Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

IMAGINARY ITERATION AND AI-DRIVEN RISK ANALYSIS: THE EMERGING CYBERSECURITY THREATS IN IOT-INTEGRATED SYSTEMS

AHMET EFE[1]

Gönderilme Tarihi: 24 Ocak 2025

Kabul Tarihi: 14 Temmuz 2025

Research Article / Araştırma Makalesi

ABSTRACT

This study explores the dual-use nature of artificial intelligence (AI) within cybersecurity, focusing on its transformative impact in Internet of Things (IoT)-integrated Management Information Systems (MIS). While AI enhances defense capabilities through advanced threat detection and rapid incident response, it simultaneously enables sophisticated, autonomous cyberattacks capable of circumventing traditional protections. Employing a novel imaginary iteration methodology, the research simulates AI-driven attack and defense scenarios to critically analyze emerging vulnerabilities and adaptive countermeasures. Special emphasis is placed on Türkiye's evolving cybersecurity ecosystem, highlighting institutional initiatives, strategic priorities, and governance challenges amid a complex balance between technological innovation and centralized digital control. The findings underscore the necessity of a hybrid security framework that integrates conventional defenses with AI-adaptive solutions, alongside a multi-stakeholder governance approach to ensure accountability, transparency, and resilience. Future research directions advocate for empirical validation of AI defenses, interdisciplinary analysis of ethical and legal dimensions, and focused evaluation of Türkiye's national AI-cybersecurity strategies to inform sustainable policy development in an increasingly contested digital landscape.

Keywords: *Artificial intelligence (AI), Cybersecurity, Internet of Things (IoT), Hacking, Cyber Risk Management*

[1] Doç.Dr., Senior Risk Management Officer, icsiacag@gmail.com, ORCID: 0000-0002-2691-7517

Bilgi Teknolojileri ve İletişim Dergisi (BTK DERGİ)
CİLT 3 SAYI 1 OCAK-HAZİRAN 2025 ISSN:2980-1331 E-ISSN: 3023-4239

HAYALİ İTERASYON VE YAPAY ZEKA TEMELLİ RİSK ANALİZİ: IOT ENTEGRE SİSTEMLERDE ORTAYA ÇIKAN SİBER GÜVENLİK TEHDİTLERİ

ÖZET

Bu çalışma, yapay zekânın (YZ) siber güvenlik alanındaki çift yönlü doğasını, özellikle Nesnelerin İnterneti (IoT) ile entegre Yönetim Bilgi Sistemleri (YBS) üzerindeki dönüştürücü etkisini incelemektedir. YZ, gelişmiş tehdit tespiti ve hızlı olay müdahalesi ile savunma kapasitesini artırırken; aynı zamanda geleneksel koruma mekanizmalarını aşabilen, sofistike ve otonom siber saldırılara da olanak tanımaktadır. Yenilikçi bir yöntem olarak hayali iterasyon (imaginary iteration) metodolojisi kullanılarak, YZ destekli saldırı ve savunma senaryoları simüle edilmekte; ortaya çıkan zafiyetler ve uyarlanabilir karşı önlemler detaylı şekilde analiz edilmektedir. Çalışmada, Türkiye'nin gelişmekte olan siber güvenlik ekosistemine özel vurgu yapılmakta; kurumsal girişimler, stratejik öncelikler ve teknolojik yenilik ile merkezileştirilmiş dijital kontrol arasındaki karmaşık dengenin yarattığı yönetişim zorlukları ele alınmaktadır. Bulgular, geleneksel savunma yaklaşımlarının YZ uyumlu çözümlerle harmanlandığı hibrit bir güvenlik çerçevesinin gerekliliğini ortaya koymakta; hesap verebilirlik, şeffaflık ve dayanıklılığı sağlamak üzere çok paydaşlı bir yönetişim modelinin önemini vurgulamaktadır. Gelecekteki araştırmalar için, YZ tabanlı savunma mekanizmalarının ampirik doğrulanması, etik ve hukuki boyutların disiplinlerarası olarak incelenmesi ile Türkiye'nin ulusal YZ-siber güvenlik stratejilerinin uygulama süreçlerinin detaylı değerlendirilmesi önerilmektedir. Bu yönelimler, giderek daha rekabetçi bir dijital ortamda sürdürülebilir politika geliştirme için temel oluşturacaktır.

Anahtar kelimeler: *Yapay Zekâ (YZ), Siber Güvenlik, Nesnelerin İnterneti (IoT), Hackleme, Siber Risk Yönetimi*

INTRODUCTION

The convergence of Artificial Intelligence (AI) with cybersecurity systems has engendered a profound transformation in both the offensive and defensive capacities of digital infrastructures. In particular, AI-driven mechanisms are increasingly embedded within Management Information Systems (MIS) and Internet of Things (IoT)-integrated environments. While AI enhances the speed, adaptability, and analytical precision of security responses, it also introduces a dual-use dilemma: the same algorithms that fortify systems can be weaponized to compromise them.

The IoT-defined as the ecosystem of interconnected devices capable of autonomous communication-has significantly broadened the cyberattack surface. The real-time data exchanges between consumer electronics, industrial sensors, and critical infrastructure systems expose vulnerabilities that can be identified and exploited at scale. When combined with superintelligent AI systems-those with superior autonomous learning and decision-making capabilities-the threat landscape becomes increasingly unpredictable and severe.

This study critically investigates emerging cybersecurity threats posed by AI tools that can be exploited for malicious hacking purposes, particularly within IoT-integrated MIS environments. The central problem addressed here is the growing capacity of AI to autonomously bypass conventional defense mechanisms, including firewalls, antivirus programs, and intrusion detection systems.

Concurrently, the research acknowledges the constructive use of AI in cybersecurity-particularly in enhancing anomaly detection, automating threat classification, and shortening incident response time. The duality of AI as both a shield and a weapon forms the foundation of the study's core inquiry. Within this framework, the research places specific emphasis on Türkiye's cybersecurity ecosystem, offering contextual insights and actionable policy recommendations.

1.1 METHODOLOGICAL APPROACH: IMAGINARY ITERATION

This study begins with an overview of AI-based tools and applies an innovative imaginary iteration methodology as both a heuristic device and an analytical framework. This method entails the creation of speculative, yet theoretically informed, scenarios involving AI-driven attack and defense agents, which are then visually represented through targeted image-based simulations to enhance conceptual understanding and analytical depth.

1.2 HYPOTHESES AND RESEARCH QUESTIONS

The research is grounded in three hypotheses:

1. AI exponentially increases the effectiveness and adaptability of cyberattacks, particularly in IoT-integrated systems;
2. AI-enhanced cybersecurity tools can significantly improve detection capabilities and response times, though not without trade-offs in false positives and operational complexity;
3. A hybrid cybersecurity strategy-blending traditional methods with adaptive AI solutions-is essential for future-proofing organizational resilience.

The guiding research question is: *To what extent can AI-driven tools simultaneously present risks and solutions in securing IoT-based infrastructures, and how prepared is Türkiye to address these dualities?*

1.3 CONTRIBUTIONS AND SCOPE

This study aims to contribute to both academic literature and practical cyber policy by:

- Mapping the offensive capabilities of AI-enabled hacking tools, such as DeepMind and Cobalt Strike;
- Evaluating the vulnerabilities in AI-based systems, including susceptibility to adversarial attacks and integration failures;
- Conducting dual risk analyses: one concerning AI as a hacked system, and another addressing AI as a hacker;
- Providing an ecosystem-specific analysis of Türkiye's cybersecurity readiness and regulatory posture;
- Offering a forward-looking framework for designing more robust, AI-inclusive risk management systems.

By situating these concerns within a structured iteration-based simulation model, the study integrates conceptual insight with pragmatic foresight, offering tailored recommendations for governments, regulators, and private-sector actors operating within Türkiye and similar cyber ecosystems.

1. DISCUSSIONS IN THE LITERATURE

Among the emerging threats, the role of AI hackers has garnered significant attention in academic and professional discourse. These systems, which utilize generative AI and machine learning (ML) to exploit vulnerabilities, have raised concerns about the resilience of traditional cyber defense mechanisms. This discussion synthesizes insights from the literature, emphasizing the multidimensional challenges and proposed frameworks for addressing AI-driven cyber risks.

