A Novel Approach to Cybersecurity Threats Classification by its Nature

https://doi.org/10.31713/MCIT.2024.056

Alla Pinchuk
Department of Telecommunication and
Radio Electronic Systems
National Aviation University
Kyiv, Ukraine
alla.pinchuk@nau.edu.ua

Oleh Polihenko
Department of Telecommunication and
Radio Electronic Systems
National Aviation University
Kyiv, Ukraine
o.poligenko@ukr.net

Roman Odarchenko
Faculty of Air Navigation, Electronics and Telecommunications
National Aviation University
Kyiv, Ukraine
odarchenko.r.s@ukr.net

Abstract—**A comprehensive and precise classification framework is vital for understanding and categorizing cyber threats in the rapidly evolving cybersecurity landscape. Many existing classification models fail to adequately address the diverse and dynamic nature of modern threats. This paper proposes a refined approach to classification, focusing on the nature of cyber threats to provide a more accurate and detailed understanding.**

Keywords—cyber threats, classification approach, cyber threat nature

I. Introduction

Cybersecurity threat nature includes diverse traits, such as the origin, behavior, and motivation of each threat. To the threat nature aspect, the organization can measure how well it can defend itself against such a threat, predict its behavior, and weigh the risk it poses out of which they will design a better defense mechanism. Traditional methods of threat classification mostly rely on a few aspects, which are not capable of catching up with the more sophisticated and adaptive attacks. The requirement to classify threats in a new way can hardly be overlooked nowadays with cyber-attackers that are getting increasingly smarter through the usage of artificial intelligence (AI), and machine learning (ML) techniques to effectively bypass traditional detection systems. This paper examines a new classification of cybersecurity threats that are based on their nature to give a more flexible and dynamic comprehension of modern cyber threats.

II. Problem statement

Existing cybersecurity threats classifications don’t consider threats' nature with enough granularity which makes it ineffective nowadays. Usually, it covered just a few aspects of cyber threat nature. Thus, to achieve the goal of this paper, the next research tasks should be solved:

- analyzing the possible cyber threat nature;
- identifying gaps in existing classifications;
- a classification approach development.

III. Analyzing of the possible cyber threat nature

First of all, cyber threats can have an insider or outsider nature. Insider threats originate from individuals within the organization, such as employees or contractors, while outsider threats come from external actors like cybercriminals or nation-state hackers. Understanding the distinction between these two types is critical for developing tailored security measures. In [1] discussed possible insider threats.

Also, cyber threats nature can be intentional (deliberate actions) or accidental. The categorization of these two types is of prime importance because the plan for handling and decreasing the risks that come with each depends on the same. On purpose, threats often are to be faced with defense practices that involve information like advanced threat detection systems, and real-time monitoring, while accidental threats need to be controlled by regular audits, security training, and policy enforcement to minimize the threats.

Regarding intentional cyber threats, the special report of the Horizon 2020 project highlighted the next: foreign agents, industrial or economic espionage, terrorists, organized crime, insiders, hackers and crackers, political dissidents, vendors, and suppliers [2]. This also lies in the concept of hybrid threats, as described in [3]. It is mentioned that modern cybersecurity threats have a hybrid nature in diplomacy, sabotage and espionage efforts, propaganda, and arms race.

Existing cybersecurity threats can also be defined as technical or non-technical. These threats are discussed in detail in [4-5].

It is also worth to mention AI-driven cyber threats. Nowadays, cyber-attacks become more complicated with AI technologies that describe their evolving nature.

IV. GAPS IN EXISTING CLASSIFICATIONS

As all existing cybersecurity threat classifications can be divided into two categories, based on attack techniques and impact, the last one does not consider cyber threats' nature at all.

In [6], the authors proposed a C^3 model for classifying cyber threats. This model considers two types of threat sources (nature), insiders and outsiders. The authors mentioned that it is possible to develop different subcategories, but an initial version is limited by these two types.

