Identification of the Emerging Sources of Cybersecurity Threats

Tiina Leppänen and Jussi Simola
University of Jyväskylä, Finland

tiina.s.leppanen@student.jyu.fi
jussi.hm.simola@jyu.fi

Abstract: Rapid evolution of technology has led to the emergence of new and sophisticated cybersecurity threats. Simultaneously, there is an increasing need to enhance understanding of the dynamic and evolving landscape. Organizations balance in managing a sufficient level of information security risks and establish protection against perceived cyber threats, for example, by training employees to identify and report suspicious emails and by adjusting security measures to a level that is pleasing to top management. The landscape of cybersecurity threats has appeared stable in recent years, and cyber criminals' methods may be familiar and in the everyday news, but our vigilance should not be lowered. While overall awareness and capabilities are improving, cyberattacks are unfortunately matching that progress with increasingly sophisticated means. Technologically cyber threats are getting more sophisticated and intense challenging human minds by cleverly covered social engineering and unexpected zero-day exploits. Emerging technologies like generative Artificial Intelligence (AI), the global geopolitical situation, and aggressively evolving ransomware attacks are keeping cybersecurity professionals on their toes. What are the chances of winning the race against these invisible enemies without continuous monitoring and staying current with threat intelligence? This study aims to identify and analyse emerging threat sources by systematically reviewing recent research and examining well-established threat actor frameworks. The goal is to uncover the latest cybersecurity threats and signals that indicate their emergence. By using the present state of threat landscape within the European Union (EU) as a reference framework, this assessment provides a comprehensive. Key signals for identifying new threats are highlighted, such as unusual activity patterns and risk-based assessments. Additionally, the study identifies the most frequently used sources of threat information, emphasizing the importance of real-time data and recent publications in maintaining up-to-date threat awareness. The results highlight key themes and trends in the current cybersecurity landscape, revealing significant threat actors and novel attack vectors.

Keywords: Cybersecurity threats, Emerging threats, Threat actors, Threat sources

1. Introduction

Identifying various types of threats has been a cornerstone of security in protecting critical infrastructure and vital functions. In our digitalized environments, the significance of gathering information from diverse sources is increasingly evident. Adversaries try to find different ways to damage or interrupt common values in societies. Ongoing hybrid warfare requires efficient response mechanisms against cyber threats. The fundamental need is to take a few steps onward cybersecurity before anything may happen.

Latest security tendencies are detecting and gathering weak but necessary signals based on broader EU-level strategic lines (European Commission, 2020, 2022). Decision-makers need coherent information to form overall situational awareness. Technical solutions, processes, and humans form the cybersecurity triangle. Sharing emerging data is insufficient, the key is to understand its implications from different viewpoints. The challenge lies in creating secure ecosystems in a globalized world where businesses operate without borders. While it is necessary to follow directives, guidelines, or standards, we can only aim to mitigate or manage risks.

It is a reality that technology is evolving rapidly, and so are threats. The race is a continuous battle where technological advancements frequently introduce new vulnerabilities, while cybersecurity innovations tirelessly work to counteract these emerging threats. Threats are disrupting our digital life. Cybercrime can impact organisations quickly and unexpectedly, and expenses encompass various aspects: data manipulation or theft, decreased productivity, forensic investigations, recovery, reputational damage, and regulatory penalties.

AI is still considered newcomer in cybersecurity arena, yet it has already gained big foothold on both fronts: AI enhances proactive threat identification methods but simultaneously it offers a whole new world of opportunities for cyberattacks and bypassing defences.

Although cyber threats have existed for ages, term "emerging" is justified by several factors that highlight evolving nature and increasing sophistication of these threats. To identify emerging threat sources, systematic literature review was conducted. This paper outlines the research process and findings that address the research questions, followed by conclusions drawn from these answers.