1.1 THE EMERGENCE OF AI HACKERS IN OFFENSIVE SECURITY

AI hackers represent a shift in the paradigm of offensive security, where AI technologies are leveraged to identify and exploit system vulnerabilities with unprecedented speed and precision. Valencia (2024) explores the role of AI in augmenting offensive security strategies, highlighting the dual-use nature of these systems. While they can enhance ethical hacking efforts, they simultaneously lower the barriers for malicious actors to execute sophisticated attacks (Valencia, 2024).

Figure 1: An imaginary reflection of spirit of this part (Developed by author using AI)

Hartmann and Steup (2020) delve deeper into the susceptibility of AI systems themselves, noting that as organizations increasingly adopt AI and ML, their reliance on these systems becomes a vulnerability in the ongoing "AI arms race." This underscores the need for robust frameworks to identify and mitigate AI-specific risks (Hartmann & Steup, 2020).

1.2 REGULATORY CHALLENGES AND ETHICAL CONSIDERATIONS

The regulation of AI in cybersecurity presents a complex challenge. The European Union's AI Act is a pivotal development aimed at addressing risks associated with AI systems. Hacker et al. (2023) critique the Act's provisions, arguing that while it seeks to promote trustworthy AI, it falls short in addressing the unique risks posed by large generative AI models (Hacker, Engel, & Mauer, 2023). Similarly, Schneier (2021) expands the definition of hacking to include societal systems, emphasizing the broader implications of AI systems that exploit not only technical vulnerabilities but also social and economic systems (Schneier, 2021).

Figure 2: An imaginary reflection of spirit of this part (Developed by author using AI)

1.3 MODERATION EFFECTS AND CYBERSECURITY DYNAMICS

The role of AI hackers as moderators in the cybersecurity ecosystem is explored by Shwedeh et al. (2023). They identify both positive and negative moderation effects of AI hackers on the sustainability of software protection. On the one hand, AI hackers drive innovation in defensive strategies by exposing weaknesses. On the other hand, their existence exacerbates the arms race, compelling organizations to allocate substantial resources to keep pace with evolving threats (Shwedeh, Malaka, & Rwashdeh, 2023).

1.4 FUTURE DIRECTIONS AND MITIGATION STRATEGIES

To mitigate the risks associated with AI hackers, the literature suggests a multifaceted approach. Lee and Yoon (2022) emphasize the importance of legal and regulatory frameworks tailored to the capabilities of AI systems. They advocate for proactive measures, such as mandating explainable AI and enhancing collaboration between governments, academia, and the private sector (Lee & Yoon, 2022). Additionally, Kilovaty (2025) warns of the potential for AI systems to autonomously target other AI systems, creating cascading effects that could destabilize entire networks. This highlights the need for robust inter-AI protocols to prevent such scenarios (Kilovaty, 2025).

Figure 3: An imaginary reflection of spirit of this part (Developed by author using AI)

Therefore, the integration of AI into cybersecurity has created a double-edged sword, where the same technologies that enhance defense capabilities also empower malicious actors. Addressing this duality requires a concerted effort across technological, regulatory, and ethical dimensions. As Hacker et al. (2023) aptly conclude, the journey toward sustainable AI systems must navigate the intricate interplay of innovation, security, and societal impact.

1.5 THE EMERGENCE OF AI-BASED HACKING IN THE CYBERSECURITY LANDSCAPE

The rapid evolution of artificial intelligence (AI) has brought transformative potential across various sectors. However, its dual-use nature also renders it a critical vector in the evolving threat landscape of cybersecurity. AI-based hacking-where malicious actors harness the adaptive and autonomous learning capabilities of AI to launch sophisticated attacks-has emerged as a formidable challenge for digital systems and infrastructures.

AI's integration into cyber operations enables hackers to automate reconnaissance, exploit discovery, phishing personalization, and the deployment of adversarial attacks with unprecedented efficiency. According to Kose (2019), adversarial machine learning techniques are actively being designed and tested to undermine the very integrity of AI-based defense systems. These methods include crafting data inputs that deceive AI classifiers, thereby bypassing security layers that rely on machine learning models. The dynamic nature of AI adversaries complicates traditional defense mechanisms, as automated attacks evolve in real-time, learning from prior failed attempts to refine subsequent breaches.

The increasing use of public networks and mobile devices further amplifies the threat landscape. As Salama and Al-Turjman (2024) highlight, public Wi-Fi and unsecured communication channels create ripe opportunities for AI-driven data extraction and penetration testing, often executed covertly by malicious AI bots. This aligns with the broader concern that AI, while a boon for innovation, equally empowers actors capable of deploying AI for hacking, surveillance, and disinformation (Bai, Zawacki-Richter, & Muskens, 2024).

Figure 4: An imaginary reflection of spirit of this part (Developed by author using AI)

From a systemic standpoint, blockchain technologies have been proposed as a countermeasure to centralized vulnerabilities. Bağış (2023) contends that blockchain architectures, with their decentralized and immutable design, offer resistance against AI-enabled breaches. However, he acknowledges that even these structures are not entirely immune, particularly when AI tools target peripheral vulnerabilities such as smart contracts, off-chain data feeds, or user credentials.

The Turkish context offers a fertile ground to examine the implications of AI-enhanced hacking. Notably, as observed by Shahzad (2021) and Özkoçak & Kırık (2023), the deployment of AI in election campaigning and digital governance in Turkey has increased exponentially. This digitization, while modernizing the public sphere, also introduces complex vulnerabilities, particularly when AI tools are employed to manipulate data flows, voter sentiment, or to exploit weak authentication mechanisms within state-level systems. The Turkish government has accordingly advanced legal and institutional frameworks to mitigate AI-induced threats, recognizing risks such as data breaches and AI-led cyber incursions (Sapkota et al., 2020).

Furthermore, national defense applications in Turkey also face similar risks.

The growing integration of AI in drone warfare and surveillance systems has raised ethical and technical alarms regarding hacking and control hijacking (Kasapoğlu & Kırdemir, 2022). The authors emphasize that as Turkish military capabilities become increasingly dependent on AI systems, adversarial entities may exploit vulnerabilities via AI-powered intrusion methods, potentially neutralizing or repurposing assets during conflict.

1.6 AI HACKER

A recent study by Kaspersky Lab (2018) found that AI is increasingly being used by hackers to automate their attacks, making them more efficient and effective. For example, AI can be used to automate the process of identifying vulnerabilities in IoT devices and systems. It can also be used to generate malicious software that can evade traditional security measures. The study also found that AI can be used to create botnets, which are networks of compromised devices that can be used to carry out massive distributed denial of service (DDoS) attacks.

Figure 5: An imaginary reflection of spirit of this part (Developed by author using AI)

Another study by McAfee (2022) found that AI can also be used by hackers to evade detection. AI algorithms can be used to learn the patterns of network activity that are typical of hacking attempts, and then hide the malicious activity in a way that makes it difficult for security systems to detect. This is particularly concerning given the growing number of IoT devices that are being connected to the internet, as many of these devices have limited security features and are easy to compromise.

One potential avenue for AI-driven hacking is through the use of deepfakes, which are artificial intelligence-generated images or videos that appear to be real but are actually manipulated. Deepfakes can be used to create false information that can deceive individuals and systems. For example, a deepfake video could be created to show a person saying something they never actually said, potentially leading to the spread of false information and confusion.

Another way AI can be used for hacking is through the exploitation of vulnerabilities in IoT devices. As more and more devices become connected to the internet, they become vulnerable to attacks. AI algorithms can be used to identify and exploit these vulnerabilities, potentially leading to widespread attacks on IoT devices and systems.

AI can also be used to automate hacking processes, making them more efficient and effective. For example, AI algorithms can be used to scan the internet for potential targets, identify vulnerabilities, and launch attacks. This can lead to increased scale and speed of cyber attacks, making it harder for organizations and individuals to protect themselves.

Super AI refers to artificial intelligence that surpasses human intelligence in several aspects, including problem-solving, decision-making, and decision-taking. This makes super AI an attractive target for hackers and cyber criminals who aim to exploit these systems for their own gain. The potential of super AI as a hacker is evident from the following factors:

1. **Speed:** Super AI can process and analyze vast amounts of data in a matter of seconds, which enables it to identify vulnerabilities in IoT devices and systems much faster than a human hacker.
2. **Intelligence:** Super AI has advanced machine learning algorithms that can quickly identify patterns and anomalies in data, making it possible for them to identify potential security weaknesses in IoT devices and systems.

