IgMin Research STEM ISSN: 2995-8067 A Multidisciplinary Open Access Journal

TECHNOLOGY SUBJECT
Information Security | Network Security | Technology and Society TOPIC(S)

Article Information

Submitted: March 03, 2024
Approved: April 15, 2024
Published: April 16, 2024

How to cite this article: Ciekanowski Z, Żurawski S. Cyber Threat Analysis (CTA) in Current Conflicts. IgMin Res. April 16, 2024; 2(4): 224-227. IgMin ID: igmin169; DOI: 10.61927/igmin169; Available at: igmin.link/p169

ORCIDs:

Żurawski S: https://orcid.org/0000-0001-9527-3391

Ciekanowski Z: https://orcid.org/0000-0002-0549-894X

Keywords: Analysis; Cybersecurity; Cyberspace; Intelligence; Conflicts; Artificial intelligence; New technologies

Research Article

Cyber Threat Analysis (CTA) in Current Conflicts

Zbigniew Ciekanowski[1] and Sławomir Żurawski[2]*

[1]John Paul II University of Applied Sciences, Biała Podlaska, Poland

[2]State Academy of Applied Sciences, Chełm, Poland

***Correspondence:** Sławomir Żurawski, PhD, State Academy of Applied Sciences, Chełm, Poland, Email: slawomir.zurawski@onet.pl

Abstract

Cyber Threat Analysis (CTA) in current conflicts focuses on identifying, monitoring, and assessing potential cyber threats. The main objective is to understand how the parties to the conflict use information and network technologies to conduct warfare, espionage, disinformation, or attacks on digital infrastructure. This analysis includes the identification of actors involved in conflicts and their targets in cyberspace, as well as the analysis of techniques and tools used in cyber activities. The aim of the article is to identify the role of cyber threat analysis in the context of two current conflicts - the war in Ukraine and the Hamas attack on Israel. The article describes the essence of cyber threat analysis. The research problem focuses on identifying and understanding the role of cyber threat analysis in these conflicts and their potential consequences for international security and regional stability. Through the analysis of reports, online sources, and scientific literature, the article aims to familiarize readers with the role of cyber threat analysis in the context of these conflicts and to propose possible strategies for cyber risk management in the face of contemporary armed conflicts. The results of the analysis of cyber threats (CTA) in current conflicts include the identification of specific actors operating in cyberspace, their modus operandi, their objectives, and the techniques and tools used. In addition, the analysis can reveal existing vulnerabilities in digital security and areas that are particularly vulnerable to attacks. To sum up, it is necessary to create recommendations and directions for changes regarding the strengthening of digital security measures, such as software updates, implementation of network security, and increasing staff awareness of cyber threats. In addition, the CTA may suggest the need for better international cooperation to combat cyber threats and the need to develop strategies to prevent and respond to cyber-attacks.

Introduction

The subject of the article is the analysis of cyber threats in current conflicts. In today's fast-paced digital world, where technology is constantly evolving and cybercrime threats are increasingly sophisticated, it is critical to have an effective defense strategy. In response to the growing risk of cyberattacks, organizations around the world are increasingly turning to Cyber Threat Intelligence (CTI) as a key tool in the fight against cyber threats. CTA, or Cyber Threat Intelligence, is the process of collecting, analyzing, and interpreting information about threats to understand their nature, sources, modus operandi, and potential impacts. With CTA, organizations can better understand current and potential threats and make more informed security decisions.

The current situation in Ukraine, where an armed conflict is taking place, has significant consequences not only in the geopolitical context but also in the area of cybersecurity. In the face of this conflict, Cyber Threat Intelligence (CTI) is becoming an even more crucial tool for states, institutions, and enterprises that have to deal with increasingly complex digital threats.

In this article, we will analyze potential cyber threats related to the conflict in Ukraine and discuss the role of CTAs in identifying, monitoring, and repelling these threats. We'll also look at possible cyber-attack scenarios and precautions organizations can take to minimize the risk of security breaches.

Through this analysis, we want to better understand how the conflict in Ukraine is impacting the cybersecurity landscape and what concrete actions can be taken to protect against potential cyberattacks in this changing geopolitical situation.

Research methodology

The research project aimed to present the role of cyber

threat analysis in the context of current conflicts, with a particular focus on the war in Ukraine and the Hamas attack on Israel. The study was based mainly on the analysis of available reports, online sources, and scientific literature in the fields of cybersecurity, geopolitics, and armed conflicts. In the first stage of the study, appropriate sources of information were selected. The focus was on reports from government agencies, international organizations, scientific publications, and credible media. A thorough analysis of the latest cybersecurity reports issued by government agencies, security consultancies, and cybersecurity organizations was conducted. Articles, press releases, and online information on cyber activity related to the conflict in Ukraine and the Hamas attack on Israel were reviewed. It also reviewed the scientific literature on cybersecurity, hybrid warfare, and geopolitics to understand the context and nature of cyber threats in current conflicts. Based on the data collected, an analysis was conducted, conclusions were drawn and a discussion was initiated by following the above steps and procedures, the study provided a comprehensive analysis of the role of Cyber Threat Intelligence (CTI) in the context of current conflicts, allowing replication and further research in the field. Cyber Threat Analysis (CTA) in current conflicts was conducted using a wide variety of data sources and analytical methods. Data collection included a review of available scientific literature, reports, and newspaper articles, as well as publicly available data on cyber incidents and international conflicts.