Another existing classification model is the Three orthogonal dimensional model, proposed in [7]. Here, the authors highlighted threat actors' motivation and agents on their own separately. They described motivation as accidental and deliberate, while threat actors (agents) can be human, technological, and “force majeure”.

The pyramidal model [8] highlighted cyber threats nature as cybercriminal's prior knowledge of the system without any further subcategories.

The more detailed classification by cyber threat nature is proposed in [9]. Here authors move with more granularity by adding more layers to classification:

↓ external/internal threat;
↓ human/environmental/technological threat;
↓ malicious/non-malicious threat;
↓ accidental/intentional threat.

However, even the last model fails to encompass all aspects of modern cyber threats nature, especially those posed by AI-driven threats. Given the evolving nature and complexity of contemporary cyber threats, there is a pressing need to develop a more precise and granular classification model that can better accommodate new challenges, including the rise of AI-enhanced attacks.

V. PROPOSED APPROACH

Based on a deep analysis of possible cybersecurity threats nature and existing approaches to classifying by threats nature, we are considering the next main categories: threat actor nature, constantly and rapidly evolving cyber threat nature, threat covert nature, and technical/non-technical threats (Fig.1). Each of them also has subcategories that allow us to classify threats more accurately, except a covert nature.

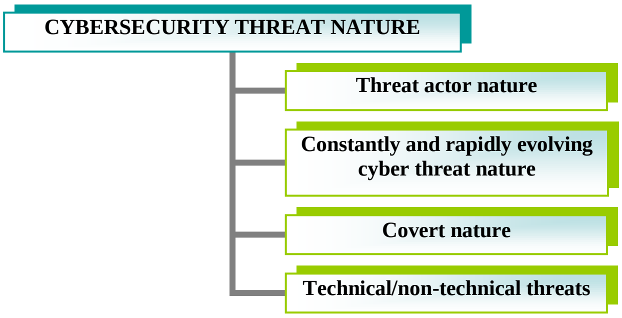
CYBERSECURITY THREAT NATURE
Threat actor nature
Constantly and rapidly evolving cyber threat nature
Covert nature
Technical/non-technical threats

Figure 1. The proposed approach to the classification of cyber threats' nature

A. Threat actor nature

This section aims to subcategorize threat actor nature more granular. First of all, the threat actor can be an *insider* or *outsider* threat. Let’s dive deeply into insider threats. Based on [1, 10-11], insiders can be *unintentional (accidental)* and *intentional (deliberate)*. For the first one, it is possible to include the following:

- *negligent insiders*: an insider who has no malicious intent behind their deliberate inactivity, but caused or raised the possibility of possible future harm to the company's information systems through passive-risk behavior;
- *accidental insiders*: an insider who has no malicious intent behind their deliberate inactivity, but due to a lapse makes an error that caused or raises the possibility of possible future harm to the company's information systems;
- *third-party insider*: a business partner or contractor who has no malicious intent behind their deliberate inactivity, but caused or raised the possibility of possible future harm to the company's information systems through passive-risk behavior or due to a lapse makes an error [11].

The intentional nature can be characterized by the following aspects:

- *malicious insider:* an insider who has malicious intent behind their deliberate inactivity and caused or raised the possibility of possible future harm to the company's information systems;
- *insider collusion:* a type of malicious insider, in which one or more insider threat individuals work with an external partner to compromise their organization. Collusive insider threats often involve a cybercriminal recruiting an employee to steal intellectual property on their behalf for financial gain [11];
- *disgruntled employee:* a malicious insider who may commit deliberate sabotage of security tools, data security controls, or commit intellectual property theft [12];
- *third-party threats:* a business partner or contractor who has malicious intent behind their deliberate inactivity and caused or raised the possibility of possible future harm to the company's information systems [11].

