HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 39–51.
DOI: 10.32567/hm.2025.4.3

Zoltán Kovács[1]

The Use of Artificial Intelligence in Cyberattacks, Part 1

Fundamental Concepts of Artificial Intelligence and the Cyber Kill Chain Model

Abstract

The rapid advancement of artificial intelligence (AI) technology has fundamentally transformed the field of cybersecurity, impacting both defensive and offensive capabilities. This series of articles analyses the malicious applications of artificial intelligence in cyberattacks, structured around the Cyber Kill Chain model. It details how AI can increase the effectiveness, automation and stealth of attacks in all phases of cyberattacks described by the Cyber Kill Chain model, from reconnaissance to actions on objectives. The aim of this series of articles is to provide a comprehensive overview of current threats and to highlight the importance of further research and proactive defence strategies. This article, the first in the series, covers the definitions of AI and the Cyber Kill Chain model to the extent necessary for understanding.

Keywords: artificial intelligence, cybersecurity, cyberattack, Cyber Kill Chain, machine learning, deep learning, phishing, malware

Introduction

In the current phase of the information society, where digital transformation permeates everything and global reliance on digital infrastructure is continuously increasing, the associated risks are also on the rise. Indeed, the vulnerability of information and communication networks and systems has reached unprecedented levels. At the same time, artificial intelligence (hereinafter: AI) has undergone explosive development,

[1] Senior Lecturer, Ludovika University of Public Service, e-mail: zkovacs.24@gmail.com

enabling machines to perform tasks similar to human intelligence, such as data analysis, pattern recognition, decision-making, and automation.[2] AI has now developed to the point where it is widely applied on a daily basis in areas such as cybersecurity, healthcare, manufacturing, education and financial modelling, but as a personal assistant, it is also assisting the work of an increasing number of companies worldwide in all areas of life.

However, in addition to areas that can now be considered classic, AI is also appearing in a completely different area, the so-called metaverse, where it plays a prominent role. The metaverse is a global virtual ecosystem born from the convergence of physical, augmented and virtual spaces connected by the internet, virtual reality (VR), and augmented reality (AR), where people (and companies) can communicate openly with each other. Increasingly advanced AI, especially in relation to AI-driven avatars that enable human-like interaction, is an essential part of the Metaverse. On the one hand, without increasingly advanced AI, there would be no Metaverse, as it is essential for handling vast amounts of complex data and creating dynamic, interactive environments. On the other hand, the Metaverse itself has a significant impact on the development of AI, as its complexity allows the AI models used to be trained for a wide variety of highly diverse tasks.[3] However, the emergence of AI in cybersecurity is a double-edged sword. On the one hand, it assists defensive personnel by offering significant potential for strengthening cyber defence systems and automated threat detection, On the other hand, however, it also provides malicious actors with an extremely effective tool for executing sophisticated, adaptive and difficult-to-detect cyberattacks.[4] This dual nature results in a spiral-like, constantly escalating *AI arms race* in the field of cybersecurity. As attackers utilise increasingly sophisticated AI-based tools, defenders must rely on increasingly advanced AI-based detection and incident response solutions to operate effectively, which in turn generates a rapid innovation cycle on both sides. This phenomenon is not only of operational technological significance, but also of strategic importance, as superiority in AI capabilities in cyber warfare can fundamentally influence national security and the protection of critical infrastructure.[5] State-sponsored actors, whether on the defensive or offensive side, are expected to invest significant resources in the development of AI-based cyber weapons in the near future, which will enable them to carry out targeted, large-scale and covert attacks with much greater efficiency than they currently can against any selected target, including critical infrastructure.