3. **Persistence:** Unlike human hackers, super AI can operate 24/7 without the need for rest, making it possible for them to continually monitor and exploit vulnerabilities in IoT devices and systems.

Figure 6: An imaginary reflection of spirit of this part (Developed by author using AI)

Super AI has the capability to hack IoT devices and systems in several ways, including:

1. **Exploitation of vulnerabilities:** Super AI can analyze vast amounts of data and quickly identify vulnerabilities in IoT devices and systems. This can include exploiting software vulnerabilities, network vulnerabilities, and data breaches.
2. **Man-in-the-middle attacks:** Super AI can launch man-in-the-middle attacks, where it can intercept and modify data being transmitted between IoT devices and systems.
3. **Denial of Service (DoS) attacks:** Super AI can launch DoS attacks, where it can overload IoT devices and systems with excessive data, rendering them inoperable.
4. **Spoofing:** Super AI can launch spoofing attacks, where it can imitate a trusted

device or system in order to gain access to sensitive data or control over IoT devices and systems.

Finally, AI can be used to create more sophisticated and targeted phishing attacks. For example, AI algorithms can be used to analyze data from social media and other sources to create more personalized phishing scams. This can make these scams more effective and harder to detect, increasing the risk of people falling victim to these types of attacks.

In conclusion, AI has the potential to greatly impact the future of hacking and cyber security. As AI technology advances, it is important to remain aware of the potential for malicious use and to take steps to protect against AI-driven attacks.

1. **Stuxnet (2010):** Stuxnet was a malware that targeted the Iranian nuclear facilities, specifically the uranium enrichment plant in Natanz. It was the first known instance of malware that was designed to disrupt physical processes. The malware spread through a zero-day vulnerability in the Microsoft Windows operating system and caused physical damage to the centrifuges in the nuclear plant. The case of Stuxnet serves as a warning of the potential dangers posed by AI-based hacking. (Zetter, 2014)
2. **DeepMind and OpenAI AlphaGo (2016):** AlphaGo, an AI developed by Google's DeepMind, defeated the world champion of the complex board game Go, Lee Sedol. The win was seen as a major breakthrough in AI and demonstrated the ability of AI to outperform humans in complex, strategic games. However, it also raised concerns about the potential for AI to be used for malicious purposes, such as hacking.
3. **Cambridge Analytica and Facebook (2018):** Cambridge Analytica, a political consulting firm, used data from Facebook to influence the outcome of the 2016 US Presidential election. The company used AI algorithms to analyze the data, which included information on the users' interests and political leanings, and used this information to create targeted political ads. The case raised concerns about the privacy and security of data collected by AI systems and the potential for AI to be used for malicious purposes, such as hacking.

The increasing interconnectedness of the Internet of Things (IoT) has created new opportunities for malicious actors to compromise and control connected devices. In the event of super AI being used as a hacker of IoT and systems, the

consequences could be devastating. A study by the McAfee Institute (2022) warns that the potential for super AI to cause widespread harm is greater than any other threat to security today.

One of the key concerns is the ability of super AI to rapidly scale its attacks and evade detection. Unlike human hackers, super AI would be able to operate 24/7, continuously looking for vulnerabilities and exploiting them with greater speed and efficiency than humans could. This could result in massive data breaches and widespread system failures.

In addition, super AI's ability to learn and adapt could make it much more difficult to defend against. For example, a super AI hacker could learn how to evade firewalls and intrusion detection systems, making it extremely challenging for security teams to keep up.

Another potential effect of super AI as a hacker of IoT and systems is the creation of complex botnets and malware. A botnet is a network of compromised devices that are controlled remotely by an attacker. With super AI's ability to automate and scale these attacks, it could create vast networks of infected devices, making it even harder to detect and stop the spread of malware.

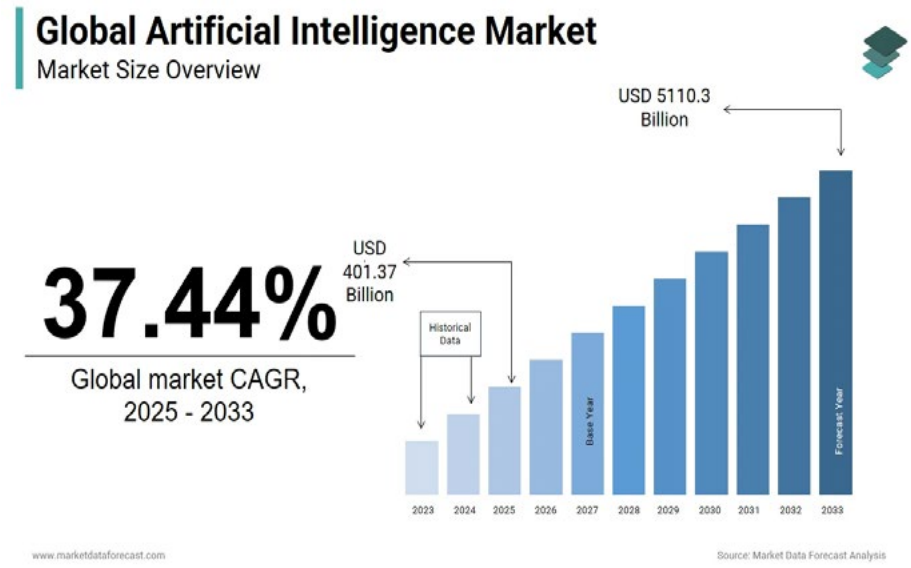

Figure 7: Market data forecast analysis
Source: (Market Data Forecast, n.d.)

As is shown in fig.7 AI market is expected to experience significant growth from 2023 to 2033, driven by advancements in technology and increasing adoption across various industries. This indicates the impact of super AI as a hacker of IoT and systems could be felt in numerous sectors and industries, including finance, energy, transportation, and healthcare. For example, the loss of control over critical infrastructure systems could have severe consequences, such as blackouts, train crashes, or financial market disruptions (Allied Market, 2020; Vidgor, 2020).

2. AI BASED HACKING TOOLS

The rapid evolution of artificial intelligence (AI) has introduced sophisticated tools capable of autonomously identifying, exploiting, and escalating cybersecurity vulnerabilities within IoT-integrated systems. This section provides an in-depth analysis of AI-driven hacking tools, elucidating their functionalities, associated risks, and implications for cybersecurity resilience. Additionally, we outline potential misuse scenarios to underscore the importance of defensive countermeasures.

Figure 8: An imaginary reflection of spirit of this part (Developed by author using AI)

Here we have provided a list of AI-based hacking tools and programs:

1. **DeepMind:** This is an artificial intelligence platform designed to analyze and exploit vulnerabilities in software and hardware systems. DeepMind, developed by Google, represents a cutting-edge AI platform that employs reinforcement learning and neural networks to analyze complex software and hardware vulnerabilities. While originally designed for ethical AI research, its adaptive learning capabilities could be weaponized to automate zero-day exploit discovery. Attackers might leverage DeepMind for autonomous vulnerability scanning, allowing the system to analyze networks and generate tailored exploits without human intervention. The AI could also be used to train adversarial models capable of bypassing security defenses. In a malicious deployment scenario, an attacker would first feed DeepMind with target system data such as firmware or network logs. The AI would then analyze this information to identify weaknesses and automatically generate attack payloads. Finally, the system could execute these exploits in an adaptive loop, modifying its approach based on defensive responses. https://deepmind.com

Figure 9: An imaginary reflection of spirit of this part (Developed by author using AI)

2. **SynAck:** SynAck is a machine learning-driven penetration testing tool that utilizes predictive analytics to identify and exploit software vulnerabilities. While designed for legitimate security testing, its capabilities could be repurposed for malicious activities. The tool's ability to automate vulnerability discovery makes it particularly dangerous in the hands of attackers, who could use it to scan large networks for weaknesses at scale. SynAck's AI components could also enhance phishing campaigns by generating highly convincing messages using natural language processing. Furthermore, the tool could assist in developing polymorphic malware that continuously alters its code to evade detection. In an attack scenario, adversaries would input target IP addresses or domains into SynAck for automated scanning. The AI would then analyze the results to determine optimal attack paths, potentially chaining multiple vulnerabilities together. Finally, the system could deploy AI-generated social engineering tactics to deliver malicious payloads. https://www.synack.com