The collected data were then analysed using qualitative and quantitative methods. Quantitative methods included statistical analysis of cyber incident data, such as attack frequency, impact, and attacker profiles. Qualitative methods focus on analysing the content of information sources in order to understand the motivations, strategies, and goals of the parties involved. In addition, an interdisciplinary approach was used that integrated knowledge from fields such as cybersecurity, political science, and geopolitics. This combination of different perspectives allowed for a better understanding of the complexity of cyber threats in the context of current conflicts and for the development of more comprehensive conclusions and recommendations. Through the use of various methods of analysis and data collection, our work provides a comprehensive view of the issue of cyber threats in the context of conflicts, which enables us to explore the important aspects of this phenomenon and generate accurate conclusions and recommendations.

What is cyber threat intelligence?

Threat intelligence is data that is collected, processed, and analyzed to understand the motives, goals, and behaviors associated with threat actor attacks. Threat intelligence enables us to make faster, more informed, data-driven security decisions and shift their behavior from reactive to proactive in the fight against cybercriminals [1]. The ever-increasing number of cyberattacks requires cybersecurity and forensics professionals to detect, analyze, and defend against cyber threats in near real-time [2]. Cyber threat intelligence (CTI) sharing promises to be a new method of creating situational awareness among data-sharing stakeholders. Moreover, it is seen as a necessity to survive current and future attacks by acting proactively, not just reactively. Organizations may be required to have a threat intelligence program as part of proactive cybersecurity and share their information. Stakeholders may be held accountable in the future for failing to share known risks that impacted others and led to the breach [3]. ENISA has recognised the need to include CTAs in the certification area. In 2020, ENISA set up an ad hoc working group to integrate risk management and CTAs into practices for determining assurance levels [4]. Companies that stick to this basic level of threat intelligence are missing out on real benefits that could significantly strengthen their security posture.

- Threat intelligence is important for the following reasons:
- Sheds light on the unknown, empowering security teams to make better decisions
- Empowers cybersecurity stakeholders by exposing hostile motives and their tactics, techniques, and procedures (TTPs)
- Helps security professionals better understand the decision-making process of cybercriminals
- Empowers business stakeholders such as the board of directors, chief information security officers, chief information officers, and CTOs to invest wisely, mitigate risk, become more efficient, and make faster decisions [5].

The discipline of cyber threat analysis (CTA) has matured significantly over the past year, with organizations across industries adopting it to support their overall security operations. Geopolitical events, in particular the Russia-Ukraine war, have played a key role in convincing the organization that CTA should be considered a central operational requirement [6] (Figure 1).

Cyber threat intelligence in current armed conflicts

How bad can modern cyberwarfare be, and will it affect other countries? “Unfortunately, Ukraine has been Russia’s cyber playground for years,” notes Ciaran Martin, founder of Chief Executive of the National Cyber Security Centre, the defensive arm of GCHQ- Government Communications Headquarters, the UK’s signals intelligence agency [7].

ISSN 2995-8067 DOI: 10.61927/igmin169

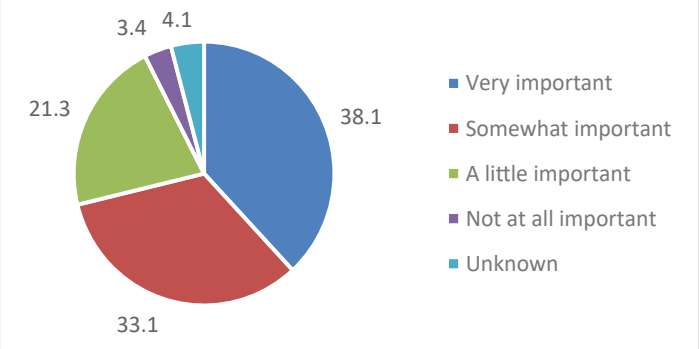

Figure 1: The Figure shows the CTI Survey (2023) for the importance of geopolitics in developing intelligence requirements. Source: SANS 2023 CTI Survey.

Russia's invasion of Ukraine in February 2022 reverberated around the world, and there is no doubt that this has prompted organizations to reevaluate their CTA strategies. In the 2023 SANS CTA survey, 71% of respondents said that geopolitical developments now play a very or fairly important role in determining their intelligence needs. The percentage of responses on the role of geopolitical changes in the CTA is presented below.

Russian cyber operations will evolve as the war continues [8]. Unlike the Russia-Ukraine war, where known cyber operations directly contributed to the conflict, those involved in the Israel-Hamas conflict did not directly contribute to Hamas's military operations against Israel. The full extent and effects of the actions against Israel, particularly by Iranian adversaries in-state ties and allied proxies, are almost certainly not fully known. However, the incidents identified were largely unrelated to early concerns that Iranian cyberattacks could cause significant disruption to critical sectors of Israel and extend their reach to allied countries. This discrepancy may indicate the inability or lack of preparation of Iranian forces and their desire to avoid an unintended escalation that could draw Iran in a more direct way [9].