2. Research Posture and Design

Cyber threat landscape is evolving rapidly with attack methods quickly adapting to new technologies and exploiting vulnerabilities. According to CrowdStrike (2025), average breakout time for adversaries has drastically declined, with the fastest recorded being less than a minute. Organizations must urgently understand the surrounding threats and prioritize safeguarding their critical assets against specific threats they face. This requires adaptive risk management strategies that evolve with potential threats (Ncube, 2024). Manoharan (2024) identifies key factors challenging the understanding of cybersecurity risks: evolving threat tactics, expanding attack surfaces, regulatory compliance requirements, impact of cyber-attacks and cybersecurity skills gap.

2.1 Emerging Threats

A threat is any deliberate or unintentional action by an individual or organization that can harm automated information system or activity (NIST, 2025). Damingo et al. (2024) describe threats as 'hostile acts' originating from humans or nature. Cyber threats have existed since the early days of computer networks, evolving from 1970s hacking incidents to today's massive data breaches and financial losses. These threats include actions like stealing or destroying data, breaching privacy, spreading misinformation, and disrupting network functions. They range from simple phishing attempts to complex, multi-vector attacks by organized groups (Snyder, 2023)."

At high-level glance, the landscape of cyber threat terrain seems stable. News of stolen identities and lost savings due to email phishing and ransomware attacks are daily occurrence. Citizens are being warned about fake messages from authorities and informed on how to identify false web addresses.

What are emerging threats, then? According to Cambridge Dictionary ‘emerging’ (2025) is - in addition to “becoming apparent, prominent, or starting to exist” - often used to describe something that is “in the process of developing or gaining recognition”. In this study, an emerging threat is defined as threat which is commonly observed, growing, and becoming more significant.

2.2 Threat Sources and Actors

Definitions of threat entities can vary widely due to synonyms and differing contexts. For example, the NIST glossary defines that ‘threat source’ as the intent and method used to intentionally exploit a vulnerability, or situation that could unintentionally activate vulnerability. It also refers to ‘malicious person’ and is synonymous with ‘threat agent’. Despite of source type, threat source can harm an organization’s operations, assets, or other organizations through unauthorized access, destruction, disclosure, modification of information, or denial of service.

Proactive and robust cyber threat management and incident response require understanding how threat actors assess objectives and methods. A threat actor is an individual or group exploiting vulnerabilities in computer systems and networks, or conducting malicious activities like phishing, ransomware and malware attacks. (NIST, 2025; ENISA, 2024; IBM,2023) Terminology for threat actors varies widely, potentially causing confusion in threat intelligence. Table 1. presents examples of these naming differences.

Table 1: Examples highlighting differences in threat actor naming conventions

ENISA (2024)	IBM (2023)	Microsoft (2025)	SentinelOne (2021)
State-nexus actors	Nation-state actors	Nation-state actors	Nation-States
Cybercrime actors	Cybercriminals	Financially motivated actors	Cybercriminals
Hacker-for-hire actors	Cyberterrorists	Private sector offensive actors	Terrorist Groups
Private sector offensive actors	Thrill-seekers	Influence operations	Thrill-seekers
Hacktivists	Hacktivists	Groups in development	Hackers
Insider threats	Insider threats		Insider Threats

Threat actors are typically motivated by financial gain, espionage, destruction, and ideology. However, the distinctions between them are becoming blurred as they collaborate and share resources, tactics, and objectives. This makes it challenging to base mitigation and response strategies on anticipated motivations.

2.3 Research Questions

The objective of this research is twofold. The aim is to compile and analyse recent findings on new threat sources and related information. By comparing the results with the existing threat landscape report of this field, this study also aims to investigate a possible lack of comprehensive studies identifying emerging threat sources and signals. To achieve these objectives, the following research questions are posed:

- Q1: What are the emerging threat sources identified by research studies?
- Q2: What are the signals that identify new and emerging threats?
- Q3: What are the most used sources of threat information, and where is the most recent information?

The first research question investigates what the most mentioned emerging threats in the most recent studies are. Findings are analysed using results and frameworks defined in ENISA's threat landscape report. The second question focuses on identifying indicators that can help in the early detection of threats. Signals mean in this context, information or data and data sources. The third question evaluates the reliability and timeliness of various threat information sources. These three research questions provide information on current research on emerging threats.

