STRATEGIC CONSIDERATIONS FOR AI-ENHANCED CYBERCRIME

Introduction

The AI reveals innumerable options to malicious actors. It is so efficient in a number of activities, that even state-sponsored hacker groups are exploring its capabilities. The automation of malicious actions through AI brought fundamental transformation of cybercrime. With its implementation, specialized tools for targeted malicious activities have emerged with striking speed. Phishing and social engineering are among the most proliferated cybercrimes. Moreover, due to AI, the threshold for committing sophisticated malicious actions is almost non-existent. In addition, the cyberspace provides possibility for global reach and supplementary tools render the language barrier obsolete[1]. The contemporary attacks are committed with unprecedented scale and intensity as the criminal networks transform into financially oriented conglomerates with a geopolitical role and growing influence. Criminal operations in cyberspace are already becoming a routine and efficient activity, difficult to intercept and mitigate. Malicious codes, written by AI, have already been detected in various cybercrimes.

Illegal markets for sophisticated malicious tools are easy to find on the Dark Net, where multi-vector attacking malware could be purchased with cryptocurrency. The utilization of AI by cybercriminals makes the symbiosis between phishing and deepfakes an extremely dangerous phenomenon, which already claimed victims of specialized extortion. The listed circumstances, although far from exhaustive, testify the end of the single isolated cyberattacks. Through AI, they are transformed into continuous campaigns with perpetrators and their goals hard to determine. Nation-states with enormous financial and technological resources often hide themselves among the vast quantity of cybercrimes. As AI offers malicious actors speed, adaptability and a huge choice of tools, new tactics and techniques for compromising systems are on the rise too.

Methodology

[1] Syed, S. A. (2022). Ai-powered cybercrime: the new frontier of digital threats. International Journal of Engineering Technology Research & Management (IJETRM), 6(02).

This study uses a comprehensive interdisciplinary approach that combines analytical, systemic and prognostic methods. The analytical method examines the main features of AI-enhanced cybercrime, including its technological, economic and strategic aspects. The systemic approach analyzes cybercrime as a part of a broader socio-technical environment, where technologies, public institutions, legal norms and behavioral patterns interact dynamically. The prognostic method helps identify emerging trends and future risks caused by the automation, autonomy, and economic rationalization of malicious cyber activities. Additionally, a comparative analysis of current academic research and doctrinal viewpoints is conducted to identify recurring patterns and strategic weaknesses in existing cybersecurity and public governance frameworks.

Discussion

The efficiency of AI in gathering and processing information from open sources, such as social networks and profiles on various platforms, pushes personalized attacks to their peak. There is no shortage of evidence of AI written scripts utilized to gain unauthorized access to networks. Together with the aforementioned, trust and authority are exploited through AI generated deep fakes as synthetic immoral content floods cyberspace to create more uncertainty and spread disinformation. The formation of autonomous networks, consisted of AI agents capable of planning and carrying out cybercrimes by themselves, already have all necessary prerequisites[2]. Compromised devices could be guided by AI to initiate DDoS attacks as well, despite existing technical limitations that are surmountable for entities with the necessary resources. Amidst all the risks, state actors are exploring the possible use of AI to make their shadow operations even more efficient at lower cost.

AI is proving to be an extremely versatile technology that can be compiled with others to bring about unexpected results. The massive integration of AI with multiple types of devices and hardware means increased security risks too. Thus, AI sets a new criterion for the nature of malicious actions, enabling a technological ecosystem in which pretrained models adapt their actions independently with time. AI also erases the divide between human action and machine execution. Hacking activity, earlier a skill of a small number of tech savvy individuals, has now been irrevocably democratized with AI, saturating cyberspace with anonymous entities capable of operating on an unrestrained time frame. The perception of

[2] Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36-51). IGI Global.

longevity of the attacks has changed, as malicious activity has become a constant and is maintained by self-adaptive agents. The result is the emergence of an ecosystem of permanent threat, in which machines interact with each other, seek vulnerabilities and transform to avoid detection[3].

The relative balance of power between attackers and defenders has also been altered, due to the existence of ethical and legal restrictions for the defenders[4]. These asymmetric dynamics strongly favor malicious actors, who always find themselves with an advantage due to lack of restraint. However, the traditional understanding of cybersecurity is yet unable to offer adequate solutions to automated threats. AI is already more of a technology that has been utilized predominantly as an amplifier for strategic influence. As AI development gains traction, it spurs a new generation of cybercrime, which does not simply commit malicious activities, but constitutes a systemic and integrative function of the technological environment.

It is undeniable that AI automatically multiplies the number of attacks, but it also provokes a systemic change in the construction of cyberspace itself. Its development stretches beyond a collection of technical infrastructure and software to evolve into a habitat of algorithms and agents with ability to interact in real time. The loss of predictability is among the main properties of the transformed cyberspace under the influence of AI. To be efficient, defenders previously relied on historical models in and archives for attack detection in less dynamic environments, but with the evolution of AI, this logic became irrelevant, because each attack could be unique. This brings cyberchaos that hampers the static nature of the technical infrastructure, rendering the adaptability of organizations a matter of survival[5].

