DISCUSSION PAPER

AI Regulation in Türkiye: Bringing International Laws into the Discussion

Şeymanur Yönt

TRT WORLD research centre

DISCUSSION PAPER

AI Regulation in Türkiye:
Bringing International Laws into the Discussion

Şeymanur Yönt

TRT WORLD research centre

WRITTEN BY

Şeymanur Yönt

PUBLISHER

TRT TRAINING AND RESEARCH DEPARTMENT

January 2025

TRT TRAINING AND RESEARCH DEPARTMENT

AHMET ADNAN SAYGUN STREET NO:83 34347

ULUS, BEŞİKTAŞ

İSTANBUL / TÜRKİYE

TRT WORLD LONDON

PORTLAND HOUSE

4 GREAT PORTLAND STREET NO:4

LONDON / UNITED KINGDOM

TRT WORLD WASHINGTON D.C.

1819 L STREET NW SUITE 700 20036

WASHINGTON DC

researchcentre.trtworld.com

Introduction:
Incorporating International Cyberlaws and AI-Specific International Treaties

The growing prominence of AI underscores the need for enhanced regulations across various domains, including data privacy and international law, to effectively address AI-specific challenges. Another critical area in need of stronger regulation is cyberlaw, which encompasses e-commerce, digital privacy, and cybercrimes. While previous papers of this series have addressed e-commerce, privacy regulations, and AI legislation in Türkiye, this paper focuses specifically on the cybersecurity dimension of cyberlaws. As the third instalment in a broader series on AI regulation in Türkiye, this discussion will explore how to effectively regulate the cybersecurity aspects of AI within the Turkish context.

Cyber Security Week Opening and International Cyber Warfare and Security Conference' was organised. Former President of the Secretariat of Defence Industries, İsmail Demir, attended the conference and made a speech. (Aytaç Ünal - Anadolu Agency)

1. Türkiye's Current Regulatory Context for AI and Cyberlaws

Türkiye's legal framework on cybersecurity, with its data protection, intellectual property, and criminal laws, provides a foundation for AI regulation. For example, Türkiye's Turkish Penal Code (TCK) criminalises certain activities like unauthorised access to information systems (Turkish Penal Code, 2004, Article 243) and distorting, destroying, altering and rendering inaccessible the data in the information system (Turkish Penal Code, 2004, Article 244), which can also apply to AI-driven cybercrimes such as AI-generated phishing and deepfake attacks. Similarly, the Turkish Penal Code also criminalises when AI systems are exclusively developed or used to commit certain crimes, including data breaches, fraud, or unauthorised access (Turkish Penal Code, 2004, Article 245/A). Moreover, the Anti-Terror Law stipulates that these offences (Articles 243 and 244 of the Turkish Penal Code) will be considered acts of terrorism if committed within the scope of activities of a terrorist organisation (Anti-Terror Law, 1991, Article 4). Thus, it is acknowledged by the Turkish legislature that cyberspace can serve as a domain for terrorist activities (Karasoy & Babaoğlu).

On the other hand, the Law on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting (No. 5651) governs the Internet, including regulating the criminal liability of Internet actors, access restriction procedures for certain crimes, and Internet surveillance. Türkiye has also taken proactive steps to combat cybercrime through action plans and establishing dedicated institutions. Between 2006 and 2010, the Information Society Strategy Action Plan set an objective to establish a "Computer Emergency Response Team (CERT)" to address cyber threats, an initiative implemented by TÜBİTAK-UEKAE under the name TR-BOME (State Planning Organisation, 2006).

The 2013-2014 National Cybersecurity Strategy and Action Plan marked a significant milestone as the first document in Türkiye solely focused on cybersecurity. It identified Türkiye-specific risks, such as low cybersecurity awareness among senior executives and insufficient human resources (Turkish Ministry of Transport, Maritime Affairs and Communications, 2013, paras 5, 8, 18). Furthermore, the establishment of the National Cyber Incident Response Centre (USOM) within the now-defunct TİB was envisaged, and the creation of Cyber Incident Response Teams (SOMEs) to support both the public and private sectors was also foreseen (Turkish Ministry of Transport, Maritime Affairs and Communications, 2013, p. 19). While these laws and plans do not explicitly set rules for AI, they apply to crimes involving AI systems, particularly when such systems are used to perpetrate or facilitate cyberattacks or data misuse and foresee measures to prevent misuse of AI in that regard.