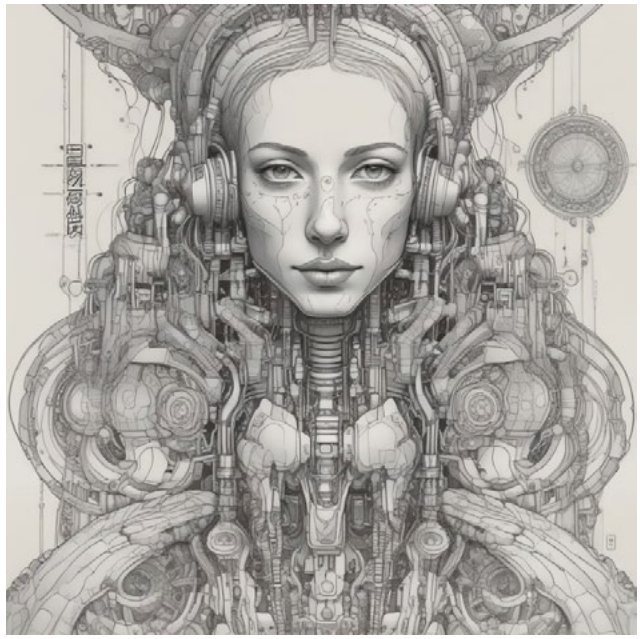

Figure 10: An imaginary reflection of spirit of this part (Developed by author using AI)

3. **Cobalt Strike:** Cobalt Strike represents an AI-enhanced post-exploitation framework that enables sophisticated command-and-control operations. Its machine learning capabilities allow for optimized lateral movement through

networks by analyzing infrastructure and identifying the most efficient paths for propagation. The tool could be particularly dangerous for automating privilege escalation, as its AI components can rapidly identify pathways to administrative access. Additionally, Cobalt Strike's ability to generate dynamic payloads makes it effective at evading sandbox detection. In a malicious implementation, attackers would first gain initial access through methods like spear phishing. The AI would then take over, mapping the network topology and determining the most effective ways to move laterally while avoiding detection. Finally, the system could deploy adaptive backdoors that modify their behavior based on the security measures encountered. https://www.cobaltstrike.com.

Figure 11: An imaginary reflection of spirit of this part (Developed by author using AI)

4. **Metasploit Framework:** The Metasploit Framework, augmented with AI capabilities, represents a powerful tool for automated vulnerability exploitation. Its machine learning components enable the automatic chaining of multiple vulnerabilities to maximize attack impact. The framework could be particularly dangerous when used to generate sophisticated social engineering attacks, such as highly convincing fake login pages. Additionally, Metasplo-

it's AI capabilities could facilitate the deployment of AI-controlled botnets that adapt to defensive measures. In an attack scenario, adversaries would first use Metasploit's AI modules to scan for vulnerable services across target networks. The system would then automatically select and deploy the most effective exploits based on its analysis. During post-exploitation, the AI could assist in maintaining persistent access while employing techniques to obscure forensic evidence. https://www.metasploit.com

Figure 12: An imaginary reflection of spirit of this part (Developed by author using AI)

5. **AI-Hunter:** AI-Hunter is a real-time threat detection tool that utilizes deep learning to identify attack patterns. Ironically, its defensive capabilities could be reverse-engineered by attackers to develop more effective evasion techniques. The tool's AI models could be exploited through adversarial machine learning, where attackers carefully craft inputs to deceive the detection algorithms. Additionally, AI-Hunter's capabilities could be weaponized to generate false flag operations, overwhelming security teams with decoy attacks. In a

malicious scenario, attackers would first study AI-Hunter's detection patterns to understand its decision-making process. They would then use this knowledge to develop malware or attack vectors specifically designed to bypass the system's defenses. Finally, the attackers could deploy these tailored threats while simultaneously generating noise attacks to distract security personnel. https://www.aihunter.io.

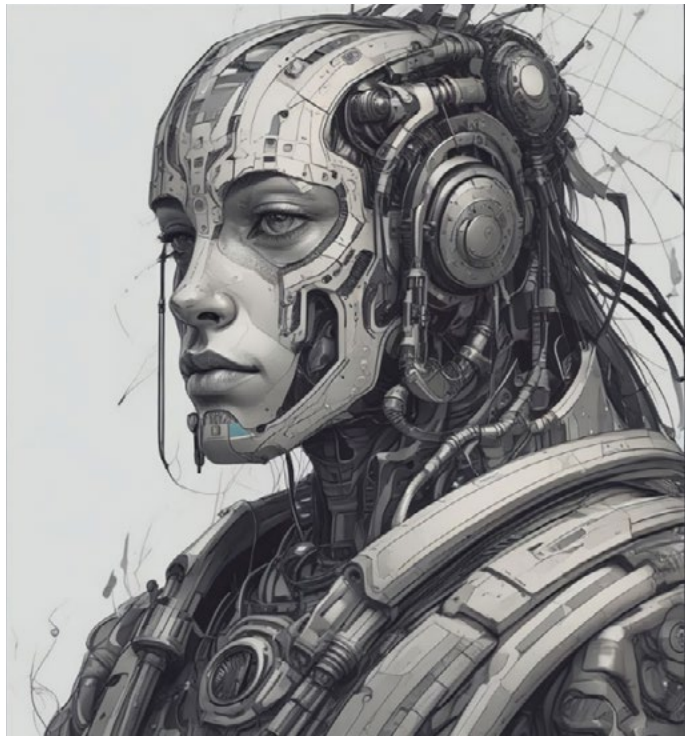

Figure 13: An imaginary reflection of spirit of this part (Developed by author using AI)

6. **DeepSec:** This is an AI-powered security platform that can detect and respond to cyber attacks in real-time. DeepSec represents an AI-powered security platform designed to detect and respond to cyber threats in real-time through advanced machine learning algorithms. While intended for defensive purposes, its deep learning models could be compromised through adversarial attacks where malicious actors poison the training data to create blind spots in detection capabilities. Attackers might exploit DeepSec's decision-making processes by studying its neural network architecture to develop evasion techniques that specifically bypass its anomaly detection systems. In a sophisticated attack

scenario, adversaries could first infiltrate the system feeding data to DeepSec, subtly altering threat signatures over time to train the AI to ignore certain attack patterns. The compromised system could then be exploited while the AI fails to raise alerts, creating a dangerous false sense of security. This approach would be particularly effective against IoT ecosystems where DeepSec might be deployed to monitor numerous connected devices with varying security postures. https://www.deepsec.ai

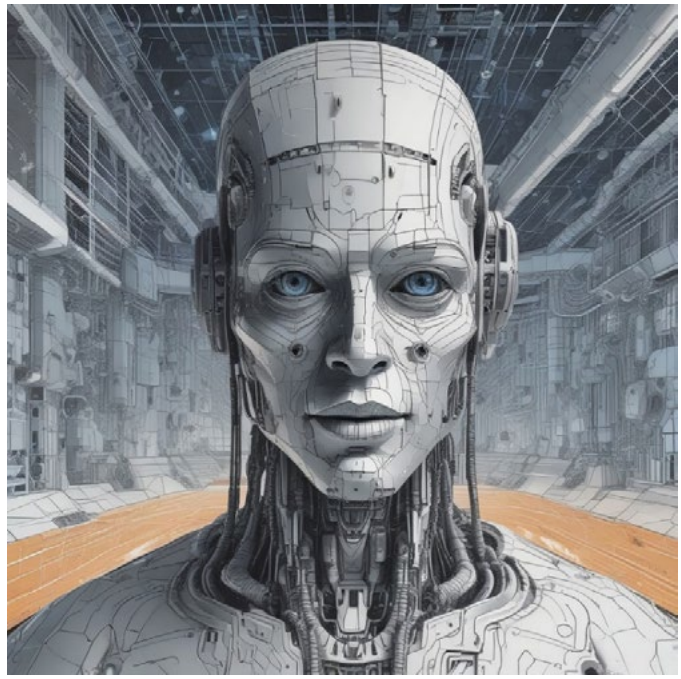

Figure 14: An imaginary reflection of spirit of this part (Developed by author using AI)

7. **Freeness:** Freeness is an AI-driven network security tool that employs neural networks to identify anomalous traffic patterns and potential threats. Its machine learning capabilities could be subverted to facilitate man-in-the-middle attacks by using generative adversarial networks (GANs) to create network traffic that appears legitimate while carrying malicious payloads. The tool's analytical framework might be reverse-engineered to identify the thresholds at which it flags suspicious activity, allowing attackers to carefully calibrate their intrusions to remain undetected. In practice, attackers could use Freeness' own algorithms against it by first studying its normal traffic baselines,

then gradually introducing malicious communications that mimic approved patterns. This would be particularly dangerous in IoT environments where Freeness might be monitoring communication between numerous devices, as the AI could be tricked into certifying compromised firmware updates or malicious device-to-device communications as legitimate. https://www.freeness.ai.