The systemic change could also be detected in the communication channels, due to the growing volume of synthetic content, created by AI. The quality and value of information are threatened by the petabytes of synthetic noise generated daily and spread through algorithms. This phenomenon actually affects the cognitive ability of societies and worsens their ability to distinguish between facts and fiction. The entities who control ecosystems with AI models in their center accumulate a tremendous power in the AI race between states,

[3] Mijwil, M. M., Aljanabi, M., & ChatGPT, C. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. *Iraqi Journal For Computer Science and Mathematics*, *4*(1), 8.

[4] Volodymyr, Z., Valery, B., Borys, K., Volodymyr, S., Oleksiy, O., & Yehor, P. T. (2025). ARTIFICIAL INTELLIGENCE AND CYBERCRIME: NEW CHALLENGES AND PROSPECTS FOR LEGAL REGULATION. Contemporary Issues in Artificial Intelligence, 1.

[5] Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. In *Journal of Physics: Conference Series* (Vol. 1533, No. 3, p. 032014). IOP Publishing.

criminal networks and corporations. The aim of gaining a strategic advantage in the aforementioned context fragments cyberspace and stirs harsher competition in the now permanent race for control of information and the access to it. Influenced by these circumstances, contemporary cybersecurity can no longer be determined by static protocols as it is rapidly transformed into activity of critical balance between human factor, technology and information flow, where any change brings consequences to the other parts of a system. In this context, AI represents an evolutionary stepping stone in the development of cyberspace which is headed towards increasingly independent dynamics.

AI opens up a plethora of new tactics, tools, and operational techniques for hackers, but more than that, it is redefining the economic logic of malicious actions as the main drive behind cybercrime. Isolated independent crimes are now a rare occurrence due to the emerging cybercrime economy, in which information, AI models, and algorithms are treated as tradeable assets. The observed shift is an indicator for the transformation of cybercrime and its evolution from a multilayered network of independent players to quasi-corporate grid with shared connections and infrastructure for tool exchange[6]. The existing Cybercrime-as-a-Service (CaaS) model is mutating into a new automated form known as AIaaS, in which criminal groups offer paid access to models trained for criminal purposes. The provision of models for phishing, malware creation, and biometric spoofing in the form of monthly subscription with updates and technical support, points out that cybercrime has entered a stage of economic rationalization favoring an adaptive supply chain that focuses on demand and profitability.

A concerning trend is the lack of a clear strategy for intercepting and deterring attacks enhanced by AI. There is also no clear mechanism between nation states for mutual deterrence in the usage of AI, similar to the nuclear deterrence. There is a lack of guarantees for the security of critical infrastructure attacked by AI and autonomous agents. The ability of AI to generate massive amounts of disinformation concerns the governments as it is a powerful tool for destabilization of social order[7]. The race to develop AI, which is already considered an imperative for technological supremacy, has been compared to the nuclear arms race from the last century. The AI competition between the United States, China and Russia has now moved beyond physical and geographical dimensions and has been

[6] Hussain, M., & Soomro, T. R. (2024, December). AI-Powered Cybercrime: A Survey on Emerging Threats, Tools & Techniques for Countermeasures. In 2024 26th International Multi-Topic Conference (INMIC) (pp. 1-6). IEEE.

[7] Kamat, P., & Gautam, A. S. (2018). Recent trends in the era of cybercrime and the measures to control them. In Handbook of e-business security (pp. 243-258). Auerbach Publications.

transformed in a strife for control over the cognitive resilience of societies. AI is emerging as a factor influencing the global hierarchical order and a catalyst for systemic uncertainty, increasing the asymmetry in power relations between key players.

AI also erodes the foundations of knowledge and trust. Information entropy is gaining momentum with the vast volumes of synthetic content, which makes the distinction between authentic and fake almost an impossible task. In such an environment, cybersecurity ceases to be a solely technical discipline and evolves into an active struggle to preserve social order based on cognitive perception. The frequent hallucinations of AI are a threat by themselves, but in combination with targeted efforts for fake news creation, the objective truth becomes a target to malicious actors. Through its various products like deep fakes, synthetic personalities, and disinformation, the perception of reality is substituted by a firm trust in conspiracy theories and plausible-sounding untruths[8].

The state of cognitive chaos has consequences that fuel public skepticism and destabilize democratic institutions that rely on informed decision-making by citizens. The changed nature of communication leads to a large number of people conversing with chatbots without realization, thus creating new vulnerabilities because of increased dependence on algorithmic intermediaries in the search for knowledge and facts. Information ceases to be factually sound and instead becomes a mixed narrative, often in the service of political and economic interests. Such an information environment is extremely beneficial for cybercriminals, who manipulate perceptions to provoke public behavior in their interest. Thus, the concept of cybersecurity must evolve to successfully protect the cognitive integrity of societies.

