CYBER SECURITY IN THE AGE OF ARTIFICIAL INTELLIGENCE

Mehmet Emin ERENDOR*
ORCID ID: 0000-0002-8467-0743

Declaration*

With the acceleration of digitalization, cyberspace has become one of the most important areas of competition between states, economic conflicts of interest and social interactions. Especially when evaluated in the context of the developments in the last 10 years, the increase in the dependence of critical infrastructures on digital networks, the transfer of public services to online platforms and the fact that artificial intelligence (AI)-supported technologies have become an integral part of daily life have revealed that cyber security is not only a technical issue, but rather one of the basic components of national and international security. Today's cyber attacks are no longer considered only as isolated incidents targeting information systems, but also as multidimensional security problems that directly affect economic stability, democratic processes, critical infrastructures and national security strategies of states.

AI has brought about a paradigm shift in the field of cybersecurity in recent years. While rapid advances in machine learning, deep learning, and especially generative AI applications have significantly increased defense capacity in threat detection, anomaly analysis, incident response, and malware analysis, they have also brought new risks such as automating cyberattacks, preparing advanced phishing campaigns, synthetic media production, and rapid exploitation of vulnerabilities. Therefore, AI should be considered not only as a protective technology or a new threat source in terms of cyber security, but also as a dual-use strategic technology that transforms the nature of competition between attack and defense.

However, it would be an incomplete approach to evaluate the impact of AI on cyber security only through technological developments. The real transformation lies in the fact that AI is changing the functioning of the international security environment by increasing the speed, scale, level of autonomy and uncertainties of cyber conflicts. Many cyber operations, which traditionally required high technical expertise, significant financial resources and long preparation processes, can be carried out at lower costs, in less time and on a larger scale

* Prof. Dr. At International Relations, ATÜ, merendor@atu.edu.tr
* The opinions expressed belong to the authors only and do not reflect the official position of the institutions they are affiliated with.

thanks to AI. This situation facilitates the access of not only states but also organized crime organizations, terrorist organizations, private companies and individual actors to advanced cyber capacities, thus reshaping the distribution of cyber power.

In this context, the main issue in the age of AI is not whether the technology will be used in the field of cyber security. The main question is how this technology will be managed in a way that supports international peace and security, in line with which normative principles it will be limited, and with which governance mechanisms will new risks be controlled. The widening gap between the pace of development of technological innovations and the compliance capacity of international law, ethical principles and institutional regulations constitutes one of the most important security problems of today. Therefore, the relationship between AI and cybersecurity should be considered not only as a technical transformation but also as a structural issue that shapes the future of international governance, strategic stability, and global security architecture.

How is AI Changing the Character of Cyber Conflicts?

The transformation in the field of cyber security is often explained through new attack techniques or advanced defense tools. However, the impact of AI is much deeper than adding a new dimension to existing cyber threats. The real change is manifesting in the way cyber conflicts are conducted, in the capacity of the actors and in the nature of strategic calculations. In other words, AI transforms the speed, scale, autonomy and accessibility of existing threats rather than creating an entirely new threat landscape in cyberspace.

In the past, carrying out an advanced cyber operation required high technical expertise, long preparation processes, strong financial resources and qualified human resources. State-sponsored advanced persistent threat groups have therefore been at the top of the cyber power hierarchy for many years. Today, generative AI and large language models significantly facilitate the processes of generating code, analyzing security vulnerabilities, preparing phishing content, and developing malware, even for actors with a certain amount of technical knowledge. This indicates a new trend that can be expressed as the democratization of cyber operations. Of course, AI alone does not create an advanced attack capacity, but it lowers the barriers to entry by reducing the need for technical knowledge and makes it possible for a wider group of actors to access advanced cyber tools.

This transformation not only increases the diversity of actors, but also radically changes the pace of cyber operations. AI-powered systems can analyze network traffic in real-time, automatically detect security vulnerabilities, and manage attack or defense processes without human intervention under certain conditions. Thus, the time between decision-making and implementation is getting shorter and shorter, and interactions that take place in seconds or even milliseconds push the limits of human control. This increases the risk of false alarms, erroneous judgments or involuntary escalation, especially in times of crisis. In this new environment where speed gains strategic importance, the capacity of decision-makers to evaluate events and develop appropriate reactions is gradually narrowing.

Another element that AI is transforming is the scale of cyber operations. While phishing attacks carried out with traditional methods are prepared for a certain number of targets, generative AI can produce messages that can be sent to millions of people in a short time, grammatically correct and tailored to the target. Similarly, synthetic audio and video technologies increase the persuasiveness of social engineering attacks and make disinformation campaigns aimed at manipulating public opinion more effective. Therefore, AI strengthens not only attacks targeting technical systems but also cognitive security threats centered on the human factor. This development demonstrates that cybersecurity is no longer merely a matter of safeguarding networks and information systems, necessitating a broader understanding of security that encompasses the preservation of the information ecosystem and societal trust.