2.4 Literature Review

This research, based on a systematic literature review (Kitchenham and Brereton, 2013), utilizes scientific publications, cybersecurity directives, reports and guidelines to form its framework. How much research has been conducted on identifying emerging threat sources?

2.4.1 Selection criteria and process

The search focused on research papers and studies identifying emerging threats, narrowed to the past three years to ensure up-to-date results. Defining search criteria was challenging since all cybersecurity research involves threats. Therefore, specific inclusion criteria were established:

- Research meets defined search criteria, discussing emerging threats from a general perspective and covering widely recognized threats.
- Research paper is peer-reviewed and openly available with University of Jyväskylä access rights.
- Publications are from years 2023 to 2025 and in English.

The following exclusion criteria were used to assess the significance of search results:

- Research focuses on specific threats, technology (e.g., AI, Quantum computing or IoT), location or context (e.g., healthcare or finance sector).
- Publications from Russian and Chinese institutions, unclassified articles.
- Publications with incomplete publication information or meanings.

2.4.2 Search criteria

To gain good coverage of research articles, used scientific databases used were IEEE Xplore library, Jyväskylä University Library JYKDOK, Scopus, SpringerLink and Google Scholar. Searches were focused on title, abstract and keywords using criteria: ("cybersecurity" OR "cyber security") AND ("emerging threats" OR "new threats" OR "threat landscape"). The number of search results was IEEE Xplore 208, JYKDOK 234, Scopus 350, SpringerLink 350 and Google Scholar 88. Searches were conducted between February and March 2025.

2.4.3 Data extraction

Titles and abstracts were initially screened to identify relevant results. Data extraction was organized in a spreadsheet based on the study's objectives: emerging threats, identification methods, and data sources. Table 2 presents the most relevant research papers.

Table 2: Relevant research papers.

Title	Authors	Published in	Year
Emerging Threats in Cybersecurity: A Review Article	Kumar, I.	International Journal of Applied and Natural Science	2023
The New Frontier of Cybersecurity: Emerging Threats and Innovations	Dave, D., Sawhney, G., Aggarwal, P., Silswal, N. and Khut, D.	29th International Conference on Telecommunications	2023

Title	Authors	Published in	Year
Emerging threats in cybersecurity: Risk and vulnerability management	Ncube, Z. M.	Journal of Innovative Technologies	2024
Understanding the Threat Landscape: A Comprehensive Analysis of Cyber-security Risks in 2024	Manoharan, A.	International Research Journal of Modernization in Engineering Technology and Science	2024
Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age	Jony, A. I. and Hamim, S. A.	Journal of Information Technology and Cyber Security	2023
AI and Cybersecurity in 2024: Navigating New Threats and Unseen Opportunities	Praveen, T.	International Journal of Computer Trends and Technology	2024
Emerging Threats in Cybersecurity Space	Damingo, L. A., Elliot, K. N. and Ojekudo, N. A.	International Research Journal of Modernization in Engineering Technology and Science	2024
AI-Enhanced Cybersecurity Proactive Measures against Ransomware and Emerging Threats	Rossi, A. and Bianchi, G.	Innovative: International Multidisciplinary Journal of Applied Technology	2024
Fast-changing cyber threat landscape and a new reality of cybersecurity	Kedys, A.	Cyber Security	2025

In addition to research papers, publicly available reports and white papers were reviewed. With similar search and selection criteria, following documents were included in this research:

- CrowdStrike 2025 Global Threat Report
- CyberProof 2025 Global Threat Intelligence Report: Mapping Threats and Trends
- ENISA Threat Landscape 2024
- ENISA Foresight Cybersecurity Threats for 2030
- SANS 2024 CTI Survey: Managing the Evolving Threat Landscape
- World Economic Forum, Global Cybersecurity Outlook 2025

3. ENISA Threat Landscape

Since 2004, the European Union Agency for Cybersecurity (ENISA) has worked to ensure high cybersecurity standards across Europe. By sharing knowledge, building capacity, and raising awareness, ENISA collaborates with key stakeholders to enhance trust in the digital economy, improve infrastructure resilience, and ensure digital security for Europe's society and citizens. ENISA tracks the cybersecurity threat landscape through its annual ENISA Threat Landscape (ETL) report. (ENISA, 2024)

The ETL 2024 report was chosen as the reference framework for its comprehensiveness, covering various sectors and technologies while remaining vendor and industry-agnostic. Its reliability is based on information from open sources, ENISA's Cyber Threat Intelligence (CTI), security researchers, blogs, and news. CVE landscape, a new addition, highlights threat actor targets and underscores the importance of vulnerability disclosure and timely patching.