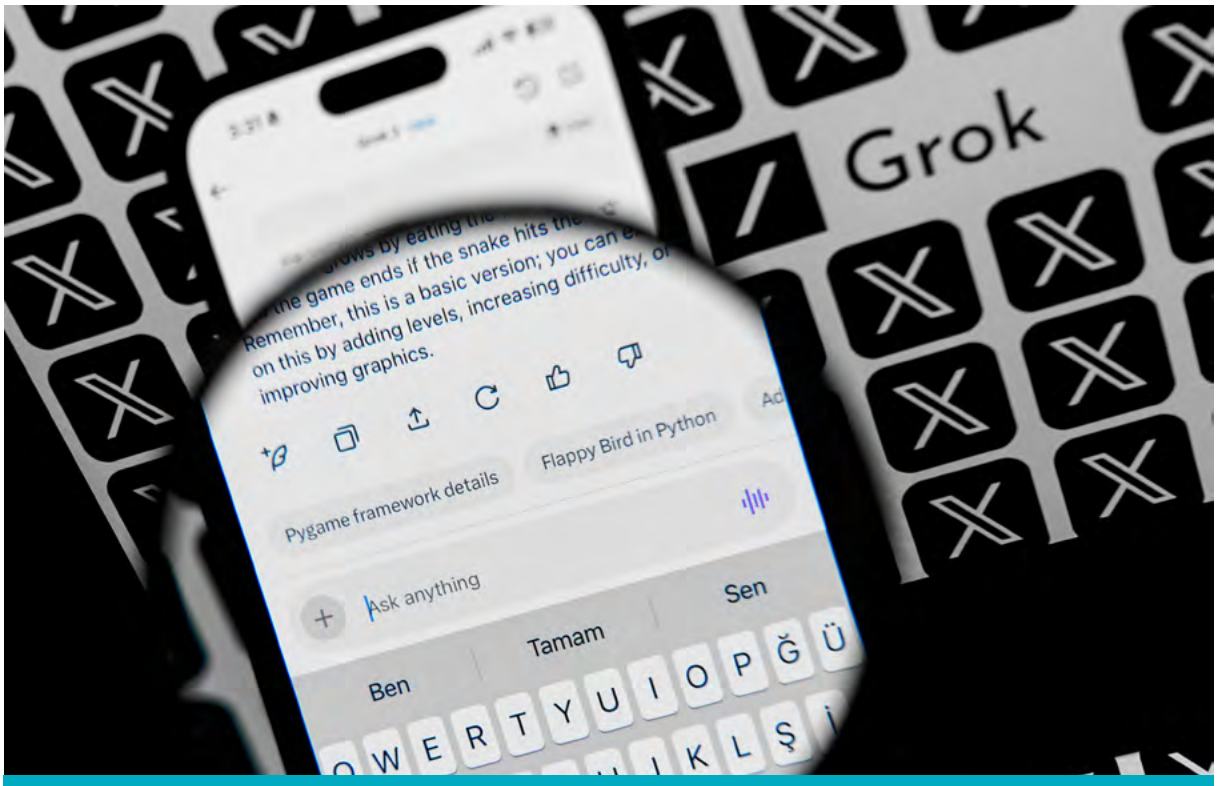
However, they often fail to comprehensively address the unique challenges posed by AI. AI falls under the scope of cyberlaws either via AI systems' facilitation of crimes or through crimes committed directly by AI systems. In this context, existing laws generally address AI-facilitated crimes, offenses where AI used as a tool to commit the crime. For example, Article 245/A of the Turkish Penal Code (TCK) explicitly criminalises the design or use of AI systems for unlawful purposes; highlighting how AI can be employed to execute or enhance criminal activities. However, even in addressing AI-facilitated crimes, there are significant shortcomings. For instance, TCK Article 245/A does not apply when AI systems generally developed for broad, legitimate purposes are occasionally used for unlawful acts.