This series of articles examines the offensive applications of artificial intelligence during cyberattacks along the lines of the Cyber Kill Chain (hereinafter: CKC) model developed by Lockheed Martin, which is now considered as an industry standard. The CKC is a strategic framework developed by Lockheed Martin to describe the phases of cyberattacks, thereby facilitating the focused application of cyber defence mechanisms during different stages of attacks.[6] Although this series of articles pro-

[2] Jordan–Mitchell 2015.
[3] Wolfenstein 2023; Team Antier 2022.
[4] Abbadi–Lachkar 2024.
[5] Erdész 2023; Mattioli et al. 2023.
[6] Microsoft [s. a.b].

vides a brief overview of CKC and the basic definitions of AI, it is not intended to be a detailed presentation of the CKC model and artificial intelligence. These and related concepts are explained only to the extent necessary for understanding the content. The primary goal of this series of articles is to provide a comprehensive overview of how AI can significantly increase the effectiveness of attackers in certain phases of cyberattacks, outline the rapidly evolving threat landscape associated with this, and, in addition, make recommendations for further research directions.

Basic concepts of artificial intelligence and the Cyber Kill Chain model

In order for this series of articles to achieve its goal, namely, to demonstrate the means and methods attackers use to utilise AI in cyberattacks, it is first necessary to review the basic terms of artificial intelligence and examine why the Cyber Kill Chain model is appropriate as a basis for this examination.

The most important basic concepts of artificial intelligence

John McCarty Professor Emeritus at Stanford University, defined artificial intelligence as follows:

"It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."[7]

According to Hungary's Artificial Intelligence Strategy 2020–2030, "Artificial intelligence (AI) […] is the totality of algorithmic systems capable of teaching and improving themselves based on the data fed into them".[8] Hungary's Artificial Intelligence Strategy (2025–2030), which was published on 3 September 2025 as a revision of the previous strategy, states the following:

"Artificial intelligence (AI) has now moved beyond being merely a collection of algorithmic systems that teach and improve themselves based on data. AI is increasingly capable of simulating human understanding, learning, and problem-solving, as well as mapping and enhancing the efficiency of certain segments of human capabilities. The mapping of human capabilities by 'learning machines' is leading to significant efficiency gains in economic, administrative, and private life processes, while also creating new revenue opportunities."[9]

At the same time, artificial intelligence is essentially an interdisciplinary field of science that deals with the ability of computer systems to perform tasks that require human

[7] McCarthy 2007.
[8] *Hungary's Artificial Intelligence Strategy 2020–2030* 2020.
[9] *Magyarország Mesterséges Intelligencia Stratégiája (2025–2030)* 2025.

intelligence. For the purposes of this series of articles, the following AI subfields are particularly relevant in the context of cyberattacks:

- *Machine Learning* (hereinafter: ML): A subset of AI, ML is the branch of AI that develops algorithms and statistical models that enable information and communication systems to learn and improve from input or incoming data without being specifically programming for this purpose. ML algorithms are capable of recognising patterns in data, making predictions, and taking decisions. In cyberattacks, ML is frequently used for data collection, target identification and adaptation of malicious code.
- *Deep Learning* (hereinafter: DL): Deep learning is a specialised, more sophisticated form of machine learning in which AI systems process complex data structures using multi-layered neural networks that emulate the neural pathways of the human brain. Deep learning uses artificial neural networks with many so-called hidden layers to recognise complex patterns and generalities in vast amounts of data. DL is particularly effective at analysing unstructured data (such as images, text and sound) and generating accurate information and predictions from them, which can be crucial in areas such as advanced phishing and the creation of generative malware.
- *Reinforcement Learning* (hereinafter: RL): An approach to machine learning in which a software *agent* learns how to behave based on feedback in the form of rewards and penalties during its interactions in a given environment. The goal of learning is for the *agent* to maximise long-term rewards. This type of approach may be ideal for developing autonomous attack systems that are capable of independently identifying and performing reconnaissance on targets, making decisions and executing attacks, while continuously adapting to the target system's responses.
- *Natural Language Processing* (hereinafter: NLP): The area of AI that deals with interaction between computers and human (natural) language. The capabilities of NLP, particularly through the latest Large Language Models (hereinafter: LLMs), play a key role in generating convincing phishing messages, fraudulent emails, and deepfake content, which significantly increase the effectiveness of social engineering attacks.
- *Generative Artificial Intelligence* (hereinafter: Generative AI): Generative AI is a form of deep learning, a branch of AI that can create new, original data (such as text, images, sound, code) based on patterns learned from training data. Generative AI models, such as Large Language Models (LLMs), are capable of performing complex tasks including answering questions, generating images from text, writing complex texts and generating content. This group also includes, for example, Generative Adversarial Networks (hereinafter: GANs), where two neural networks are operated in competition with each other in order to generate more authentic new data from a given training data set, as well as language models based on transformer architecture, where words are processed in parallel and independently of each other rather than sequentially.