Hacktivist activity will almost certainly continue as related geopolitical developments fluctuate. The escalation of kinetic warfare can lead to related actions. This assessment is made with a high degree of confidence based on past patterns of action, as well as consistent patterns observed in other similar conflicts.

Discussion

In the context of the war in Ukraine, we are seeing increased activity from hacking groups, which can be both linked to the countries involved in the conflict and act independently, seeking their own benefits. These attacks can target critical infrastructure, government institutions, and private enterprises, which poses a significant threat to the stability of the country and the region. By contrast, Hamas's attack on Israel reminds us of the growing importance of asymmetric warfare, where terrorist groups use cyberspace as a tool to conduct military operations. Cyber-attacks can be used to sabotage infrastructure, attack communications systems, and spread disinformation to weaken an adversary and undermine its defensive capabilities. The discussion on cyber threats in current conflicts points to the need to develop and strengthen defence capabilities and cybersecurity awareness. Organizations, both public and private, need to invest in Cyber Threat Intelligence (CTA), develop strategies to respond to cyberattacks, and work together to build resilience to cyber threats. A joint response of the international community, information sharing, and cross-sectoral cooperation is key to effectively defending against growing cyber threats in armed conflicts. Protecting critical infrastructure, data and communication systems is becoming a priority in the digital age, where cyberspace is becoming the next battlefield. Current research on cyber threats in the context of current conflicts, is important to discuss the existing literature and the relevance of the topic to the field of digital security and geopolitics. There is a growing interest in research on cyber threats, especially in the context of their role in international conflicts and national defence strategies. The academic literature in this field focuses on various aspects of cyber threats, including the identification of actors, attack techniques, tools used by cybercriminals, and how to prevent and respond to attacks. There are also research papers that specifically analyze cases of conflict in which cyberspace plays a significant role. The novelty of our work lies in the focus on current conflicts and current cyber threats, which allows us to explore the specific challenges and strategies used by the parties to the conflict. Our analysis takes into account the latest data and developments, which makes our conclusions and recommendations up-to-date and actionable. By discussing the available literature and highlighting the importance of the topic, our work makes an important contribution to the discussion of cyber threats in the context of conflict, and can also provide a valuable starting point for further research in this field. As a result, readers can better understand the dynamics of cyber warfare and how to effectively protect against cyber threats in times of conflict.

Conclusion

An analysis of cyber threats in current conflicts, such as the war in Ukraine or Hamas's attack on Israel, sheds light on the growing risk of attacks in the digital space. Armed conflicts not only destabilize the political situation but also open the way for the activity of cybercriminals acting on behalf of states or on their own. Hacking attacks, disinformation, and propaganda activities are becoming common tools in the information conflict. In the context of CTA, a proactive approach becomes crucial. Organizations

need to be able to quickly identify, analyze, and respond to possible threats. Raising awareness, investing in CTA technologies, and strengthening security infrastructure and procedures are becoming imperative. The conclusion is that the effective use of Cyber Threat Intelligence in the face of current conflicts requires not only technological know-how but also a strategic approach, analytical capabilities, and cross-sectoral cooperation. These actions are necessary for the protection of critical infrastructure, national security, and private interests against growing cyber threats.

References

1. Strike C. What is Cyber Threat Intelligence? crowdstrike.com. 2024, April 3. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
2. Dehghantanha M. Dargahi CT. Cyber Threat Intelligence: Challenges and Opportunities. Advances in Information Security, ADIS. 2018; 70:1-6.
3. Wagner TD, Mahbub K, Palomar E, Abdallah AE. Cyber threat intelligence sharing: Survey and research directions, Computers & Security. 2019; 87.
4. ENISA Threat Landscape 2020 - Cyber threat intelligence overview. ENISA. 2020, October 20. https://www.enisa.europa.eu/publications/cyberthreat-intelligence-overview
5. CrowdStrike. What is Cyber Threat Intelligence? 2024, April 3. https://www.crowdstrike.com/cybersecurity
6. Fonseca M. SANS 2023 CTI Survey shows cyber threat intelligence is taking root. Silobreaker. 2023, December 11. https://www.silobreaker.com/blog/sans-2023-cti-survey-shows-cyber-threat-intelligence-is-taking-root/
7. The Economist. Will war in Ukraine lead to a wider cyber-conflict? The Economist. 2022, February 24. https://www.economist.com/europe/2022/02/23/will-war-in-ukraine-lead-to-a-wider-cyber-conflict?
8. Grossman T, Kaminska M, Shires J, Smeets M. The Cyber Dimensions of the Russia-Ukraine War, European Cyber Conflict Research Initiative. April 2023.
9. Crowdstrike. Global Threat Report 2024. 2024. https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

How to cite this article: Ciekanowski Z, Żurawski S. Cyber Threat Analysis (CTA) in Current Conflicts. IgMin Res. April 16, 2024; 2(4): 224-227. IgMin ID: igmin169; DOI: 10.61927/igmin169; Available at: igmin.link/p169