On the other hand, AI-committed crimes refer to offenses carried out autonomously by AI systems without direct human involvement—such as an AI program automatically breaking passwords, bypassing security systems, or spreading malware. The current legal framework largely fails to address the issue of liability in such scenarios, leaving a significant gap in regulating accountability for harm caused directly by autonomous AI actions. Under Turkish law, the concept of criminal liability is traditionally based on human intent and actions, leaving a significant gap in addressing offences committed autonomously by AI systems. This gap can be addressed by considering the criminal liability of the AI programmer or user. However, it remains unclear under which circumstances these individuals would be held liable—whether under strict liability or fault-based liability, and whether the offence would be considered intentional or negligent. On the other hand, recognising AI as a legal entity would subject it to security measures applicable to legal entities that are subject to criminal penalties. However, this regime does not exist under Turkish law.

In practical terms, cyber attackers increasingly use more advanced tactics, employing malicious software, dark websites, and other tools enhanced by generative AI (Ning & Wu, n.d.). Moreover, attackers can now leverage generative AI to replicate legitimate traffic patterns, allowing them to bypass detection by security systems (Ning & Wu, n.d.). Given that the TCK and other relevant laws do not provide a framework for addressing or punishing the misuse of AI systems, significant gaps remain in ensuring security and ethical use. These gaps extend to assigning accountability when autonomous AI systems cause harm, breach cybersecurity protocols, infringe intellectual property rights, or perpetuate discrimination through biased algorithms. To address these challenges, Türkiye should seek guidance from international laws to develop a more comprehensive regulatory framework.

2. The Role of International Cyberlaws in AI Regulation

International laws, including those related to state responsibility and international humanitarian laws, already serve as a starting point for regulating cyberspace in Türkiye and provide specific rules and overarching principles on cybersecurity. These laws apply to cyberattacks by states while upholding states' national sovereignty, as well as supply critical tools for minimising AI-related risks, such as data breaches, malicious algorithms, and state-sponsored cyber operations. For instance, the Budapest Convention on Cybercrime, a binding agreement to which Türkiye is among 76 signatories, acts as a framework for countries to create their own cybercrime laws (Council of Europe, 2024). The Convention outlines offences such as unauthorised access, interference with data and systems, computer-related fraud, acts amounting to racism and xenophobia, as well as child pornography, and grants



(Dilara İrem Sancar - Anadolu Agency)

procedural tools to investigate cybercrime (Council of Europe, 2024). Addressing these offences, the Convention lays the framework relevant to AI systems, particularly when such systems involve unauthorised access, data interference, or other cybercrimes.

The Convention primarily serves as a binding framework, providing recommendations on the types of laws states should adopt rather than establishing directly enforceable rules. By providing guidance instead of setting forth solid rules, the Convention allows countries to adopt legislation tailored to their specific needs, such as those in consideration in their legal systems. While this approach is advantageous in addressing country-specific needs, it can result in inconsistencies across jurisdictions due to countries' different legal traditions, cultural aspects, and historical factors (Clough, 2014, p. 701). Different interpretations could complicate cooperation, which is critically important in the fight against cybercrimes because of cybercrimes' extraterritorial nature (Aldoori, 2020, p. 11).

Moreover, while the Convention provides a robust foundation, it fails to address emerging challenges posed by AI technologies. The Convention's technology-neutral approach ensures a broad application to various cybercrimes, including AI-related ones. For example, it covers AI-facilitated system interference and misuse of devices. However, the Convention fails to address crimes committed by AI through AI's ability to adapt and learn autonomously. For instance, the Convention does not apply to AI systems that autonomously generate deepfake videos for disinformation campaigns or to AI-powered malware that evolves to bypass traditional cybersecurity measures, thereby increasing the scale and complexity of cyberattacks.

The Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) is another source addressing the most severe cyber operations—those that constitute the use of force, justify a state's right to self-defence, or occur during armed conflict. While the Tallinn Manual offers a comprehensive examination of such scenarios, it is a non-binding academic source exploring existing international cyber warfare laws. This includes interconnected legal domains, such as state responsibility, which addresses a nation's obligation to prevent harmful activities originating from its territory, and humanitarian law, which governs the ethical implications and regulations of AI applications in conflict scenarios, such as autonomous weapons (Schmitt, 2017), which are already binding for Türkiye and to which Türkiye is under an obligation to respect to them. However, the Manual's scope is limited to situations involving the use of force and operations occurring within or above the threshold of armed conflict (Adams, 2017). As a result, it falls short of providing direct guidance for situations that do not involve state participation or that occur below the threshold of armed conflict.