Key findings on 2024 cybersecurity threat landscape highlight the influence of regional conflicts and the expansion of hacktivism, driven by major events like European elections. Data availability remains the most targeted threat. Seven primary threat types are identified due to their consistent prominence, widespread occurrence, and substantial impact:

- *Distributed Denial of Service* (DDoS) is *threat against availability* where attackers aim to make service and resources unavailable by overloading it with flood of superfluous network requests. This threat source has been around for 25 years and continues to lead charts. The scale of attacks has increased due to the availability of easily deployable tools and services (e.g., DDoS-for-Hire services).
- *Ransomware* is a threat source where malicious actors take control of the target's assets and demand ransom to restore asset's availability or to prevent public exposure of the target's data. Evolving threat landscape, rise of multiple extortion techniques, and diverse objectives of these actors contribute to the complexity of the situation.
- Data breaches and data leaks are *threats against data* that can result in account takeovers and identity theft. The difference between them lies in their occurrence: a data breach is a deliberate

attack with the intent to steal data, while a data leak occurs unintentionally due to poor security practices.

- *Social engineering* covers a wide selection of activities that aim to exploit human error or human behaviour and gain access to information. Typical attack vectors are phishing, spear-phishing, honey traps and vishing, increasingly empowered with AI. Fake AI chatbots are novel attack vectors for stealing login credentials, while the quality and believability of generative AI-assisted scams have developed dramatically fast.
- *Malware* is software typically delivered to a target through social engineering or by compromising system protections. Its aim is to disrupt operations, steal sensitive information, or gain unauthorized access to systems. Common types of malware include viruses, worms, Trojan horses, ransomware and spyware.
- *Supply chain attacks* target organizations by exploiting vulnerabilities within their supply chains. Attackers often focus on third parties, believing they have least effective defences. This threat source is emerging through social engineering.
- *Information manipulation and interference* is ranked mainly because of the geopolitical situation aiming to negatively impact values, procedures and political processes. An evolving aspect is the experimental use of AI in information manipulation.

Trends related to threat actors shed light on the most significant ones. Assessment provides an overview of the most significant threats observed at a strategic level. These five threat actor categories are:

- *State-nexus actors:* Their objectives are espionage and disruption. While not novel, their methods are advanced, large-scale, and long-term enhanced with AI. They spend considerable time investigating targets to identify weaknesses and entry points, focusing on avoiding operational mistakes. Their widespread adoption introduces new challenges for defenders, such as increased fleetingness and temporariness of indicators.
- *Cybercrime actors:* Driven by financial gain or profits, their attacks are opportunistic and indiscriminate, involving theft, extortion, and monetization of information. Increased level of collaboration and professionalization is making them a formidable force.
- *Hacker-for-hire actors:* The Professionalization of the cybercrime market has led to the provision of services to state-affiliated actors, thereby lowering the barriers to entry for criminal activities. This includes offerings such as Ransomware-as-a-Service (RaaS).
- *Private sector offensive actors (PSOA):* Developing and selling cyberweapons to a variety of clients. Growing concern in the cybersecurity landscape due to their ability to provide advanced cyber capabilities to a wide range of clients.
- *Hacktivists:* Highly motivated actors. Targeting disruption to affect some form of political or social change. Diverse and vary heavily in skillsets and capabilities.

Absence of *internal threats* from the list has been explained by a low number of reported incidents. However, the risk level has not decreased; instead, information has not been shared of the events.