However, the impact of AI is not limited to its attack capacity alone. The same technologies also provide significant advantages in the field of defense. Analyzing large datasets, detecting anomalous network behavior, processing threat intelligence, and automating incident response processes allow defenders to achieve significant gains in speed and accuracy. Especially in the protection of critical infrastructures, AI-supported early warning systems can identify patterns that human operators may have difficulty noticing and enable faster reactions to possible attacks.

Yet, this does not mean that there is a definite superiority between attackers and defenders. On the contrary, AI emerges as a technology that constantly increases the tempo of competition instead of making one of the parties permanently advantageous. As defense systems become stronger with AI, attackers develop more complex and adaptable methods using the same technology. Thus, a constantly renewed and accelerating technological

competition cycle is formed in the field of cyber security. This cycle dictates that security can no longer be achieved through static measures, necessitating defense approaches that continuously learn, adapt, and innovate.

As a result, the most important impact of AI on cyber security is not that it gives the offensive or defense side an absolute superiority. The real transformation lies in changing the strategic logic of cyber conflicts. The fact that operations are becoming faster, more autonomous, more scalable and more uncertain raises new questions in a wide range of areas, from threat perceptions of states to crisis management, from deterrence strategies to international cooperation mechanisms. Therefore, understanding the impact of AI on cybersecurity requires not only following technological developments but also analyzing how these developments are reshaping the international security order.

Governance Gap, Attribution Problem, and the Future of Cyber Deterrence

The effects of AI in the field of cyber security are often evaluated through the increase in technical capacity. However, the real importance of this technology in terms of international security stems from the difficulty of existing governance mechanisms in adapting to the new dynamics created by AI-supported cyber operations. In other words, the main problem we face today is not the technological progress itself, but the inability of the legal, institutional and normative framework to regulate this progress to develop at the same pace. This situation creates a "governance gap" that is getting deeper.

Cyberspace is an environment that inherently extends beyond national borders and in which numerous non-state actors operate. AI makes this structure even more complex. Today, not only governments but also technology companies, organized crime organizations, private security firms, open source developer communities, and individual actors can access AI-based tools and use them for different purposes. In such an environment, it is becoming increasingly difficult to ensure security only with state-centered approaches. Cybersecurity is no longer just a military or technical issue, but a multidimensional security area at the intersection of public policy, international law, private sector management, and digital governance.

One of the most important consequences of AI-supported cyber operations is that it further complicates the citation problem, which has been one of the main problems of cyber security literature for many years. It is already technically and politically difficult to determine the exact identity of the attacker in cyber attacks. Attacks are routed through servers located in

different countries, using third-party infrastructure, or conducted through proxy actors, making it difficult to determine responsibility. AI takes this uncertainty to a new level. Adaptive malware, attack systems that can make automatic decisions, and algorithms that can generate synthetic digital traces can make it possible to deliberately hide the source of the attack or produce false evidence that makes different actors look guilty. This situation directly affects not only technical analysis processes but also political decision-making mechanisms.

The deepening of the citation problem has important consequences in terms of cyber deterrence. The classical understanding of deterrence is based on the ability to identify the potential attacker, increase the cost of the attack, and provide a reliable response when necessary. Yet, when there is a high level of uncertainty about the perpetrator of the attack, the credibility of the threat of retaliation weakens and the deterrence mechanism loses its effectiveness. The speed, automation, and anonymity provided by AI-powered cyber operations make this issue even more pronounced. States are often forced to make political decisions without being able to definitively identify the actor behind the attack, which can lead to either unnecessarily harsh reactions or passive approaches that weaken deterrence.

More importantly, the increasing use of AI in decision support systems poses new risks in terms of crisis management. Today, many governments use AI-based analysis systems in the detection, prioritization and evaluation processes of cyber threats. Although these systems are capable of processing large amounts of data in a short amount of time, algorithmic errors, incomplete data sets, or deliberate manipulations can result in inaccurate threat assessments. Especially in times of international crisis, the unquestioned acceptance of an erroneous warning generated by AI by human decision-makers can increase the risk of miscalculation. In such a scenario, the issue is not merely a technical error but a vulnerability that could directly impact strategic stability.

For this reason, cyber security discussions in the age of AI cannot be carried out only on attack and defense capacity. The real issue is how to develop the institutional and normative capacity to manage the effects of AI on the international security architecture. Today, although the rules of international law regulating the behavior of states, norm development studies carried out within the United Nations, and various regional initiatives are important steps, they are far from comprehensively solving the problems posed by AI-supported cyber operations. In particular, issues such as algorithmic responsibility, accountability of AI

systems, the limits of autonomous cyber operations, and the role of the private sector in international security remain significantly unclear.