While the Tallinn Manual focuses on certain state-centric cyber operations, the UN provides a broader framework addressing both state and non-state actors. The United Nations, with its committees, expert groups, and bodies such as the Security Council, actively works on cybersecurity. Maintaining the focus on preserving international peace and security, the UN provides valuable guidance on applying international law to cyber operations, focusing on principles such as sovereignty, state responsibility, and the peaceful settlement of disputes in cyberspace. While most of the UN reports and resolutions on the issue are non-binding, they outline norms and rules for responsible state behaviour, emphasising the applicability of international law, including the UN Charter, to cyber activities. Their scope covers critical areas like preventing cyber operations against essential infrastructure, ensuring supply chain security, and fostering international cooperation to combat cybercrime. For instance, the 2021 report of the Group of Governmental Experts, recognising the emerging technologies and associated vulnerabilities, sets norms such as avoiding harm to critical infrastructure, ensuring the integrity of supply chains, and preventing the exploitation of information and communication technology vulnerabilities through responsible disclosure (UN General Assembly, 2021). Moreover, UN General Assembly Resolution 73/27 emphasises the importance of preventing the misuse of information and communication technologies (ICTs) for criminal purposes, which can be extended to address AI-driven cybercrimes (UN General Assembly, 2018). Resolution 64/211, on the other hand, guides nations by introducing a self-assessment tool, helping them determine stakeholder roles and responsibilities (UN General Assembly, 2009).

Türkiye could draw from these resolutions to develop policies ensuring the ethical use of AI in cyberspace and preventing its exploitation for malicious purposes, such as automated phishing or AI-enhanced malware attacks. It could also prevent its territory from being knowingly used for international wrongful acts through ICTs (UN General Assembly, 2018, 1.3). Additionally, these resolutions often encourage international cooperation, providing a platform for Türkiye to engage with other nations in establishing shared norms and best practices for AI governance in cybersecurity.

3. Challenges in Integrating International Laws into Türkiye's AI Framework

Integrating international laws into Türkiye's AI framework presents challenges, particularly in navigating cyberspace regulations' legal, political, and technical complexities. One of the key obstacles is the need for skilled personnel who understand the intricacies of applying international law to AI and cybersecurity (Hollis, 2021). As also recognised by the 2013-2014 National Cybersecurity Strategy and Action Plan (Turkish Ministry of Transport, Maritime Affairs and Communications, 2013, paras 5, 8, 18), Türkiye must invest in educating and training experts capable of addressing these issues to translate international norms and standards into domestic law effectively. Türkiye has already taken several steps in this regard, including the National Cybersecurity Strategy and Action Plan (2020-2023), which aims to contribute to increasing the country's trained human resources and competency levels through practical cybersecurity training in both online and laboratory settings (Ministry of Transport and Infrastructure, 2024, p. 14), as well as the National Cybersecurity Strategy and Action Plan (2016-2019), which involved activities such as training, camps, and competitions to develop the necessary human resources for the country (Ministry of Transport and Infrastructure, 2024, p. 12). By establishing the Cybersecurity Agency, Türkiye further proved that it is on track to bring together and raise experts to determine cybersecurity policies, draft action plans, and carry on legislative activities (Tufan, 2025). As set out by the Presidential Decree (2025), the Cybersecurity Agency will develop policies, strategies, and goals, create action plans, and coordinate relevant activities. Additionally, it is expected that the Agency will enhance awareness through training, foster collaboration between the public, private sector, and universities, and promote the development of indigenous and national products and technologies in the cybersecurity field. Advancing these efforts by appointing qualified individuals to facilitate collaboration between the private sector and the government will enable Türkiye to overcome this challenge.

International law's integration into Türkiye's AI Framework is further complicated by the fact that international law, while guiding state conduct, does not hold exclusive authority over cyberspace regulation (Hollis, 2021). The involvement of non-state actors, such as industry players and civil society, complicates the application of international law, as alternative regulatory mechanisms like industry self-regulation often take precedence in cyberspace. To overcome this challenge, developing cybersecurity standards, adopting a multi-stakeholder model involving regular consultations between government bodies, industry players, and civil society groups in cybersecurity incidents, establishing a market oversight and regulatory authority for cybersecurity, and harmonising sector-specific cybersecurity regulations would be effective measures (Kaya, 2025).