ETL report predicts that AI is very likely to amplify the frequency and severity of cyber-attacks in the coming two years. Threat actors are using generative AI to develop new zero-day ransomware and malware, enhance the sophistication of phishing attack artifacts, serve as a personal assistant for hacker training, support bypassing defence systems, and produce deepfakes. (ENISA, 2024)

4. Findings

4.1 Emerging Threats

According to ETL 2024 report, DDoS and ransomware attacks are the most reported threats for the second consecutive year, accounting for nearly 70% of all analysed incidents. Combined with threats against data, this figure rises to 90%. The World Economic Forum (2025) findings align, with nearly half of organizations ranking ransomware as their top concern. This study reviewed selected papers and reports against ETL 2024 threat trends, identifying ransomware, malware, threats to data availability, and supply chain attacks as the most mentioned threat sources. A summary of these findings follows.

Ransomware attacks, which began in the 2010s, have become increasingly complex and targeted. ‘Ransomware 2.0’ uses AI to identify high-value targets and automate ransom negotiations (Praveen, 2024). Modern and complex attack techniques are not hindering attackers, as Ransomware-as-a-Service (RaaS), cybercrime business

model to purchase RaaS kit and launch attack, does not require technical skills. (Dave et al, 2023; Manoharan, 2024) The financial impact of ransomware is substantial, and recovery measures exert pressure on business continuity, adding financial strain. (Ncube, 2024) Although a type of malware, ransomware is often classified separately due to its specific nature. (Kumar, 2023) Future ransomware developments are expected to involve quicker and more aggressive tactics. Attackers are leveraging AI to improve accuracy and exploiting interconnected systems for widespread disruption. (CyberProof, 2024)

Malware is one of the oldest groups of cyber threats. The development of malicious software and its delivery channels follows the evolution of information technology, and it is designed to harm or exploit computers or networks. (Kumar, 2023) Malware can gather data and conduct surveillance over a long period without triggering any alerts (Damingo et al, 2024). Self-learning malware is an emerging AI-driven malware being able to autonomously learn from its environment and adapt its actions to avoid being detected. (Praveen, 2024)

Threats against availability have increasingly become a significant trend throughout this millennium. The research results show that the means of DDoS attacks vary. Evolution started from single source attacks and the current trend is botnet or multiple systems based, where networks of compromised gadgets are used. While countermeasures against Denial of Service (DoS) attacks are advancing and disruptions can often be prevented on minimized, attackers are expanding their global army by enlisting unprotected devices like routers and IoT gadgets. (Dave et al, 2023; Ncube, 2024; Jony and Hamim, 2023) The role of a comprehensive incident response plan is highlighted to efficiently mitigate attack effects and minimize damage. Varied motivations associated with this threat source explain its persistence and complexity. Threat actors vary from experimental thrill-seekers seeking for fun to professional adversaries aiming for substantial financial rewards. (Kumar, 2023; Jony and Hamim, 2023)

Social engineering is a threat that can take various forms. (Kumar, 2023; Dave et al, 2023) Exploiting human behaviour is an attack vector that is not easy to protect with technology. That explains its popularity since the early days of computing. Among different types of phishing attacks, spear phishing and email attacks are ranked as the most common. (Damingo et al, 2024) However, an emerging trend is phishing attacks enhanced with AI by generating highly personalized and convincing emails. According to Praveen (2024), 75% of all phishing attempts were AI-driven in 2024. Powered by AI, voice phishing (vishing) saw explosive growth of 442% in 2024 (CrowdStrike, 2025).

Threats against data can be data breaches or data leaks. The data breach is an intentional attack, while a data leak is an unintentional event. One of the major data breach attacks is identity theft. As a result, sensitive, confidential, or protected data is released or exposed. Manoharan (2024) predicts that privacy will be a significant challenge in a hyper-connected world. For example, biometric data is highly targeted by cybercriminals for theft and manipulation.

Supply chain attacks are targeting interconnected networks of organizations. These attacks thrive in complex relationships and connections between suppliers and sub-suppliers. Exploiting one vulnerability in the chain can cause a domino effect, infiltrating multiple organisations and potentially compromising the data of clients or citizens. CyberProof (2024) has observed a significant trend where a smaller number of software supply chain breaches are affecting a larger number of customers. This underscores the extensive reach and effectiveness of these attacks. According to the report of the World Economic Forum (2025), supply chain challenges were identified by 54% of large organizations as the primary obstacle to achieving cyber resilience. Global statistics indicate that supply chain breaches increased by 68% in 2024. In addition to growing dependence of digital ecosystems, evolving tactics of adversaries reflect growth in supply chain attacks.