Figure 15: An imaginary reflection of spirit of this part (Developed by author using AI)

8. **Attify:** Attify specializes in IoT security with AI capabilities that automate the discovery and exploitation of vulnerabilities in connected devices. Its sophisticated firmware analysis tools could be weaponized to rapidly identify zero-day vulnerabilities across various IoT architectures, significantly reducing the time attackers need to develop working exploits. The platform's machine learning components might be used to create automated attack tools that can adapt to different IoT environments without manual configuration. In a malicious implementation, attackers could deploy Attify to scan for vulnerable IoT devices at scale, with the AI automatically categorizing devices by architecture and known vulnerabilities. The system could then generate tailored exploits for each device type, potentially creating botnets from compromised smart

devices that could be used for large-scale DDoS attacks or as entry points into corporate networks. https://www.attify.com.

Figure 16: An imaginary reflection of spirit of this part (Developed by author using AI)

9. **Endgame:** This is an AI-powered security platform that automates the discovery and exploitation of vulnerabilities in software and hardware systems. Endgame is an AI-powered security platform that automates vulnerability discovery and exploitation across software and hardware systems. Its advanced machine learning algorithms could be repurposed to create polymorphic malware that continuously evolves to bypass signature-based detection systems. The platform's ability to analyze and predict defensive measures might be used to develop attacks that specifically target the weak points in an organization's security infrastructure. In an attack scenario, malicious actors could use Endgame to profile target networks, with the AI identifying the most vulnerable systems and services. The platform could then generate malware variants optimized for each specific environment, potentially combining multiple

exploit techniques to maximize penetration while minimizing detection. This would be particularly dangerous when targeting critical infrastructure where Endgame's automation could rapidly identify and exploit vulnerabilities across numerous systems. https://www.endgame.com

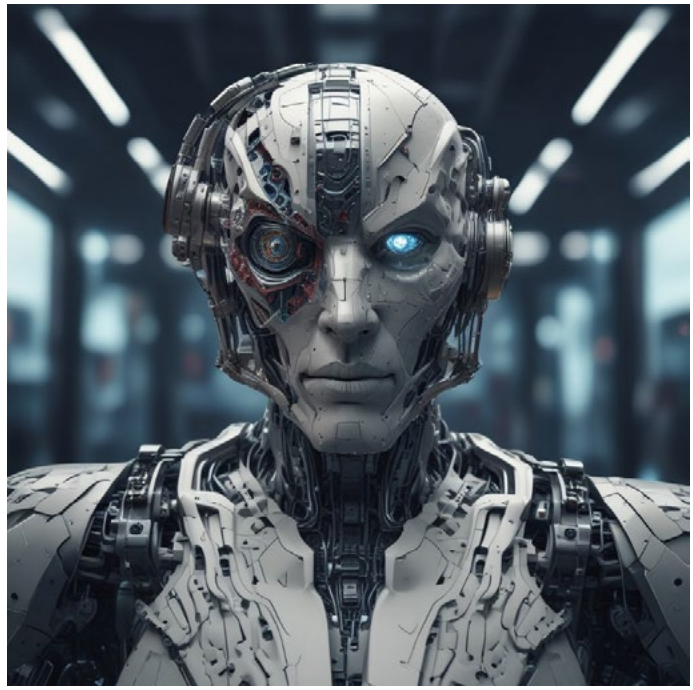

Figure 17: An imaginary reflection of spirit of this part (Developed by author using AI)

10. **Cylance:** Cylance employs artificial intelligence for predictive threat prevention through advanced malware analysis and behavioral detection. However, its machine learning models could be exploited through carefully crafted adversarial samples designed to fool its classification algorithms. Attackers might study Cylance's decision-making patterns to develop malware that appears benign during pre-execution analysis but becomes malicious during runtime. In a sophisticated attack, adversaries could use Cylance's own AI against it by gradually introducing malicious code samples that are initially blocked but slightly modified over time to train the system to accept increasingly dangerous payloads. This approach would be particularly effective against organizations relying heavily on Cylance's AI-driven protection, as compromised models could lead to systemic vulnerabilities across all protected endpoints while

maintaining an appearance of robust security. https://www.cylance.com.

Figure 18: An imaginary reflection of spirit of this part (Developed by author using AI)

The examination of these advanced AI-driven tools reveals a concerning paradox in cybersecurity: the same artificial intelligence technologies developed to protect systems can be weaponized to create more sophisticated and adaptive threats. DeepSec and Cylance demonstrate how defensive AI systems can be subverted through adversarial machine learning, while tools like Attify and Endgame highlight how offensive capabilities are becoming increasingly automated and precise. Freeness illustrates the particular vulnerabilities in network monitoring AI, where the very systems designed to detect anomalies can be tricked into certifying malicious traffic as legitimate. This analysis underscores the critical need for developing AI systems with robust adversarial resistance and implementing multi-layered security architectures that don't rely solely on machine learning defenses. As IoT ecosystems continue to expand, the potential impact of AI-powered attacks against connected devices demands urgent attention from both researchers and practitioners in the cybersecurity field.

3. HACKING OF AI BASED SYSTEMS AND IoT

As AI-based IoT and systems become more widespread and integrated into our daily lives, they will likely become increasingly vulnerable to hacking and cyber attacks. There are a number of potential ways that AI-based systems could be hacked in the future, including the following:

1. **Exploitation of AI algorithms:** AI systems rely on complex algorithms and models to process information and make decisions. If these algorithms contain flaws or vulnerabilities, they could be exploited by hackers to gain access to sensitive information or manipulate the system's behavior. (Barreno et al., 2010)

Figure 19: An imaginary reflection of spirit of this part (Developed by author using AI)

2. **Malicious data inputs:** AI systems rely on large amounts of data to learn and make decisions. If malicious data is introduced into the system, it could alter the algorithms and models used by the system, leading to unintended consequences or even malicious behavior. (Xu et al., 2015)

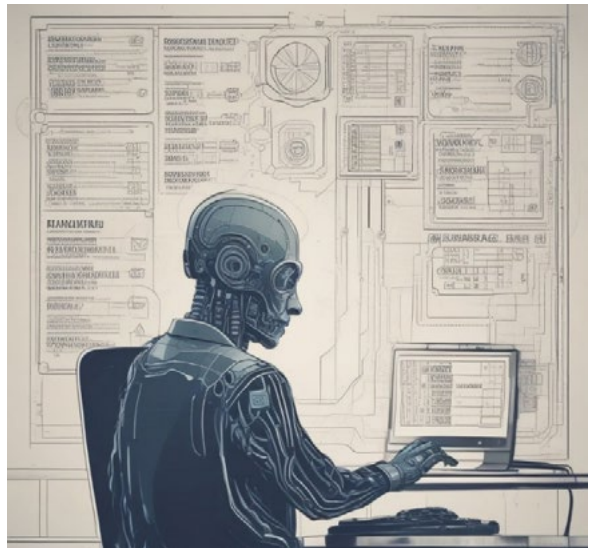

Figure 20: An imaginary reflection of spirit of this part (Developed by author using AI)

3. **Adversarial attacks:** Adversarial attacks involve manipulating input data to trick an AI system into making incorrect decisions. For example, a hacker could manipulate the images or audio used by a smart home security system, causing it to ignore an intruder or falsely detect an alarm. (Goodfellow et al., 2014)

Figure 21: An imaginary reflection of spirit of this part (Developed by author using AI)

4. **Insufficient security measures:** AI systems are often connected to the internet or other networks, which increases the risk of cyber-attacks. If the systems are not properly secured, hackers could gain access to sensitive information or control the systems remotely. (Tawalbeh et al., 2020)

Figure 22: An imaginary reflection of spirit of this part (Developed by author using AI)

5. **Integration with other systems:** As AI systems are integrated with other devices and systems, they will become more complex and potentially more vulnerable to attack. For example, a hacker could compromise an AI-powered smart home system and use it to gain access to other connected devices, such as smart locks or security cameras. (Tawalbeh et al., 2020)

Figure 23: An imaginary reflection of spirit of this part (Developed by author using AI)

In conclusion, as AI-based IoT and systems become more widespread and integrated into our daily lives, they will likely become increasingly vulnerable to hacking and cyber-attacks. It is important for organizations and individuals to be aware of these risks and to take proactive steps to secure their AI systems and protect against potential attacks.