Another significant challenge lies in the ambiguous interpretation of international legal principles such as non-intervention, sovereignty, and human rights when applied to AI and cyberspace (Hollis, 2021). International law traditionally governs the actions of states, primarily focusing on state responsibility in international relations. However, its application becomes less clear when regulating non-state actors, such as individuals or private companies, who are generally subject to domestic legal systems. This creates a grey area regarding accountability, particularly when actions involving AI systems cross borders or occur in a digital space without clear jurisdiction. For example, AI technologies developed in one country may be used in another, raising questions about the scope of state responsibility and enforcement of international law.

To address these issues, Türkiye could work towards clearer definitions in national legislation regarding the roles and responsibilities of AI developers, operators, and users. This might include specifying the legal obligations of AI developers to ensure compliance with international human rights standards or establishing frameworks for cross-border cooperation in regulating AI-driven activities. Additionally, Türkiye could seek international cooperation through treaties or agreements to ensure that the responsibilities of non-state actors in cyberspace are consistently addressed across jurisdictions. Clarifying these responsibilities in both national and international contexts will be crucial to ensure the effective

implementation of international law in cyberspace and AI regulation.

Finally, the regulation of cyberspace faces significant challenges due to deep ideological divides between key global actors, particularly Russia and the United States. Russia advocates for creating a comprehensive treaty to govern cyber warfare, believing that a structured, legally binding agreement is essential for maintaining international peace and security. In contrast, the US and the EU are wary of such a treaty, fearing that it could potentially be used to restrict freedom of information and limit democratic values on the Internet (Henderson, 2015). These conflicting positions complicate the development of a unified international legal framework, as there is no consensus on whether existing international laws are sufficient or whether new, specific regulations are required. Russia, China, and other nations argue for a multilateral governance system for cyberspace, while the US maintains that existing international laws, particularly those governing jus ad bellum and jus in bello, are adequate to address cyber threats.

This ongoing disagreement makes it difficult to establish consistent global norms for cyberspace, presenting a significant challenge for Türkiye in integrating international law into its national AI framework. As Türkiye seeks to align its AI regulations with international standards, the lack of consensus on key issues—such as the governance of cyber threats and the role of state sovereignty in cyberspace—creates uncertainty and fragmentation. To address this, Türkiye could actively participate in international dialogues and multilateral forums to advocate for a balanced approach accommodating diverse perspectives. Fostering regional partnerships and bilateral agreements can also help Türkiye establish cooperative mechanisms for addressing cross-border cyber and AI-related challenges while aligning with evolving global norms.

'Cyber security training' has been added to the products and services exported by the Turkish defence industry. Providing cyber security training to public and private sector managers in Kazakhstan, STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. made its first export in this field. In line with the cooperation agreement signed with the Kazakhstan Ministry of Defence and Aerospace Industry, it is aimed to establish a similar Cyber Fusion Centre in this country and to expand cooperation through cyber security competitions. (Aytaç Ünal - Anadolu Agency)

4. Incorporating International Frameworks into Turkish AI Regulation

Türkiye's efforts to develop robust AI-specific legislation targeting cybercrimes must be complemented by a strong commitment to integrating international frameworks into its regulatory landscape. A critical first step is reinforcing Türkiye's adherence to global cybersecurity norms through the comprehensive implementation of the Budapest Convention on Cybercrime, which Türkiye has ratified. While the Convention is already applicable in Türkiye and Türkiye already aligns with many international cybersecurity standards, further harmonisation of its domestic laws with the Convention's principles is essential. This includes enacting more detailed regulations, particularly in enforcement, targeting key cybercrimes such as cyber-enabled fraud, and focusing on identifying and prosecuting offenders. It also involves fortifying the legal framework for protecting critical infrastructure from cyber-attacks. For these purposes, severe penal provisions can be introduced for cyber fraud and infrastructure attacks, with clearer criminal sanctions for offenders. Additionally, special monitoring mechanisms such as enhanced digital forensics teams, real-time threat detection systems, and international cooperation frameworks for cross-border cybercrime can be established to facilitate the tracking of cybercrimes.