In the selected research papers and reports, *advanced persistent threats (APT)* were frequently mentioned among identified emerging threats. APT has been seen as a major concern in recent years, by means of sophisticated and targeted attacks sponsored by nation-states. Typical of this threat source is that they are difficult to detect, and operations can continue for a long time.

4.2 Signals for Identifying new and Emerging Threats

To identify new and emerging threats, cybersecurity professionals must stay aware of the latest trends, vulnerabilities and attack techniques. Early identification of the latest attack vectors enables proactive responses to counter and mitigate these risks. It is essential to regularly perform network security evaluations and penetration tests to uncover vulnerabilities, misconfigurations, and weaknesses in network infrastructure, and take immediate action to resolve them. (Manoharan, 2024)

Threat hunting is a proactive approach for assessing threats that have not yet been identified or addressed within an organization's network. Especially in threat sources where attackers' tactics is to remain undetected for extended periods, threat intelligence and advanced detection technologies can help identify and respond in a timely manner. For the first time, the SANS Cyber Threat Intelligence (CTI) survey inquired about the implementation of threat modelling. Nearly half of the respondents reported having a formal threat model, and this trend is expected to increase. Use of frameworks like MITRE ATT&CK is recommended not only for categorizing attack methods but also for facilitating coherent communication. (Brown and Sfakianakis, 2024)

Modern threat hunting techniques utilize advanced tools and methodologies to identify and mitigate potential risks. One such advanced tool is behavioural analytics, in which normal behaviour, deviations can be flagged by comparing them to the baseline of normal behaviour. This approach is particularly effective in identifying insider threats and sophisticated attacks that evade traditional security measures. Integrating threat intelligence into threat hunting empowers more accurate threat detection and responding. (Kedys, 2025)

According to reviewed research, traditional methods like antivirus software and regular scanning remain essential for detecting malware. However, emerging technologies such as AI-driven solutions and big data analytics are increasingly effective in identifying anomalies and potential threats. Additionally, cloud security tools, when combined with automation, empower organizations to navigate the complex threat landscape more efficiently. (Ncube, 2024)

The most recommended way to identify threats is through a holistic and collaborative approach. As noted by Hammad, Saleh and Alomari (2024), information sharing and collaboration play an important role in signalling and threat identification. Vendors, commercial companies and public authorities are well-known threat information sources, but the level of collaboration could be better. Beyond identifying and defending against threats, knowledge gained from recovering and learning from disruptions is invaluable and should be shared. Consequently, incident reporting has become one of the primary requirements in recent regulations (e.g., in EU's NIS 2 directive).

4.3 Threat Information Sources

There are several data sources available to address emerging threats. Today, it is everybody's responsibility to stay updated on the most recent trends and means of cybersecurity threats. For cybersecurity professionals, requirements are more demanding: identifying and managing threats covers all aspects of the computing world from technology to users. In addition, there are several stakeholders (including authorities and regulations) to collaborate with. (Kumar, 2023)

With the increasing prevalence and sophistication of cyber threats, it is essential for organizations to continuously reevaluate their cybersecurity strategies and place strong emphasis on managing risks and vulnerabilities. Vulnerability management, where vulnerabilities are prioritised based on risk assessment criteria to ensure that the most critical threats are addressed first. (Ncube, 2024)

THE SANS CTI report states that analysing open-source intelligence (OSINT) from different sources helps prioritize threat scenarios and related defensive efforts. Utilizing external sources like research reports, cybersecurity news, intelligence reports, and threat feeds is getting more efficient thanks to insightful summaries and analytic tools. Survey results indicate a decline in the use of internal data, such as incident reports, analytics data, and SIEM. (Brown and Sfakianakis, 2024)

Threat information sources are crucial for delivering varied, timely, and precise data needed to identify cyber threats. This highlights the significance of having a structured collection plan to organize the data gathering process, ensuring access to the most relevant and actionable information.