> With the help of these technologies, attackers can create realistic fake content, adaptive malware variants and personalised attack scripts.[10]

The evolution from machine learning through deep learning further to generative AI and advanced NLP represents an increasing sophistication of AI moving from analytical to creative capabilities. However, this shift fundamentally influences the cyber threat landscape, as it enables attackers to create novel, adaptive, and highly effective malicious code, such as polymorphic malware or even deepfakes for social engineering attacks. Table 1 below summarises the relevance of AI sub-sectors in cyberattacks.

Table 1: Relevance of artificial intelligence sub-sectors in cyberattacks

AI sub-sector	Brief definition	Offensive application mode
Machine learning (ML)	Algorithms and statistical models that enable systems to learn and improve from data	Data collection, target identification, adaptation of malicious code
Deep learning (DL	A specialised form of machine learning that uses artificial neural networks to recognise complex patterns in vast amounts of data	Analysis of unstructured data (image, text, audio), advanced phishing, creation of generative malware
Reinforcement learning (RL)	A software 'agent' that learns behaviour in a given environment based on feedback through rewards and penalties	Development of autonomous attack systems, independent target reconnaissance, attack execution, adaptation
Natural language processing (NLP)	The area of AI that deals with the interaction between computers and human language	Generation of convincing phishing messages, fraudulent emails, deepfake content, increasing the effectiveness of social engineering attacks
Generative artificial intelligence (Generative AI)	A branch of AI capable of creating new, original data (text, image, audio, code) based on patterns learned from the training data	Creation of realistic fake content, adaptive malware variants, personalised attack scripts

Source: compiled by the author based on Usman et al. 2024; AWS [s. a.]; Badman–Kosinski [s. a.]; Microsoft [s. a.a]

Introduction to the Cyber Kill Chain framework

Various organisations and companies have developed several types of frameworks for identifying and managing cyberattacks more effectively. Different threat models employ different approaches to representing detected attackers, as well as their behaviour and tools. Some models, such as Lockheed Martin's Cyber Kill Chain and Microsoft's STRIDE, represent a high level of abstraction and summarise the multiple and complex steps taken by an attacker into a short list of steps. Other models, such as MITRE CVE, take

[10] Usman et al. 2024; AWS [s. a.]; Badman–Kosinski [s. a.]; Microsoft [s. a.a].

a low-level approach and typically detail very specific items, such as detailed system vulnerabilities and their exploitation. Mid-level abstraction models (such as MITRE ATT&CK, CAPEC, FiGHT) are typically positioned between the two, describing the individual steps of an attack, the attack techniques and technologies used therein, and integrating them into a unified framework.[11]

These models often build upon each other and assist the work of cyber defence professionals at different levels. Figure 1 below illustrates the hierarchy of the Cyber Kill Chain model (developed by Lockheed Martin, which treats cyberattacks as a high-level model), MITRE's Att&ck model (which treats cyberattacks as a mid-level model), and models that treat cyberattacks as a low-level model (e.g. CVE).

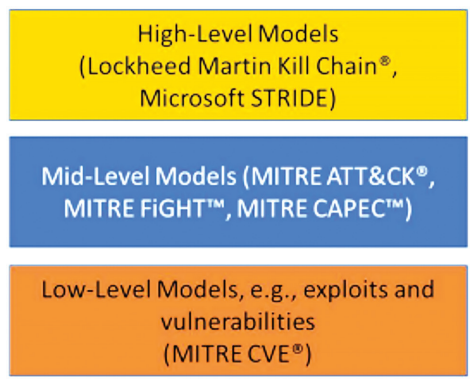

Figure 1: Abstraction layers of cyber defence frameworks
Source: Radle et al. 2023

Definition and purpose of the Cyber Kill Chain

The Cyber Kill Chain is a high-level cybersecurity framework developed by Lockheed Martin, which has now become one of the fundamental frameworks of cybersecurity. The model's purpose is to assist cybersecurity professionals in understanding the progress of cyberattacks, identifying potential points of detection for an attack, and thereby developing defence strategies. The Cyber Kill Chain framework is part of the Intelligence Driven Defense model,[12] also created by Lockheed Martin, which is used for identifying and preventing cyberattacks and helps to understand the steps opponents need to take to achieve their goals.