More than that, Turkish legislation should build upon and go beyond the Convention by developing comprehensive regulations that explicitly address the criminal use of AI technologies. These regulations should include penalties for deploying general-use AI in cyberattacks, creating or spreading harmful AI-generated content, and other AI-related cybercrimes. Additionally, it is essential to establish accountability mechanisms that clearly define the roles and responsibilities of AI system developers, users, and intermediaries, thereby ensuring transparency and oversight in AI deployment. To mitigate risks, mandatory risk assessments and audits should be required for high-risk AI systems, particularly those operating in critical infrastructure or cybersecurity-sensitive areas. Furthermore, given the extraterritorial nature of AI-related cybercrimes, Turkish legislation must align with international best practices and promote cross-border cooperation in enforcement and information sharing. By going beyond the Convention's technology-neutral framework by setting specific provisions on AI and cybercrimes, Türkiye can effectively address the unique challenges posed by AI technologies and close existing regulatory gaps.

Türkiye's recently proposed cybersecurity law represents a significant milestone in this regard. The proposal introduces clear definitions for critical terms such as "cybersecurity," "cyber threats," "cyber incidents," "critical infrastructure," and "vulnerabilities" (Yılmaz, 2025). Moreover, as a framework law, the proposal sets forth principles such as accountability to regulate cyberspace and determines the responsibilities of the relevant state institutions. These foundational principles go beyond the Budapest Convention scope by introducing standardisation and certification processes (Cybersecurity Law Proposal, 2025) to ensure preventative, by-design protection. However, as the proposal serves as a framework law, it does not provide detailed rules on offences, penalties, or preventive measures. Therefore, Turkish legislation should take the framework law as a starting point and introduce detailed regulations addressing AI-facilitated or AI-committed cybercrimes.

Tallinn Manual, on the other hand, even though a non-binding scholarly document, can serve as a valuable reference for Türkiye in regulating cyberlaws. To address scenarios below the threshold of armed conflict, incidents that do not constitute a conflict, or those that do not involve states, Türkiye could adopt principles from international frameworks designed for armed conflict by analogy. This would enable the development of regulations covering a broader spectrum of cyber operations, including those involving non-state actors or actions falling outside the traditional definitions of conflict. For instance, the Tallinn Manual emphasises that a cyber act can be considered internationally wrongful even without causing physical damage or injury (Jensen, 2017). In line with this thinking, Türkiye could establish legal provisions to penalise wrongful acts such as the unauthorised manipulation or exploitation of AI systems regardless of their tangible outcomes. To implement this, Türkiye could introduce a

specific legal framework within the Turkish Penal Code that categorises the unauthorised manipulation or exploitation of AI systems as a distinct criminal offense. This could include defining the act, outlining penalties such as fines or imprisonment based on the severity of the manipulation, and establishing clear guidelines for AI system developers and users on their legal responsibilities regarding the security and integrity of these systems. Moreover, the Manual's discussion of due diligence—requiring states to prevent their territory from being used for harmful cyber operations—can inform Türkiye's policies for cross-border cooperation and the development of bilateral or multilateral agreements on cybersecurity. Accordingly, Türkiye can introduce a due diligence requirement by mandating that all entities operating within its borders implement robust cybersecurity measures, report cyber incidents promptly, and cooperate with international law enforcement to prevent the use of its territory for launching or facilitating cyber attacks.

Finally, under the UN framework, including the UN Charter and relevant UN Security Council resolutions, Türkiye is already bound by obligations to prevent harmful activities originating from its jurisdiction. Therefore, there is no immediate need for Türkiye to enact additional domestic legislation to recognise these obligations. However, to ensure stronger compliance, Türkiye could introduce measures to enhance deterrence. In the context of international law, while the matter remains debated, there is an accepted view that states have an obligation to prevent activities within their territory that cause harm to other states, including within the realm of cyber law (Moynihan, 2019, para. 74). This perspective is reflected in Rule 6 of the Tallinn Manual 2.0, which states: 'A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.' (Schmitt, 2017). Building on this framework, Türkiye should adopt specific measures to prevent, penalise, and deter AI-facilitated and AI-committed cyberattacks, bolstering its efforts to fulfil its international obligations and effectively address emerging cybersecurity threats. This could be achieved by expanding the mandate of Türkiye's National Cybersecurity Council to include a dedicated focus on AI-driven cyber threats, allowing the task force to develop specialised strategies, monitor AI-related vulnerabilities, and enhance international cooperation in combating AI-enabled cybercrime. Moreover, Türkiye can implement a national AI cybersecurity framework that outlines specific protocols for identifying, reporting, and mitigating AI-driven cyber threats, ensuring a coordinated response across all relevant sectors. Finally, Türkiye could establish a subunit under the Department of Combating Cybercrime specifically aimed at detecting and investigating AI-driven cyber threats. This could include developing specialized AI tools for crime detection and enhancing the capacity of law enforcement to identify new AI-based criminal methods.

