop the uranium enrichment process, set out in the resolutions of the period 2006-2008, led to the dissatisfaction of the world community, primarily the United States and Israel. Statements on the peaceful nature of Iran’s nuclear program were also questioned. As a result, the United States and Israel, in secrecy, began preparing military options to prevent further development of nuclear capabilities. The use of the latest weapons of cyber warfare has become part of this operation. Stuxnet is malware used jointly by the United States and Israel against Iran in order to undermine the further development of the latter’s nuclear program [3;6].

The structure and functionality of “Stuxnet”. Stuxnet uses a variety of distribution methods, including infected USB sticks and network vulnerabilities. It likewise contains several zero-day exploits to gain access to vulnerabilities in “Windows” operating systems. After getting into the computer, Stuxnet tries to spread over the local network by finding vulnerable systems. One of the main tasks of Stuxnet is to damage the centrifuges used in nuclear installations so that they can quickly fail [7].

On the domestic political level, the cyberattack discredited the Iranian government, as the Iranian authorities were not able to protect their nuclear facilities against a foreign cyberattack. Moreover, Iranian authorities did not retaliate against cyberattacks because the identity of the perpetrators was unknown or unclear, and because there was no precedent for how a state should respond to such an attack. Iran acknowledged a cyberattack on its nuclear program, but did not specifically mention “Stuxnet” [3]. This prompted Iran to step up measures to protect its critical systems and infrastructure, as well as to develop its cyber capabilities in response to such a threat. It is believed that Iran is responsible for the course of the retaliatory counter-attack called Ababil [4]. Iran tried to portray itself as a victim of foreign aggression and deflect attention from its own actions. Iran called on international organisations such as the UN and The International Atomic Energy Agency to increase their controls. IAEA began investigating and analysing the attack in order to determine its source and implications for nuclear safety. Also, in a joint statement, the IAEA and Iran have agreed to allow inspectors to conduct closer joint inspections, though the specific terms of what that would mean are unknown [4].

In general, the “Stuxnet” increased tensions between Iran, the US, and Israel, provoked counterattacks, and escalated conflict in cyberspace. The response from the UN has been rather mixed. In 2010, Martin Schulz, then head of the UN General Secretariat, raised concerns about the use of cyber weapons against states. However, there are still no clearly defined international norms in the field of cybersecurity.

In a 2012 episode of 60 Minutes, retired US Air Force General Michael Hayden admitted that despite not being specific about Stuxnet’s creators, he considered the attack a "good idea" [6]. However, he noted that the use of sophisticated cyberweapons designed to affect the psyche has a revealed side. Such technologies are used by other countries in order to achieve their interests. He also took advantage of the fact that Stuxnet’s source code is now available on the Internet, which opens up the possibility of modifying it and targeting it against new targets. Thus, the creation of Stuxnet demonstrated a new reality in cybersecurity, where cyberweapons can take physical damage seriously and have consequences [1]. The openness and accessibility of using the Stuxnet source code highlight the irreversibility of the possibility of artificial change and cyberweapons. An article in Wired that Stuxnet developers "opened the box" demonstrated the capabilities of such a weapon that cannot be returned back [6;10]. Stuxnet has set an important precedent for cyberattacks and has raised questions about international security and the legality of such actions and showed that cyber weapons could sweep the environment with industrial systems, opening up new possibilities for countries and hackers. This is the identification of potentially dangerous vulnerabilities and the possibility of a critical security situation. Stuxnet takes advantage of possible cooperation between states in the development and assembly of cyber weapons. Israel and the US are investigated as the main contender for the creation of this worm, although the exact details have been found unknown [6].

Overall, Stuxnet has been a notable discovery of how cyberattacks can involve multiple sources and have serious consequences. This case demonstrated a new cybersecurity environment where the development and use of sophisticated cyberweapons require close attention, international cooperation, and the development of security measures.

Finally, the manifestation of the Stuxnet virus showed that there are not only amateurs who write viruses of different directions for the purpose of earning money but that technological progress has given rise to "professionals" who perceive information systems solely as a "battlefield" [1;2;10]. Such attacks can cause heightened tensions and mistrust between states, as seen in the case of the United States, Israel, and Iran.

V CONCLUSION

Nowadays, cyber warfare is an integral part of modern international relations, posing a serious threat to critical infrastructure and national security. In addition, the use of cyber weapons for the purpose of physical harm raises complex ethical and legal issues. The origin of Stuxnet remains unclear, but possible collaboration between Israel and the United States points to the need for international cybersecurity norms and agreements in the field of cybersecurity.

Based on the foregoing, it becomes clear that cyber warfare has the potential to change the geopolitical balance of power, as a successful cyber attack can seriously affect the economy, defence, national security, critical infrastructure, and political situation of the victim country. This is a matter of concern and requires continuous strengthening of the readiness and protection of the national cyberinfrastructure.

At the same time, cyber war increases the risks of nuclear war, as the use of cyber weapons becomes an alternative to traditional warfare in the doctrines of some states. For instance, penetration and control of nuclear systems through cyberattacks can have catastrophic consequences, involving unauthorised activation or destruction of nuclear facilities. This creates a potentially dangerous situation where a conflict in cyberspace could escalate into the nuclear realm, putting international stability and security at risk.

VI REFERENCES

[1] Even Sh., Siman-Tov D. Cyber Warfare: Concepts and Strategic Trends, URL: https://www.files.ethz.ch/isn/152953/inss%20memorandum_may2012_nr117.pdf

[2] Roscini M. 2014. Cyber operations and the use of force in international law. Oxford Oxford University Press.

[3] Marie; Robin, Patrice (2017) : Hotspot Analysis: Stuxnet, October 2017, Center for Security Studies (CSS), ETH Zürich, URL :

https://www.researchgate.net/publication/323199431_Stuxnet

[4] Anderson C., Sadjadpour K., 2018. Iran’s Cyber Threat, URL: https://carnegieendowment.org/files/Iran_Cyber_Final_Full_v2.pdf

[5] Volkova E. 2020. Cyber Attacks as a Means of Political Influence, URL:https://cyberleninka.ru/article/n/kiberataki-kak-sredstvo-politicheskogo-vliyaniya

[6] Wikipedia, Stuxnet, URL : https://en.wikipedia.org/wiki/Stuxnet#

[7] Falliere N., Murchu L.O., Chien E., Symantec Security Response, W32.Stuxnet Dossier, URL : https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en

[8] Broad W. Markoff J., 2011. and Sanger D. E. Israeli Test on Worm Called Crucial in Iran Nuclear Delay, URL : https://www.nytimes.com/2011/01/16/world/-middleeast/16stuxnet.html

[9] Singer P., Friedman A. Cybersecurity and cyberwar: What everyone needs to know.Oxford: Oxford univ. press, 2014. - 320 p., URL: https://cyberleninka.ru/article/n/zinger-p-fridman-a-kiberbezopasnost-i-kibervoyna-chto-kazhdyy-dolzhen-znat/viewer

[10] Belous A.I. and Solodukha V.A., 2021. Fundamentals of cybersecurity. Standards, search, methods and medium, Moscow: “Tekhnosfera”, ISBN 978-5-94836-612-8

[11] Kaplan F., 2016. Dark Territory: The Secret History of Cyber War, Simon and Schuster Paperbacks, ISBN 978-1476763262

[12] IAEA, IAEA and Iran: Chronology of Key Events, URL: https://www.iaea.org/newscenter/focus/iran/chronology-of-key-events