Regarding outsider threats, the first layer of classification is also intentional and unintentional threats. The intentional threats can be as the following:

- *criminal groups:* organized entities involved in illegal activities, such as financial fraud, data theft, or ransomware attacks, often motivated by financial gain;
- *hackers and crackers:* individuals or groups with advanced technical skills who exploit vulnerabilities in systems; hackers may operate with or without malicious intent, while

crackers specifically focus on breaking into systems for personal gain or to cause harm;

- *terrorist organizations:* actors who act to spread fear and desire social or political change;
- *nation-states:* refers to a government or state entity that is involved in cyber-attacks or other activities targeting critical infrastructures of other nations [13];
- *foreign agents:* actors who professionally gather information and commit sabotage for governments;
- *industrial or economic espionage:* refers to actions carried out by one organization against another to acquire a competitive edge in domestic or international markets;
- *political dissidents:* actors who aim to utilize information and information technology to attain a political goal.

Thus, the full classification of the threat actor nature is shown in Figure 2.

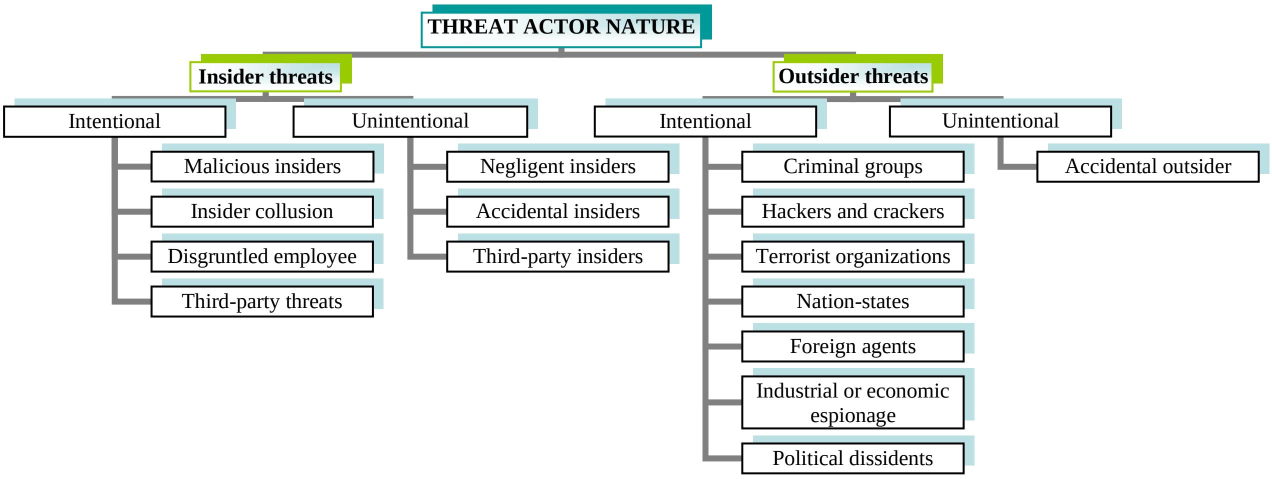

Figure 2. The threat actor's nature classification

B. *Constantly and rapidly evolving cyber threat nature*

Nowadays, the cyber threat landscape is currently and rapidly evolving that caused by utilizing AI-driven and modern technologies, such as quantum computing, etc. Tactics, techniques, and methods of modern cyber-attacks are also rapidly evolving. Another threat is APT groups. They continue to pose a significant threat by using sophisticated methods to infiltrate and dwell within networks unnoticed [14]. Regarding quantum computing, it is a fast-evolving technology that has the potential to transform cybersecurity, but it can also be exploited to break encryption protocols [15].

Thus, we decided to put this category as a cybersecurity threat nature. Subcategories are shown in Figure 3.