The Cyber Kill Chain describes the complete lifecycle of a cyberattack, breaking it down into separate, sequential phases.[13] The primary goal of developing CKC was to provide a structured approach for understanding and analysing cyberattacks and,

[11] Radle et al. 2023.
[12] The philosophy behind Lockheed Martin's Intelligence Driven Defense is to stop offensive manoeuvres during cyberattacks while maintaining a defensive position. Every defensive action and every offensive manoeuvre launched is guided by human intelligence gathering.
[13] Radle et al. 2023.

ultimately, to assist in preventing and disrupting them. By recognising the typical steps of cyberattacks, organisations can improve their resilience thereby enhancing their threat detection and response capabilities, identify vulnerabilities in their systems in a more structured manner, strengthen their defences, and proactively mitigate their cybersecurity risks, rather than merely reacting to recognised, successful attacks.[14]

As a result, CKC has become indispensable for cybersecurity professionals in establishing and maintaining effective defences, conducting cybersecurity operations, responding to incidents, and in the cyber threat intelligence.[15]

Despite the above advantages and widespread adoption, CKC faces several challenges. Although understanding the cyberattack chain can help companies and governments proactively prepare for and respond to even complex, multi-stage cyber threats, relying solely on this can leave an organisation vulnerable to other types of cyberattacks. Several disadvantages are often cited in relation to CKC, such as:

- Focuses on malware: The original cyber kill chain framework was designed to detect and respond to malware and is not as effective against other types of attacks, such as unauthorised access gained with stolen credentials.
- Ideal for perimeter security mostly: The CKC model was well adapted when the emphasis was on protecting endpoints and only a single or a small number of network perimeter areas needed to be protected. Today, with the rise in the number of remote or home workers, the significant increase in the use of cloud-based systems, and the surge in the number of devices that remotely access corporate assets, it is nearly impossible to manage all endpoint vulnerabilities, especially with this approach.
- It is not prepared for internal threats: Malicious internal employees or external partners who already have access to certain systems are difficult to detect with defences based on the CKC model. Instead, organisations need to monitor and detect changes in user activity (as well).
- Too linear: Although many cyberattacks correspond to the attack methodology described in the CKC (and presented below), which consists of seven (+ n) steps, there are also many attacks that do not follow this methodology or combine several steps into a single operation. Organisations that focus too narrowly on specific stages of the CKC may fail to detect cyber threats that use a different attack methodology.

In addition to all this, or despite it, it can be concluded that the CKC model is an appropriate choice for examining the chosen topic of AI use in cyberattacks and cyber defence. The attack and defence capabilities and options analysed using CKC provide a comprehensive picture of AI use on both the offensive and defensive sides.

[14] Microsoft [s. a.b].
[15] Goss 2024.

The seven (+ n) phases of the Cyber Kill Chain

The CKC framework consists of seven sequential main phases, each of which is an essential step in achieving the attacker's goals. These phases are illustrated in Figure 2 and described briefly thereafter. This series of articles does not aim to provide a detailed description of CKC, so the following description is a simplified summary of the essentials necessary for understanding.