5. Conclusion

The landscape of cyber threats is constantly evolving and expanding. This research revealed that classification and grouping of threats have been rather stable, but new technology trends are changing the way threat actors operate and the power of attacks. Rapid increase in AI-driven attacks and a shift towards more sophisticated and evasive techniques are trending now and are expected to grow. Intelligent and agile threat sources and actors are challenging organisations' advantages over their adversaries.

ETL 2024 report ranks threats against availability, ransomware, and data-related threats at the top. According to the literature review findings, ransomware, social engineering, and malware were the top three threat

sources compared to the prime threats in ETL 2024. The next most mentioned threat sources are threats against availability and supply chain attacks, while social engineering is next in ETL 2024.

ENISA has updated its foresight of cybersecurity threats for 2030 since 2022. In 2024, supply chain security was still ranked as the most substantial risk. When its impact and likelihood have slightly declined since 2022, AI-related threats' likelihood has arisen, which reflects heightened awareness of vulnerabilities that malicious actors may exploit in digital ecosystems. (ENISA, 2024b)

AI-enabled information manipulation is an example of a threat that has been identified but not included in ETL 2024 statistics, yet. It is in an evolving state, and threat actors are assessing how AI can be exploited. In general, the trend of AI-powered cyber-attacks is undoubtedly rising. Reviewed research indicates that emerging threat sources include quantum computing threats, IoT exploitation, biometric data breaches, and supply chain attacks. The potential of AI is also in threat identification. Predictive analytics using AI was tested by analysing historical threat data and predicting future attack vectors. The results revealed 85% accuracy rate in predicting potential threats. (Praveen, 2024) AI is expected to help in proactive threat identification in many ways. AI-powered threat intelligence platforms can collect and analyse threat data from global sources in real-time. Automatic and timely sharing of threat intelligence across organizations and industries, including their defence systems, is one probable model of collective defence against the most current threats. Preventing the same threats from affecting other organizations is a valuable goal in addition to predictive information on emerging ones.

Regulation and cybersecurity standards will have an impact on the shape of the threat landscape. When organizations focus on achieving compliance and bolstering their defences, attackers may shift their targets to less regulated areas, such as third-party vendors. Grasping the adversary and their motivations behind cybersecurity incident or targeted attack is crucial, as it reveals what the attacker is seeking. Evaluating these motives offers insight into attackers' intentions and aids entities in concentrating their defensive efforts on the most probable attack scenarios for specific assets. The results of the literature review highlight the critical need for continuous vigilance and proactive measures to counter rapidly evolving threats. Resilience, innovation, and adaptability of adversaries highlight the urgent need for a thorough understanding of contemporary threats across every aspect of the landscape.

Acknowledgments:

The research was supported by Business Finland (grant number 10337/31/2023) and the University of Jyväskylä.

Ethics declaration: Ethical clearance was not required for the research.

AI declaration: AI tools were not used in the creation of this paper.

References

Brown, R. and Sfakianakis, A. (2024) 'SANS 2024 CTI Survey: Managing the evolving threat landscape'. Available at: https://www.sans.org/white-papers/sans-2024-cti-survey-managing-the-evolving-threat-landscape/ (Accessed: 5 March 2025).'Emerging' (2025) *Cambridge Dictionary*. Available at https://dictionary.cambridge.org/dictionary/english/emerging (Accessed 8 March 2025).

CrowdStrike. (2025) 'CrowdStrike 2025 Global threat report'. Available at: https://www.crowdstrike.com/global-threat-report-2025/ (Accessed: 5 March 2025).

CyberProof. (2025) '2025 Global threat intelligence report: Mapping threats and trends'. Available at: https://www.cyberproof.com/2025-global-threat-intelligence-report/ (Accessed: 8 March 2025).

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N. and Khut, D. (2023) 'The new frontier of cybersecurity: emerging threats and innovations', *29th International Conference on Telecommunications (ICT),* pp. 1-6.