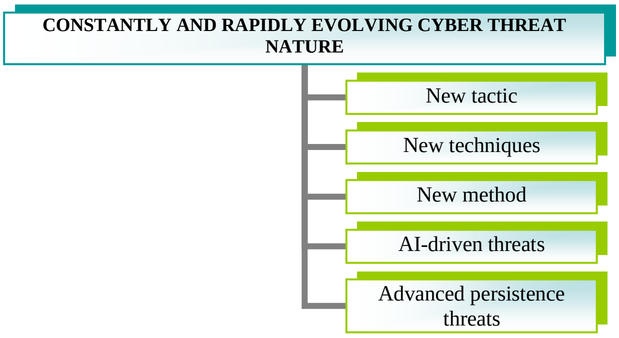
CONSTANTLY AND RAPIDLY EVOLVING CYBER THREAT NATURE
New tactic
New techniques
New method
AI-driven threats
Advanced persistence threats

Figure 3. The constantly and rapidly evolving cyber threat nature subclassification

C. *Covert nature*

Covert cyber threats pose a significant challenge due to their ability to remain undetected within target systems for extended periods. Such threats often employ advanced persistence techniques, allowing them to maintain access to compromised systems even as security measures evolve. This long-term access can enable continuous surveillance, data exfiltration, and other malicious activities without raising alarms [16]. Furthermore, these threats exploit vulnerabilities to establish a foothold within networks, utilizing covert channels to communicate with command-and-control servers while avoiding detection [17].

D. *Technical/non-technical treats*

Threats, both technical and non-technical, require more details. There are various dimensions in which it might occur, such as network-based dimension or internal dimension.

Thus, we may focus on the following aspects or dimensions of technical cyber security threats: persistent and sophisticated threats, network-based threats, credential and access threats, disruptive threats, software and web applications, modern technology threats (such as cloud computing, quantum computing, and Internet of Things (IoT) threats), social engineering (SE), and deceptive threats (here, it means SE that caused by using technologies, for example, phishing attacks, account takeover, etc.)

Threats that are not technological are those that use strategies and techniques to influence people's actions or take advantage of their weaknesses to obtain unauthorized access to private data or systems. Because these threats rely on organizational procedures, human variables, and legal nuances, they are especially difficult to prevent. The following can be highlighted as non-technical cyber security threats: the dimension of internal threats, the dimension of physical breaches, the dimension of third-party cyber security risks, the dimension of SE and identity fraud cyber security threats, and the dimension of legal and regulatory cyber security risks.

The subclassification of this threat nature is shown in Figure 4.

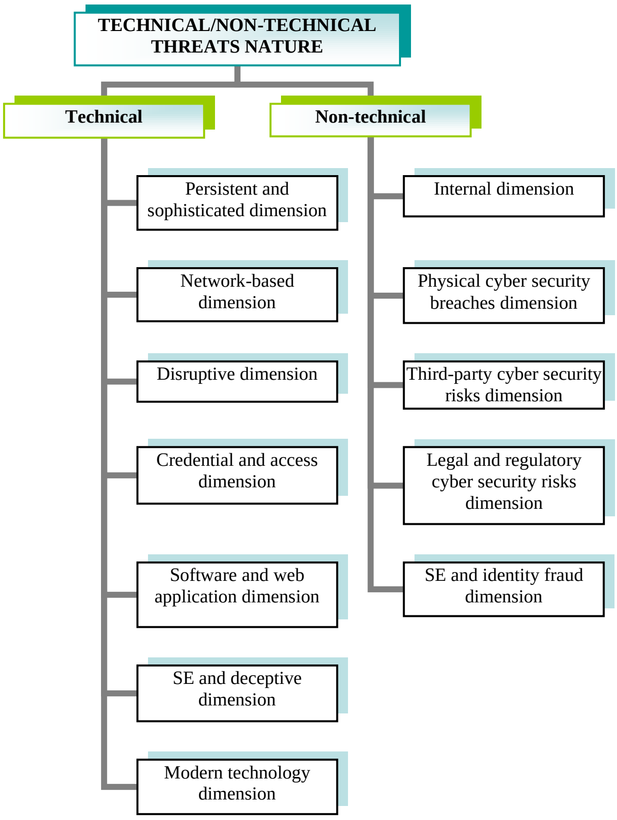
TECHNICAL/NON-TECHNICAL THREATS NATURE
Technical
Non-technical
Persistent and sophisticated dimension
Network-based dimension
Disruptive dimension
Credential and access dimension
Software and web application dimension
SE and deceptive dimension
Modern technology dimension
Internal dimension
Physical cyber security breaches dimension
Third-party cyber security risks dimension
Legal and regulatory cyber security risks dimension
SE and identity fraud dimension