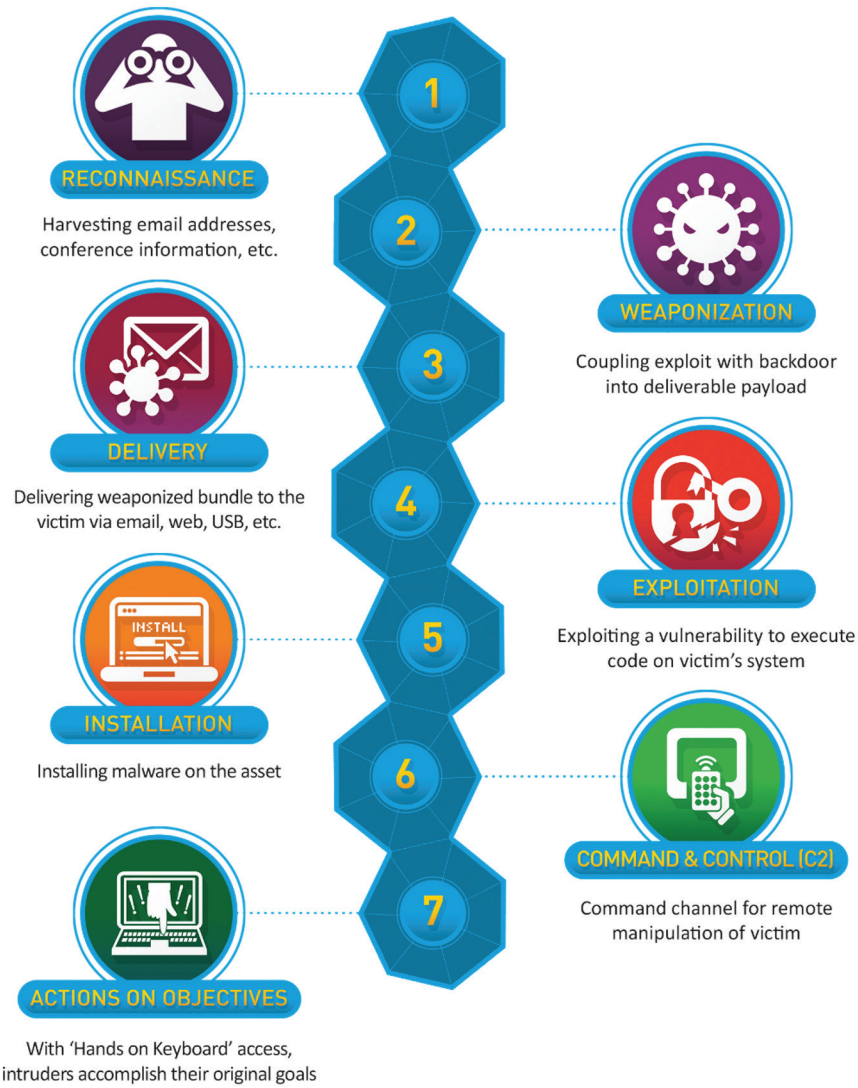

Figure 2: Phases of the Cyber Kill Chain
Source: The Cyber Kill Chain® s. a.

Reconnaissance: At this point, attackers gather information about the target, such as network structure, employees of selected companies and security technologies used for protection. In more detail, this phase includes searching for, identifying and selecting targets, followed by gathering information about the selected targets, such as finding vulnerabilities, identifying third parties connected to the target's systems, and determining what data the attackers can access. Reconnaissance can be carried out both online and offline, typically using OSINT[16] methods, which often involve mapping websites, conference publications, mailing lists, email addresses, social connections or information about specific technologies.

Weaponization: After the attacker has gathered all the necessary information about potential targets, the next step is to create or obtain malicious code or other harmful content to be delivered to the target. For example, attackers compile code that exploits a vulnerability (exploit[17]) and malicious software (payload), then package them into a format that can be delivered to the target (e.g. PDF, Word document, executable file). This can be done by modifying existing malicious attack codes or creating new types of malicious codes. An example of weaponization is combining a remote access Trojan with an exploit and integrating them into some kind of carrier (e.g. the aforementioned Adobe Portable Document Format (PDF) or Microsoft Office documents), or making minor modifications to an existing ransomware variant, etc.

Delivery: In this phase, the attackers deliver the prepared *cyber weapon* to the target. Forms of delivery include, for example, email attachments, infected websites, USB data storage devices, and exploiting vulnerabilities in the target organisation's information and communication systems.