Conclusion

The discussion so far points out several strategic considerations for AI-enhanced cybercrime. The first is that AI acts as a catalyst. It can accelerate a seemingly isolated malicious action into a global phenomenon, capable of functioning without human intervention. This property makes attacks cheap, fast and limitless. The second consideration is that AI easily automates malicious actions. Cybercrime is on the verge of systematizing a self-sustaining structure that cannot be eliminated, but only managed as a source of risk.

[8] Channapattan, V., Baram, G., Wiebe, N., & Niedzialkowski, T. C. (2025, May). AI, Cybercrime, and Society: Closing the Gap Between Threats and Defenses. In *2025 IEEE Conference on Artificial Intelligence (CAI)* (pp. 1316-1317). IEEE.

Third, cybercrime creates an independent underground market in which AI is a commodity, a service and a broker at the same time. Fourth, the merger of multiple entities with AI gives rise to a new form of confrontation called “cognitive warfare”. This is not a warfare for territory or resources, but for human perception and the interpretation of incessant information stimuli. Fifth, the resilience of cyberspace can be fostered through technological progress aligned with ethical and regulatory frameworks as a necessary addition to AI development. If not achieved, the negative processes would irreversibly go out of control. Sixth consideration proclaims that AI is a neutral technology, which can be used for both cybercrime and prevention, but the criminals have an advantage due to the lack of moral and legal restraints. Finally, we are witnessing the end of the classical understanding for cybersecurity, which must evolve to respond adequately to the risks posed by autonomous and self-learning threats with possible strategic implications.

BIBLIOGRAPHY

1. Channapattan, V., Baram, G., Wiebe, N., & Niedzialkowski, T. C. (2025, May). AI, Cybercrime, and Society: Closing the Gap Between Threats and Defenses. In 2025 IEEE Conference on Artificial Intelligence (CAI) (pp. 1316-1317). IEEE.
2. Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36-51). IGI Global.
3. Hussain, M., & Soomro, T. R. (2024, December). AI-Powered Cybercrime: A Survey on Emerging Threats, Tools & Techniques for Countermeasures. In 2024 26th International Multi-Topic Conference (INMIC) (pp. 1-6). IEEE.
4. Kamat, P., & Gautam, A. S. (2018). Recent trends in the era of cybercrime and the measures to control them. In Handbook of e-business security (pp. 243-258). Auerbach Publications.
5. Mijwil, M. M., Aljanabi, M., & ChatGPT, C. (2023). Towards artificial intelligence-based cybersecurity: The practices and ChatGPT generated ways to combat cybercrime. Iraqi Journal For Computer Science and Mathematics, 4(1), 8.
6. Syed, S. A. (2022). Ai-powered cybercrime: the new frontier of digital threats. International Journal of Engineering Technology Research & Management (IJETRM), 6(02).
7. Volodymyr, Z., Valery, B., Borys, K., Volodymyr, S., Oleksiy, O., & Yehor, P. T. (2025). ARTIFICIAL INTELLIGENCE AND CYBERCRIME: NEW CHALLENGES AND PROSPECTS FOR LEGAL REGULATION. *Contemporary Issues in Artificial Intelligence*, *1*.
8. Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. In *Journal of Physics: Conference Series* (Vol. 1533, No. 3, p. 032014). IOP Publishing.

СТРАТЕГИЧЕСКИ СЪОБРАЖЕНИЯ СПРЯМО КИБЕРПРЕСТЪПЛЕНИЯ, ИЗВЪРШВАНИ С ИЗКУСТВЕН ИНТЕЛЕКТ

Гл. ас. д-р Владимир Бабанов

Катедра „Национална сигурност и публична администрация“

Правно-исторически факултет

Югозападен университет „Неофит Рилски“, Благоевград

v.babanov@law.swu.bg

Резюме: *Статията цели да подчертае някои способи, чрез които киберпрестъпниците използват изкуствения интелект (ИИ) за извършване на киберпрестъпления. Ефектите на ИИ върху киберпрестъпността е също основен фокус, наравно с причините за бързото разпространение на моделите на ИИ в киберпространството. Резултатът от подобно сливане на технологии, криминални интереси и икономически мотиви е невъзможно да бъде предвиден, но обмислянето на основни съображения спрямо киберпрестъпността, подсилена от ИИ, би могло да послужи като важна отправна точка за последващи дискусии.*

Ключови думи: *изкуствен интелект; киберсигурност; киберпрестъпност; автоматизация; зловреден софтуер;*

Chief Assist. Prof. Vladimir Babanov, Ph.D.

Department of “National Security and Public Administration”

Faculty of Law and History

South-West University “Neofit Rilski”- Blagoevgrad

v.babanov@law.swu.bg

Summary: *The current paper aims to outline some of the ways cybercriminals utilize Artificial Intelligence (AI) for malicious actions perpetration. The effects of AI on cybercrime are also a main focus together with the reasons behind the rapid proliferation of AI models. The outcome of such a merger between technology, criminal interests and economic incentive is impossible to predict, but entertaining several considerations for AI-enhanced cybercrime might provide valuable starting points for subsequent discussions.*

Keywords: *artificial intelligence; cybercrime; cybersecurity; automation; malware;*