Figure 4. The technical/non-technical cyber threat nature subclassification

VI. Conclusions

The evolving nature of cyber threats requires a more accurate and detailed classification. Traditional models often lack the depth necessary to fully capture the complexity of modern cyber threats, especially those that use advanced technologies such as artificial intelligence and quantum computing. This paper proposes a new approach to classifying cyber threats by their nature, taking into account factors such as the nature of threat actors, the dynamic development of threat tactics, and the covert strategies often employed by sophisticated adversaries. By adopting this more detailed classification, organizations can better predict threats, strengthen their defenses, and address most aspects of today's threat landscape.

Acknowledgment

This work was supported by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060) and "Methods of building protected multilayer cellular networks 5G / 6G based on the use of artificial intelligence algorithms for monitoring country's critical infrastructure objects" (# 0124U000197).

References

[1] Prabhu, Sunitha & Thompson, N. (2020). A Unified Classification Model of Insider Threats to Information Security.

[2] "The nature of cyber threat - Horizon 2020 Projects". Horizon 2020 Projects. [Online]. Available: https://horizon2020projects.com/special-reports/the-nature-of-cyber-threat/.

[3] Tsaruk, Oleksandr, and Maria Korniiets. "Hybrid nature of modern threats for cybersecurity and information security." Smart Cities and Regional Development (SCRD) Journal 4.1 (2020): 57-78.

[4] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," Comput. & Secur. 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2017.09.001.

[5] Winkler, Ira S. "The non-technical threat to computing systems." Computing systems 9.1 (1996): 3-14.

[6] Geric, Sandro & Hutinski, Željko. (2007). Information system security threats classifications. Journal of Information and Organizational Sciences. 31.

[7] Ruf, Lukas et al. "Threat Modeling in Security Architecture – The Nature of Threats." (2008).

[8] Alhabeeb, Mohammed & Almuhaideb, Abdullah & Le, Phu & Bala, Srinivasan. (2010). Information Security Threats Classification Pyramid. 208-213. 10.1109/WAINA.2010.39.

[9] Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489-496.

[10] "Defining Insider Threats | CISA". Cybersecurity and Infrastructure Security Agency CISA. [Online]. Available: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

[11] "What Is an Insider Threat? Definition, Types, and Prevention | Fortinet". Fortinet. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/insider-threats.

[12] "What Is an Insider Threat? Definition, Examples, and Mitigations | UpGuard". Third-Party Risk and Attack Surface Management Software | UpGuard. [Online]. Available: https://www.upguard.com/blog/insider-threat.

[13] "Nation-State Actor". ScienceDirect. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/nation-state-actor.

[14] "Understanding the Evolving Cyber Threat Landscape: Key Insights from Fortinet's Latest Report - Orro". Orro. [Online]. Available: https://orro.group/understanding-the-evolving-cyber-threat-landscape-key-insights-from-fortinets-latest-report/.

[15] Alam, Shahid. "Cybersecurity: Past, present and future." arXiv preprint arXiv:2207.01227 (2022).

[16] Hall, Carissa G., and Neil C. Rowe. "Options for Persistence of Cyberweapons." (2018).

[17] Lamshöft, Kevin, et al. "Knock, knock, log: Threat analysis, detection & mitigation of covert channels in syslog using port scans as cover." Forensic Science International: Digital Investigation 40 (2022): 301335.