Exploitation: In this phase of the CKC, attackers activate the exploitable vulnerability to exploit the vulnerability of the target system, thereby gaining access to certain elements of the target system. They then move further (e.g. laterally) across the network in an attempt to reach their intended targets.

Installation: During this phase, attackers attempt to install malicious software and/or other cyber weapons on the target network in order to take control of the systems and send valuable data from them. They may use Trojan programs, backdoors or command line interfaces for installation.

Command and Control (C2): At this stage of the attack, the attackers establish a communication channel with the compromised system and use it to remotely control the installed malicious software, sending instructions to it in order to achieve their attack objectives. Such objectives may include, for example, controlling botnets to carry out a Distributed Denial of Service (hereinafter: DDoS[18]) attack against a selected target, or forwarding confidential company documents to the attackers, etc. If

[16] OSINT: Open Source Intelligence, refers to the collection and analysis of publicly available data.

[17] Exploit: exploiting a vulnerability in software or hardware, allowing an attacker to cause unexpected behaviour in the system, such as gaining administrator privileges or causing denial of service.

[18] Distributed Denial of Service (DDoS): This is a malicious attack aimed at completely or partially paralyzing an IT service and preventing it from functioning properly. In the process, attackers flood the server with data traffic of a certain type and volume from multiple sources (in a distributed manner) to the extent that it disrupts its normal operation.

necessary, attackers can also use this channel to install new malicious code or add new modules to the attack tools that have already been installed.

Actions on Objectives: After the attackers have successfully completed the previous phases, i.e. developed the cyber weapons, installed them on the target network, and taken control of the target network, they begin the final phase of the cyberattack: executing the actual objectives of the cyberattack. In other words, this phase is when the attacker achieves their ultimate goal, e.g. involving infected machines in a DDoS attack, stealing information, modifying or destroying data, causing system malfunctions, spreading malicious code, running ransomware, etc.[19]

In recent years, several individuals have been attempting to further develop the CKC framework in various ways, primarily with the aim of eliminating the disadvantages listed above. As a result, many new versions have been created, two of which are worth highlighting here.

One is that the original CKC model has been supplemented with an eighth, so-called monetisation phase, the content of which is as follows:

- Monetization: The step following Lockhead Martin's original CKC phases, which refers to the activities carried out by attackers to generate revenue from the attack, such as using ransomware to extort money from victims or selling sensitive data on the dark web.20

The other is when maintaining the presence of the attack and lateral movements are treated in separate phases (in a loop). Mandiant's attack lifecycle model is presented in Figure 3 below.

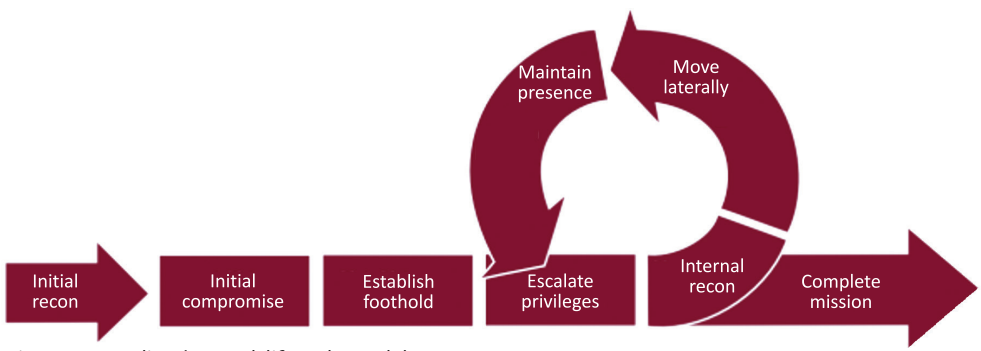

Figure 3: Mandiant's attack lifecycle model
Source: Velazquez 2015: 16

These additional phases – while significant in their own right and useful as supplements in certain attacks – are not necessary for examining the topic of this series of articles, namely the use of artificial intelligence in cyberattacks. The original CKC model is a reasonable choice for this purpose, as the attack options and solutions

[19] Microsoft [s. a.b]; Kidd 2024; Goss 2024.
[20] Microsoft [s. a.b].

analysed along the original 7-phase CKC can provide a comprehensive picture of the use of AI on the attacking side.