Damingo, L. A., Elliot, K. N. and Ojekudo, N. A. (2024) 'Emerging threats in cybersecurity space', *International Research Journal of Modernization in Engineering Technology and Science,* 6(5), pp. 10662-10671.

ENISA. (2024) 'ENISA threat landscape 2024'. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (Accessed: 20 February 2025).

ENISA. (2024b) 'Foresight cybersecurity threats for 2030'. Available at: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 (Accessed: 1 March 2025).

European Commission. (2020) Joint Communication: The EU´s Cybersecurity Strategy. Available at https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (Accessed 6.4.2025)

European Commission. (2022) NIS2 Directive (EU) 2022/2555. Available at https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (Accessed 6.4.2025)

Hammad, A., Saleh, H. and Alomari, M. (2024) 'Advancements in cybersecurity: Novel approaches to protecting against emerging threats and vulnerabilities', *CyberSystem Journal*, 1(1), pp. 9-22. doi: https://doi.org/10.57238/r15e5074.

IBM. (2023) 'What is a threat actor?'. Available at: https://www.ibm.com/security/what-is-a-threat-actor (Accessed: 10 March 2025).

Kedys, A. (2025) 'Fast-changing cyber threat landscape and a new reality of cyber security', *Cyber Security*, 8(3), pp. 273-280. doi: https://doi.org/10.69554/ZLHB7981.

Kitchenham, B. and Brereton, P. (2013) 'A systematic review of systematic review process research in software engineering', *Information and Software Technology,* 55(12), pp. 2049-2075.

Kumar, I. (2023) 'Emerging threats in cybersecurity: A review article', *International Journal of Applied and Natural Sciences*, 1(1), pp. 01–08. Available at: https://bluemarkpublishers.com/index.php/IJANS/article/view/2 (Accessed: 2 March 2025).

Manoharan, A. (2024) 'Understanding the threat landscape: A comprehensive analysis of cyber-security risks in 2024', *International Research Journal of Modernization in Engineering Technology and Science,* 6(3), pp. 5706-5713.

Microsoft. (2025) 'How Microsoft names threat actors'. Available at: https://www.microsoft.com/security/blog/2025/05/03/how-microsoft-names-threat-actors/ (Accessed: 8 March 2025).

Morgan, S. (2023) 'Cybercrime facts, figures, predictions, and statistics for C-suite executives'. Available at: https://www.secureworks.com/blog/cybercrime-facts-figures-predictions-statistics (Accessed: 9 March 2025).

Ncube, Z. M. (2024) 'Emerging threats in cybersecurity: Risk and vulnerability management', *Journal of Innovative Technologies,* 7(1), pp. 1-8. Available at: https://acadexpinnara.com/index.php/JIT/article/view/320 (Accessed: 3 March 2025).

NIST. (2025) 'Glossary'. Available at: https://csrc.nist.gov/glossary (Accessed: 2 March 2025).

Praveen, T. (2024) 'AI and cybersecurity in 2024: Navigating new threats and unseen opportunities', *International Journal of Computer Trends and Technology* 72(8), pp. 26-32. Available at: https://philpapers.org/rec/PRAAAC-2 (Accessed: 1 March 2025).

Rossi, A. and Bianchi, G. (2024) 'AI-enhanced cybersecurity: Proactive measures against ransomware and emerging threats', *Innovative: International Multidisciplinary Journal of Applied Technology*, 2(11), pp. 77-92. Available at: https://multijournals.org/index.php/innovative/article/view/2721 (Accessed: 20 February 2025).

SentinelOne. (2021) 'What is a threat actor? Types & examples'. Available at: https://www.sentinelone.com/blog/what-is-a-threat-actor-types-examples (Accessed: 4 March 2025).

Snyder, S. (2023) 'Most common types & sources of cyber threats'. Available at: https://www.secureworks.com/blog/most-common-types-sources-of-cyber-threats (Accessed: 9 March 2025).

World Economic Forum. (2025) 'Global Cybersecurity Outlook 2025'. Available at: WEF_Global_Cybersecurity_Outlook_2025.pdf (Accessed: 9 March 2025).