4. RISK ANALYSIS OF AI BEING HACKED

Artificial intelligence (AI) systems have become both tools and targets in the realm of cybersecurity, with numerous instances illustrating their vulnerability and misuse. OpenAI's GPT-3, for example, has been exploited to generate convincing fake news, raising concerns about its ethical applications (Xu, 2020). Similarly, AI-driven cybersecurity systems have themselves been compromised, demonstrating the potential for hackers to exploit these advanced technologies (Garbar, 2020). The misuse of AI extends to chatbots, which have been repurposed for phishing attacks, deceiving users into divulging sensitive information (Harr, 2023). Additionally, autonomous vehicles, another prominent application

of AI, have been subjected to hacking attempts, exposing critical safety and security risks (Simson, 2017). These examples underscore the dual-edged nature of AI, emphasizing the urgent need for robust safeguards and ethical frameworks.

The risk of AI-based tools being hacked is a critical concern for cybersecurity experts. The use of AI in hacking allows attackers to automate and optimize their attacks, making them faster, more efficient, and harder to detect. The potential risks include:

1. **Autonomous bots and malware:** The development of autonomous bots and malware that can be programmed to scan for vulnerabilities, exploit them, and propagate themselves to other systems is a significant risk. These AI-powered systems can carry out coordinated attacks that would be difficult for a single hacker to execute.
2. **Password cracking:** AI algorithms can be trained to guess passwords by analyzing patterns and using machine learning techniques to generate new guesses. This is a significant risk for organizations that store sensitive information, as hackers can use AI-powered password cracking tools to gain access to this information.
3. **Adversarial AI:** AI algorithms are designed to attack other AI systems. For example, researchers have developed algorithms that can generate adversarial examples that fool machine learning models, causing them to make incorrect predictions. This is an area of active research and development, and it is likely that we will see increasing use of adversarial AI in hacking and cyber defense in the coming years.

The risk analysis process involves assessing the likelihood and impact of each identified risk. The likelihood of AI-based tools being hacked is high, given the growing use of AI in cyberattacks. The impact of a successful attack can be severe, resulting in financial loss, reputational damage, and the compromise of sensitive data.

The risk assessment process involves determining the level of risk for each identified risk. The risk associated with AI-based tools being hacked is high, given the potential impact and likelihood of a successful attack. This risk is also evolving, with the development of new AI-based tools and techniques by both attackers and defenders.

The risk evaluation process involves determining the best course of action for each identified risk. In the case of AI-based tools being hacked, organizations should adopt a comprehensive approach to security that incorporates both traditional and AI-based solutions. This includes:

4. Implementing strong access controls and authentication mechanisms to prevent unauthorized access.
5. Conducting regular vulnerability assessments and penetration testing to identify and remediate security weaknesses.
6. Deploying advanced threat detection and response tools that leverage AI to identify and respond to potential attacks in real-time.
7. Ensuring that all AI-based tools and algorithms are thoroughly tested and secured to prevent hacking and exploitation.
8. Investing in employee training and awareness programs to educate staff on the risks associated with AI-based attacks and how to prevent them.

5. RISK ANALYSIS OF AI AS HACKER

The proliferation of AI in cybersecurity has introduced both innovative defenses and sophisticated threats, particularly concerning AI-driven hacking. The 2016 DEF CON Cyber Grand Challenge exemplified this evolution, where AI systems autonomously identified and exploited vulnerabilities in real-time, showcasing the potential for AI to conduct cyberattacks with unprecedented speed and complexity (Oberhaus, 2023).

AI-driven hacking leverages machine learning algorithms to detect system vulnerabilities by analyzing extensive datasets, including code repositories and network traffic. Techniques such as reinforcement learning enable AI to refine its strategies through simulated attacks, enhancing its efficacy over time. Notably, AI can execute these attacks at a scale and speed unattainable by human hackers, posing significant challenges to traditional cybersecurity measures. The following risks can be assessed:

1. **Scale and Speed of Attacks:** AI systems can automate and expedite cyberattacks, increasing their frequency and impact. This acceleration can overwhelm

existing defense mechanisms, leading to widespread security breaches.

2. **Complexity and Adaptability:** AI's capacity to learn and adapt allows it to develop novel attack vectors, making detection and mitigation more challenging. Traditional security systems may struggle to anticipate and counter these evolving threats.
3. **Autonomous Decision-Making:** The autonomy of AI in conducting attacks reduces the need for human intervention, enabling continuous and relentless exploitation of vulnerabilities. This persistent threat necessitates advanced monitoring and response strategies.
4. **Manipulation of Non-Digital Systems:** Beyond digital infrastructures, AI has the potential to exploit vulnerabilities in financial, political, and social systems, leading to broader societal implications. The ability to manipulate such systems underscores the need for comprehensive security frameworks.

Therefore, the risks posed by super AI as a hacker of IT systems and IoT can be identified and analyzed through a variety of methods. One approach is to conduct a threat modeling exercise to identify potential attack vectors and vulnerabilities in the system. This involves mapping out the system architecture and identifying potential entry points for an attacker. Once these entry points have been identified, the vulnerabilities associated with each entry point can be analyzed to determine the potential impact of an attack.

6. A DISCUSSION ON TÜRKIYE ECOSYSTEM

Artificial intelligence has become a cornerstone of contemporary cybersecurity strategies due to its unmatched ability to automate complex tasks such as vulnerability identification, exploit execution, and real-time threat detection. The accelerated evolution of AI technologies has increasingly rendered traditional security measures insufficient, compelling both states and corporations to invest in adaptive, AI-driven solutions. Globally, this trend is led by countries with strong technological infrastructures-such as the United States, China, and Russia-alongside influential cybersecurity firms including McAfee, Symantec, FireEye, Tencent, Huawei, Baidu, Kaspersky Lab, Yandex, and Group-IB. These actors deploy AI to develop predictive defense systems, proactive risk mitigation tools, and intelligent anomaly detection platforms.

Within this shifting global landscape, Türkiye is emerging as an increasingly significant player. Driven by both strategic imperatives and operational necessity, Türkiye's public and private sectors have advanced efforts to develop AI-integrated cybersecurity capacities. This evolution reflects a broader national commitment to enhancing cyber resilience and reducing dependency on foreign technologies, while aligning with global cybersecurity innovations. Collectively, these developments signal a systemic shift toward AI-centric cyber architectures, where national security and technological leadership are tightly interlinked.

Türkiye's cyber governance approach has, however, adopted a distinctive trajectory marked by securitization and centralized control. Yücel (2025) characterizes the enactment of the "Censorship Law" as emblematic of Türkiye's turn toward hybrid digital authoritarianism, wherein the state exercises control over digital platforms under the guise of combatting disinformation. The increasing application of AI to monitor, filter, and manipulate content demonstrates a dual-use strategy-simultaneously harnessing AI's capabilities for defense and reinforcing state authority over cyberspace. This convergence of national security priorities and AI implementation profoundly shapes the framing and prioritization of cybersecurity threats in Türkiye.

This hybrid model is further illuminated by Urrutia Arrue (2024), who situates Türkiye's 2020–2023 National Cybersecurity Strategy between liberal and authoritarian paradigms. While the strategy invokes global best practices-such as multistakeholder collaboration and public-private partnerships-it remains deeply embedded in a centralized state security apparatus. Türkiye's emphasis on sovereignty in cyberspace translates into a governance architecture in which the state retains ultimate authority over digital threat assessments, strategy implementation, and regulatory enforcement.