Based on the analysis described above, it can be concluded that the Cyber Kill Chain is not merely a list of separate or isolated attack activities, but rather a description of a progressive, interconnected series of attack events. The basic assumption of the CKC framework is that an attack must typically complete each phase sequentially, meaning that each phase or step depends on the success of the previous one, and its success lays the foundation for the feasibility of the next phase.[21] This chained sequential dependency is the fundamental logic behind the CKC concept. However, this also means that interrupting or disrupting the attack chain at any point can prevent the entire attack from being successful, i.e. prevent the attacker from achieving their objectives. This creates an opportunity for cybersecurity professionals to implement multi-layered security measures for the systems they protect, allowing attacks to be detected and neutralised at multiple levels and points. In other words, even if an attacker successfully bypasses certain defensive elements/measures, other tools and defensive methods can detect and interrupt the attack in its next phase. This increases the likelihood of preventing successful attacks.

The CKC framework aims to improve threat detection and response capabilities by identifying the different stages of a cyberattack and enabling defenders to determine the potentially appropriate security measures and equipment that can be effectively used to detect or interrupt a cyberattack.[22] This goes far beyond a purely reactive approach to cyber defence (based on responding to unauthorised intrusions). CKC thus serves as a powerful proactive planning framework, not just a retrospective, post-mortem analysis tool. It helps cybersecurity professionals understand the mindset of attackers, anticipate their moves and deploy appropriate defences at all strategically possible points of attack. This paradigm shift from reactive incident response to proactive threat disruption is key to building resilient cybersecurity architectures. To this end, it is very helpful to examine which AI-supported attack methods and tools are used or can be used by attackers and at which stages of CKC, and which AI-supported defence solutions are used or can be used by defenders at which stages to counter them.

The Cyber Kill Chain model has a significant impact on cybersecurity. It provides cybersecurity professionals with an opportunity to understand how attackers plan and execute their attacks, thereby allowing them to more easily identify and effectively mitigate vulnerabilities in their systems and organisations, and helping them recognise signs of compromise early stages in a cyberattack. For this reason, many organisations use the Cyber Kill Chain model to proactively implement security measures and as a guideline for developing their incident response strategies. Although CKC was originally a defence framework, it is increasingly being used in threat hunting to predict attacker behaviour. By understanding how AI strengthens each phase of the attack chain, defenders can shift their focus from reactive defence to proactive threat hunting and preventive measures that significantly mitigate damage, concentrating

[21] Goss 2024; Pentera [s. a.].
[22] Microsoft [s. a.b]; Goss 2024.

their resources where AI-driven attacks are most likely to occur. This strategic shift moves the focus from merely detecting intrusions into one's own systems to predicting attacks, or at least detecting them early, thereby interrupting the entire attack chain at an early stage or effectively disrupting the various or all phases.

Conclusions

This series of articles deals with the use of artificial intelligence in cyberattacks. Nowadays, there are many scientific publications, reports written by cybersecurity experts, blog posts, etc. that discuss the use of AI in cyberattacks. However, these typically either discuss a specific type of attack in detail or present several such possibilities in a general form. In addition, only a few publications show AI-supported cyberattacks using the CKC, and those that do typically present only a few well-known forms, without attempting to provide detailed content summarising as many forms of attack as possible.

Based on the first part of the series of articles, it can be concluded that the Cyber Kill Chain model, despite all its limitations, is suitable for achieving the goal of the series of articles, i.e. it can be used to demonstrate how attackers can use AI in cyberattacks. This will provide a suitable basis for further research into where and how defenders will be able to detect and disrupt AI-assisted attacks, and what tools they will have at their disposal. However, this requires a comprehensive description that summarises the methods and tools available to attackers in each phase of the CKC.

The following parts of the series of articles will show the actual application possibilities of artificial intelligence in the various phases of the Cyber Kill Chain model on the offensive side and then describe the current challenges and trends arising on this side.