Therefore, maintaining strategic stability in the age of AI is not only possible by developing more advanced defense technologies. At the same time, it is necessary to strengthen confidence-building measures between states, establish common norms, develop information sharing mechanisms, and institutionalize multi-stakeholder governance models involving the private sector. Otherwise, the gap between technological developments and governance capacity will gradually widen, which will deepen the uncertainty in cyberspace instead of reducing it. The main challenge faced in the age of AI-supported cyber security is not to achieve technological superiority, but to manage technological transformation with common rules and institutions that will support international stability.

The Future of Cybersecurity in the Age of AI: Bridging the Governance Gap

While AI-powered cybersecurity discussions focus on the pace of technological innovations, they often push the institutional and political consequences of this transformation to the background. However, the factor that will be decisive in terms of international security is not how much AI will develop, but within the framework of which rules, principles and governance mechanisms this technology will be used. The main problem experienced today is that technological capacity has surpassed international governance capacity. Therefore, the top priority of the coming period is to develop an inclusive and applicable governance framework that will reduce the risks posed by AI-powered cyber operations.

The first element of such a framework is the updating of international norms. While the principles developed to date regarding responsible state behavior in cyberspace provide an important foundation, they fall short of covering new problem areas such as the autonomy of AI-powered systems, algorithmic decision-making processes, and synthetic content generation. In particular, clearer international principles need to be developed regarding the conditions under which states will assume responsibility in AI-based cyber operations, the legal nature of AI-supported decisions, and the limits of autonomous attacks on critical infrastructure. In this context, rather than a new and comprehensive international treaty, updating the existing normative framework according to the needs of the AI age seems to be a more realistic and feasible approach.

Secondly, it is inevitable to strengthen the understanding of multi-stakeholder governance. Technology companies, cloud service providers, cybersecurity firms, and open-source software communities play critical roles in the development and operation of AI technologies. Therefore, the future of cyber security cannot be shaped solely by diplomatic negotiations between states. Multi-stakeholder mechanisms that increase information sharing between public institutions, the private sector, academia and civil society, develop common standards and ensure coordination in times of crisis will be one of the basic elements of security in the age of AI.

Third, the international community needs to expand confidence-building measures to include the AI dimension. Communication channels and crisis management mechanisms similar to those developed in the nuclear field during the Cold War are becoming increasingly important for cyberspace. Especially considering the potential of AI-powered cyber operations to lead to misunderstandings, misattribution, or involuntary escalation, communication channels that enable rapid information sharing between states, joint white review processes, and crisis management protocols can contribute to maintaining strategic stability.

In addition, the security of AI systems should become an integral part of cybersecurity discussions. While today's attention is largely focused on how AI is used in cybersecurity, AI systems themselves are exposed to various cyber threats, including data poisoning, model manipulation, prompt injection, and model theft. For this reason, in the future, the "cyber security of AI" approach will become one of the basic components of national security strategies as well as "cyber security with AI".

Lastly, policymakers need to adopt a balanced approach between technological optimism and security concerns. AI is an important technology that, when used correctly, strengthens cyber defenses, increases the resilience of critical infrastructures, and enables public institutions to respond faster to threats. However, the same technology can increase the impact of cyberattacks, make disinformation more convincing, and complicate the management of international crises if adequate control mechanisms are not established. Therefore, the main purpose of security policies should not be to limit the use of AI, but to ensure that this use takes place in accordance with the principles of transparency, accountability, human control and international law.

Conclusion

AI is not only a technology that develops new tools in the field of cybersecurity but is also at the cent**re** of a structural transformation that is reshaping the functioning of international security, the distribution of power and the dynamics of strategic stability. The most distinctive feature of this transformation is that it makes cyber operations faster, more scalable, and more autonomous, while at the same time increasing uncertainty. In particular, the deepening of the attribution problem, the increasing influence of algorithmic systems in decision-making processes, and the ease of access to advanced AI tools by non-state actors necessitate a re-evaluation of existing security approaches.

The biggest challenge posed by AI for international security is not the technology itself, but the growing mismatch between technology and governance capacity. In other words, the main problem of today is not a "technology gap", but a "governance gap". If this gap cannot be closed, AI may become a factor that increases strategic uncertainty and weakens international stability, rather than a tool that strengthens cybersecurity.

Therefore, success in the age of AI will be possible not only by producing more advanced algorithms, but also by developing common norms that will guide the use of these algorithms, strengthening international cooperation, and integrating technological innovations with a governance approach that prioritizes human safety. The future of cyberspace will largely depend on the ability of the international community to manage this capacity within the framework of common rules and shared responsibility, rather than the technical capacity of AI.