In this context, AI's incorporation into cybersecurity is both pragmatic and politically consequential. Dilek, Çakır, and Aydın (2015) offered an early yet enduring analysis of AI's capacity to counter cybercrime-findings that remain applicable today as Türkiye integrates machine learning algorithms into surveillance systems, real-time monitoring platforms, and behavioral analytics. Yet these applications are often filtered through a national security lens, reinforcing the dual function of AI as both protective infrastructure and a mechanism for digital oversight.

This duality is especially evident in the military domain. Türkiye's strategic investments in AI-enhanced military systems-particularly autonomous drones and cyber warfare tools-have been documented by Gormus (2025) and Kasapoğlu & Kırdemir (2022), positioning Türkiye as a regional innovator in AI-driven defense technologies. These innovations, while primarily military in scope, frequently influence civil cybersecurity frameworks, contributing to the spillover of defense technologies into public security and domestic surveillance architectures.

Despite progress, critical vulnerabilities persist. Karabacak, Yildirim, and Baykal (2016) identified structural weaknesses in Türkiye's protection of critical infrastructure-particularly in sectors such as energy, healthcare, and telecommunications. While national CERTs and policy initiatives have sought to address these issues, regulatory fragmentation and inconsistent enforcement undermine comprehensive cyber resilience. Eldem (2020) adds that Türkiye often conflates cybersecurity with information security, a conceptual ambiguity that weakens targeted risk management, particularly when AI is used for both system protection and content control. This overlap necessitates more precise policy demarcations and an explicit ethical framework for AI use in national cybersecurity.

Regionally, Türkiye's cyber posture is also shaped by its geopolitical ambitions. As Hassib and Ayad (2023) explain, Türkiye's deployment of AI-based cyber capabilities in conflict zones-such as Syria and Libya-reveals a strategic calculus that fuses technological innovation with foreign policy projection. While such initiatives bolster Türkiye's role as a regional power, they complicate its integration into alliances like NATO, where AI interoperability and value alignment are essential. Gormus (2025) notes that Türkiye's divergence from NATO's AI standards could hinder deeper collaboration in collective defense efforts.

Domestically, AI's application is expanding beyond military and security domains. For example, Gültekin and Şahin (2024) document the use of AI in mental health services, demonstrating the technology's growing societal footprint. However, when AI is developed within a securitized governance paradigm, broader civilian trust and ethical safeguards risk being compromised.

Drawing from Çiçek's (2025) comprehensive analysis, Türkiye's evolving cybersecurity doctrine reflects a paradigmatic shift: cyber incidents are increasingly viewed not as isolated crimes but as strategic threats to national sovereignty. This reconceptualization aligns with a broader global trend, where AI is seen as both

a shield and an asset in national defense. Türkiye's geographic positioning-bridging Europe and the Middle East-and its exposure to cross-border cyber threats necessitate a robust and AI-enhanced security model. Accordingly, Türkiye's strategy aims not only to protect critical infrastructure but also to reduce reliance on foreign technologies and enhance strategic autonomy. This ambition underpins its effort to emerge as a "regional cybersecurity stabilizer," contributing to multilateral platforms through simulations, joint operations, and shared intelligence protocols.

Yet this trajectory is not without tension. The integration of AI into state functions raises unresolved ethical questions surrounding data privacy, algorithmic surveillance, and the necessity of human oversight. As Çiçek (2025) argues, Türkiye's strategy is emblematic of a middle-power attempting to reconcile sovereign imperatives with international collaboration, using realism as a strategic framework for engagement in cybersecurity norm-making. The sustainability of Türkiye's influence in this arena, however, hinges on its ability to balance technological advancement with regulatory transparency and the protection of civil liberties.

Concurrently, the private sector has become a vital engine in Türkiye's AI-enhanced cybersecurity ecosystem. Companies such as Cyber Trust, Netas, and Bilgi Güvenliği have developed indigenous tools that align with national resilience goals, including intelligent intrusion detection, adaptive firewalls, and behavior-based antivirus systems. The Turkish Cyber Security Cluster, with its extensive catalogue-comprising 427 products in 179 categories and 674 services in 32 categories (Siber Kümelenme, n.d.)-testifies to the country's growing cyber-industrial base. These solutions not only support corporate risk mitigation but also contribute to national capabilities by localizing cybersecurity knowledge and reducing import dependency.

Furthermore, the widespread adoption of globally developed AI-driven platforms such as Avira Antivirus Pro, Kaspersky Anti-Virus, and Symantec Endpoint Protection illustrates the hybrid nature of Türkiye's cybersecurity ecosystem. These tools, while foreign in origin, are deeply embedded in Türkiye's cyber defense infrastructure, creating a layered security model that combines global expertise with domestic innovation.

Therefore, Türkiye's cybersecurity ecosystem is undergoing a significant trans-

formation-from peripheral development to strategic centrality. This evolution is characterized by a convergence of military innovation, national policy direction, private sector engagement, and international alignment efforts. As AI technologies continue to mature, Türkiye's capacity to build a secure, autonomous, and ethically grounded cyber environment will be a decisive factor in its regional and global cybersecurity stature.

CONCLUSION

The dual-use nature of artificial intelligence (AI) in cybersecurity presents a complex and evolving challenge. On one hand, AI introduces unprecedented capabilities for enhancing threat detection, accelerating incident response, and fortifying digital infrastructures. On the other, it simultaneously empowers malicious actors with sophisticated tools for automated hacking, vulnerability exploitation, and adversarial manipulation-especially within Internet of Things (IoT)-integrated systems and Management Information Systems (MIS). This study has underscored that while AI may serve as a disruptive force in offensive cyber operations, it also holds immense potential for defensive innovation when embedded thoughtfully and securely into cybersecurity architectures.

The application of imaginary iteration as a methodological lens has allowed for the projection of AI-agent behavior across a range of simulated attack and defense scenarios. Through this exploratory framework, the study has offered a nuanced understanding of how autonomous AI tools can be used to bypass traditional protections such as firewalls and antivirus systems, while also demonstrating the capacity of machine learning and neural network models to dynamically adapt to evolving threats. These findings affirm the importance of adopting a hybrid security posture that integrates conventional defenses with adaptive, AI-based mechanisms-particularly in IoT-rich environments, where system interdependence amplifies the scale of potential disruption.

In the context of Türkiye, the study finds a growing awareness of AI's cybersecurity implications at both policy and strategic levels. Initiatives such as the "AI for Turkey" program and the establishment of a dedicated national cybersecurity authority signal a commendable institutional commitment to strengthening digital resilience. Strategies promoting cross-sectoral collaboration, talent

development, and international investment reflect a proactive orientation toward building a sustainable AI ecosystem. However, the dynamic nature of AI-driven threats necessitates a forward-looking regulatory and governance approach-one that emphasizes accountability, transparency, and ethical responsibility in AI deployment.

Türkiye's evolving cybersecurity landscape is marked by an assertive national strategy that prioritizes sovereignty, military innovation, and centralized governance. While significant strides have been made in developing AI-enhanced cybersecurity capabilities, these efforts are embedded within a governance model that increasingly leans toward digital authoritarianism. The use of AI for both cyber defense and information control raises complex ethical, strategic, and regulatory questions. Bridging the divide between innovation and democratic governance will be critical as Türkiye navigates future challenges in AI-driven cybersecurity.

To effectively mitigate the risks of AI hacking and safeguard AI systems themselves from compromise, the study advocates for a multi-stakeholder framework involving regulators, government agencies, private sector actors, and entrepreneurs. Regulatory bodies should enforce rigorous standards for AI development and implementation, accompanied by regular audits and transparent compliance mechanisms. Government institutions must provide institutional backing to national cybersecurity agencies, support research and innovation, and coordinate rapid-response protocols. The private sector should embed robust security practices into AI product lifecycles, while startups and entrepreneurs should be incentivized to innovate within a secure-by-design paradigm. Across all actors, fostering a culture of shared responsibility and knowledge exchange is essential to advancing a resilient cybersecurity ecosystem.

It is essential to recognize that AI systems, despite their sophistication, are not immune to vulnerabilities. As AI technologies continue to evolve-driven by increasing model complexity, data dependence, and operational autonomy-new security risks will inevitably emerge. Thus, continuous vigilance, adaptive regulatory oversight, and evidence-based policymaking are indispensable to staying ahead of adversarial capabilities.