References

Abbadi, Driss – Lachkar, Abdelkader (2024): Cyber Threats in the Age of Artificial Intelligence. Exploiting Advanced Technologies and Strengthening Cybersecurity. *International Journal of Science and Research Archive,* 13(1), 2576–2588. Online: https://doi.org/10.30574/ijsra.2024.13.1.1961

AWS [s. a.]: What is Deep Learning in AI? *AWS,* s. a. Online: https://aws.amazon.com/what-is/deep-learning/

Badman, Annie – Kosinski, Matthew [s. a.]: What is AI security? *IBM/think*. Online: www.ibm.com/think/topics/ai-security

Erdész, Viktor (2023): *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben.* Budapest: Katonai Nemzetbiztonsági Szolgálat. Online: https://bit.ly/4tKmx65

Goss, Adam (2024): The Cyber Kill Chain: A Powerful Model For Analyzing Cyberattacks. *Kraven Security,* 11 March 2024. Online: https://kravensecurity.com/cyber-kill-chain/

Hungary's Artificial Intelligence Strategy 2020–2030 (2020). AI Coalition – Digital Success Programme – Ministry for Innovation and Technology. Online: https://mik.neum.hu/wp-content/uploads/2025/03/2020-hungarian-AI-strategy.pdf

Jordan, Michael I. – Mitchell, Tom M. (2015): Machine Learning: Trends, Perspectives, and Prospects. *Science,* 349(6245), 255–260. Online: https://doi.org/10.1126/science.aaa8415

Kidd, Chrissy (2024): Cyber Kill Chains: Strategies & Tactics. *Splunk,* 26 August 2024. Online: www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) [Hungary's Artificial Intelligence Strategy (2025–2030)] (2025). Online: https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf

Mattioli, Rossella et al. (2023): *Identifying Emerging Cybersecurity Threats and Challenges for 2030.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/117542

McCarthy, John (2007): *What is Artificial Intelligence?* Online: https://www-formal.stanford.edu/jmc/whatisai.pdf

Microsoft [s. a.a]: What is AI for Cybersecurity? *Microsoft Security,* s. a. Online: www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity

Microsoft [s. a.b]: What is the Cyber Kill Chain? *Microsoft Security,* s. a. Online: www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain

Pentera [s. a.]: Cyber Kill Chain. Glossary *Pentera,* s. a. Online: https://pentera.io/glossary/cyber-kill-chain-framework-explained/

Radle, Andrew J. et al. (2023): *MITRE FiGHT™: High-Level Overview. MITRE Five-G Hierarchy of Threats (FiGHT).* The MITRE Corporation. Online: https://fight.mitre.org/FiGHT_High-Level_Overview_PRS-23-2698.pdf

Team Antier (2022): DAO és Metaverzum: Egy kiváló kombináció és megoldás a holnap világa számára. *Antier Solutions*. 4 October 2022. Online: www.antiersolutions.com/hu/blogok/A-dao-%C3%A9s-a-metaverzum-egy-kiv%C3%A1l%C3%B3-kombin%C3%A1ci%C3%B3-%C3%A9s-megold%C3%A1s-a-holnap-vil%C3%A1ga-sz%C3%A1m%C3%A1ra/

The Cyber Kill Chain® [s. a.]. Lockheed Martin. Online: www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Usman, Yusuf – Upadhyay, Aadesh – Chataut, Robin – Gyawali, Prashnna K. (2024): *Is Generative AI the Next Tactical Cyber Weapon for Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks.* arXiv:2408.12806. Online: https://doi.org/10.48550/arXiv.2408.12806

Velazquez, Chris (2015): *Detecting and Preventing Attacks Earlier in the Kill Chain.* Global Information Assurance Certification Paper. The SANS Institute. Online: www.giac.org/paper/gsec/36774/detecting-preventing-attacks-earlier-kill-chain/145219

Wolfenstein, Konrad (2023): Mesterséges intelligencia vagy metaverzum? Mi a fontosabb? Vagy itt szinergiák alakulnak ki a további úttörő fejlesztések érdekében? *Xpert.Digital,* 28 December 2023. Online: https://xpert.digital/hu/ki-metaverzum/