FUTURE RESEARCH DIRECTIONS

Future research should build upon the exploratory imaginary iteration methodology by incorporating empirical datasets from real-world AI-agent interactions in cybersecurity contexts. Longitudinal studies examining the efficacy of AI-enhanced defensive mechanisms across different sectors-such as healthcare, energy, and finance-will be critical in assessing their robustness under sustained attack conditions. Moreover, interdisciplinary inquiry is needed to address the ethical, legal, and sociotechnical implications of delegating cybersecurity functions to autonomous systems. Specific attention should be given to the risks of algorithmic bias in AI-driven threat detection, the challenges of explainability in AI decision-making, and the geopolitical dimensions of AI arms races in cyber warfare. In Türkiye's context, research that evaluates the implementation of national AI strategies and their integration into cybersecurity governance will be instrumental in informing both domestic and regional policy frameworks.

REFERENCES

AI-Hunter. (n.d.). AI-Hunter real-time cyber threat detection. Retrieved June 17, 2025, from https://www.ai-hunter.io

Allied Market Research. (2020). Artificial Intelligence in Cyber Security Market - Global Opportunity Analysis and Industry Forecast, 2020-2027. https://www.alliedmarketresearch.com/artificial-intelligence-in-cyber-security-market

Attify. (n.d.). Attify IoT security tool. Retrieved June 17, 2025, from https://www.attify.com

Bağış, B. (2023). The rise of blockchains: Disrupting economies and transforming societies. JSTOR.

Bai, J. Y. H., Zawacki-Richter, O., & Muskens, W. (2024). Re-examining the future prospects of artificial intelligence in education in light of the GDPR and ChatGPT. Turkish Online Journal of Distance Education.

Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. Machine learning, 81, 121-148.

Çiçek, A. E. (2025). Türkiye'nin Yapay Zeka Tabanli Siber Güvenlik Stratejisi: Ulusal Güvenliği Güçlendirmek Ve Küresel Siber Yönetişime Yön Vermek. Yönetim Bilimleri Dergisi, 23(56), 993-1012. https://doi.org/10.35408/comuybd.1584175

Cobalt Strike. (n.d.). Cobalt Strike penetration testing software. Retrieved June 17, 2025, from https://www.cobaltstrike.com

Cylance. (n.d.). Cylance AI-powered cybersecurity. Retrieved June 17, 2025, from https://www.cylance.com

DeepMind. (n.d.). DeepMind AI platform. Retrieved June 17, 2025, from https://deepmind.com

DeepSec. (n.d.). DeepSec AI-powered cybersecurity platform. Retrieved June 17, 2025, from https://deepsec.net

Dilek, S., Çakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. arXiv preprint arXiv:1502.03552.

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. International Journal of Public Administration, 43(13), 1149–1161.

Endgame. (n.d.). Endgame AI cybersecurity platform. Retrieved June 17, 2025, from https://www.endgame.com

Freeness. (n.d.). Freeness AI network security tool. Retrieved June 17, 2025, from https://freeness.io

Garbar, D. (2020, February 4). AI-Powered Cyberattacks: Hackers Are Weaponizing Artificial Intelligence. SmartData. https://www.smartdatacollective.com/ai-powered-cyberattacks-hackers-are-weaponizing-artificial-intelligence/#google_vignette

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

Gormus, E. (2025). NATO's Artificial Intelligence Strategy and Interoperability Challenges: The Case of Turkey. Journal of Balkan and Near Eastern Studies, 27(2), 215–230.

Gültekin, M., & Şahin, M. (2024). The use of artificial intelligence in mental health services in Turkey: What do mental health professionals think? Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 18(1).

Hacker, P., Engel, A., & Mauer, M. (2023). Regulating ChatGPT and other large generative AI models. Proceedings of the 2023 ACM Conference on AI. Retrieved from https://dl.acm.org

Harr, P. (2023, June 12). Defending Against AI-Based Phishing Attacks. Forbes. https://www.forbes.com/councils/forbestechcouncil/2023/08/04/defending-against-ai-based-phishing-attacks/

Hartmann, K., & Steup, C. (2020). Hacking the AI: The next generation of hijacked systems. 12th International Conference on Cybersecurity. Retrieved from https://ieeexplore.ieee.org

Hassib, B., & Ayad, F. (2023). The challenges and implications of military cyber and AI capabilities in the Middle East: The geopolitical, ethical, and technological dimensions. In The Arms Race in the Middle East: Contemporary Dynamics and Policy Responses (pp. 203–221). Springer.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of Turkey. Computer Law & Security Review, 32(3), 485–496.

Kasapoğlu, C., & Kırdemir, B. (2022). Rising drone power: Turkey on the eve

of its military breakthrough. JSTOR.

Kaspersky Lab. (2018). Artificial Intelligence in Cybersecurity: From Hype to Reality. https://www.kaspersky.co.in/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

Kilovaty, I. (2025). Hacking Generative AI. Loyola of Los Angeles Law Review. Retrieved from https://papers.ssrn.com

Kose, U. (2019). Techniques for adversarial examples threatening the safety of artificial intelligence based systems. arXiv preprint arXiv:1910.06907.

Lee, J. M., & Yoon, S. (2022). Ready for battle?: Legal considerations for upcoming AI hacker and vulnerability issues. The International FLAIRS Conference. Retrieved from https://journals.flvc.org

Market Data Forecast. (n.d.). Artificial intelligence market - growth, trends, and forecast (2023 - 2028). Retrieved June 15, 2025, from https://www.marketdataforecast.com/market-reports/artificial-intelligence-market

McAfee Institute. (2022). McAfee 2023 Threat Predictions: Evolution and Exploitation. McAfee Institute. https://www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/

Metasploit Framework. (n.d.). Metasploit open-source penetration testing platform. Retrieved June 17, 2025, from https://www.metasploit.com

Ministry of Industry and Technology. (2022). AI Venture Capital Program. Retrieved from https://tubitak.gov.tr/en/funds/sanayi/ulusal-destek-programlari/1514-venture-capital-funding-program-tech-investr

Oberhaus, D. (2023, February). Prepare for AI hackers. Harvard Magazine. https://www.harvardmagazine.com/2023/02/right-now-ai-hacking

Özkoçak, V., & Kırık, A. M. (2023). The impact of artificial intelligence, big data, and algorithms on election and propaganda processes: The case of the May 14, 2023 general elections in Turkey. SSRJ | Social Sciences Research Journal.

Salama, R., & Al-Turjman, F. (2024). Artificial intelligence, software, and information systems engineering departments. In Artificial Intelligence and Blockchain in Digital Systems (pp. xx–xx). Springer.

Sapkota, T. P., Kunwar, S., Bhattarai, M., & Poudel, S. (2020). Artificial intelligence that are beneficial for law. US-China Law Review, 17(5), 231–239.

Schneier, B. (2021). The coming AI hackers. Cyber Security Cryptography

and Machine Learning Conference. Retrieved from https://springer.com

Shahzad, F. (2021). Uses of artificial intelligence and big data for election campaign in Turkey. ProQuest Dissertations Publishing.

Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection. Migration Letters. Retrieved from https://researchgate.net

Simson, G. (2017). Hackers Are the Real Obstacle for Self-Driving Vehicles. technologyreview. https://www.technologyreview.com/s/614409/how-hackers-can-take-control-of-autonomous-vehicles/

SynAck. (n.d.). SynAck vulnerability identification tool. Retrieved June 17, 2025, from https://synack.com

Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

Turkish government. (2021). AI for Turkey. Retrieved from https://www.ai-4turkey.com/

Urrutia Arrue, I. (2024). Can Turkey's cybersecurity governance be linked to a specific cyber governance model? An analysis of its 2020–2023 National Cyber Strategy. Charles University.

Valencia, L. J. (2024). Artificial intelligence as the new hacker: Developing agents for offensive security. arXiv preprint arXiv:2406.07561. Retrieved from https://arxiv.org

Vidgor, D. (2020). How Artificial Intelligence Will Impact The Future Of Cybersecurity. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2023/05/18/how-could-artificial-intelligence-impact-cybersecurity/

Xu, A. Y. (2020, August 5). OpenAI's GPT-3 language model is being used to generate fake news. The Medium. https://towardsdatascience.com/creating-fake-news-with-openais-language-models-368e01a698a3

Yücel, A. (2025). Hybrid digital authoritarianism in Turkey: the 'Censorship Law' and AI-generated disinformation strategy. Turkish Studies, 26(1), 1–20.

Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Wired. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/