Conclusion

While Türkiye's existing legal framework provides a foundational approach to regulating AI in the context of cybersecurity, significant gaps remain. These gaps primarily concern the liability of AI systems themselves and the extent to which criminal responsibility can be assigned when autonomous AI systems engage in illegal activities. As cyberattacks increasingly leverage generative AI, these legislative gaps pose a threat to cybersecurity, as current laws fail to provide adequate mechanisms for accountability and ethical use. International law proves to be beneficial for Türkiye in addressing these gaps.

Integrating international laws into Türkiye's AI framework offers both opportunities and challenges. While international conventions such as the Budapest Convention and the UN General Assembly Resolutions offer critical guidance on regulating cybercrimes, their technology-neutral approach leaves room for ambiguity regarding AI-driven offences. Türkiye can benefit from aligning its laws with these international standards, yet challenges arise from the complexities of cross-border regulation, the role of non-state actors, and the unclear application of international legal principles to AI. Addressing these issues requires Türkiye to invest in human resource development, improve legal clarity, and collaborate internationally to establish more robust cybersecurity policies. By bridging the gaps between national laws and international frameworks, Türkiye can better address the emerging risks posed by AI in cyberspace, ensuring national security and AI technologies' ethical use.

References

Aldoori, A. (2020). *Uluslararası hukukta siber suçla mücadele* [Master's thesis, Istanbul University]. Istanbul University Repository. https://nek.istanbul.edu.tr/ekos/TEZ/ET002065.pdf

Adams, M. J. (2017, January 4). A warning about Tallinn 2.0 … whatever it says. *Lawfare*. https://www.lawfaremedia.org/article/warning-about-tallinn-20-%E2%80%A6-whatever-it-says

Anti-Terror Law, Law No. 3713, Republic of Türkiye § 243-244 (1991). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=3713&MevzuatTur=1&MevzuatTertip=5

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. *Monash University Law Review, 40*(3), 698-736. Monash University Faculty of Law Legal Studies Research Paper No. 2015/06. https://ssrn.com/abstract=2615789

Council of Europe. (2024). *Joining the Convention on Cybercrime: Benefits*. https://rm.coe.int/cyber-buda-benefits-2024-july-2789-5929-5498-v-1/1680b0d659

Cybersecurity Law Proposal, Proposal No. 82, Grand National Assembly of Türkiye (2025, January 10). https://cdn.tbmm.gov.tr/KKBSPublicFile/D28/Y3/T2/WebOnergeMetni/6d-9ba10d-9be6-4838-b58f-5d9d06080ff9.pdf

Henderson, C. (2015). The United Nations and the regulation of cyber-security. In *Research handbook on international law and cyberspace* (pp. 465-490). Edward Elgar Publishing. https://ideas.repec.org/h/elg/eechap/15436_22.html

Hollis, D. B. (2021, June 14). A brief primer on international law and cyberspace. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/posts/2021/06/a-brief-primer-on-international-law-and-cyberspace?lang=en

Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and insights. *Georgetown Journal of International Law, 48*(3), 735–756. BYU Law Research Paper No. 17-10. https://ssrn.com/abstract=2932110

Karasoy, H. A., & Babaoğlu, P. (2021). Türkiye'de siber güvenlik: Yasal ve kurumsal altyapı. *Yasama Dergisi* (*44*), 123-155. https://dergipark.org.tr/tr/pub/yasamadergisi/issue/68393/1005110

Kaya, M. B. (2025, January 9). *Siber güvenlik başkanlığı nihayet kuruldu* [LinkedIn post]. LinkedIn. https://www.linkedin.com/posts/mehmet-bedii-kaya_siber-g%C3%BCvenlik-ba%C5%9Fkanl%C4%B1%C4%9F%C4%B1-nihayet-kuruldu-activity-7282590136003874816-J-nd/?utm_source=share&utm_medium=member_desktop

Ministry of Transport and Infrastructure. (2024). *National Cybersecurity Strategy and Action Plan 2024-2028*. https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf

Ministry of Transport, Maritime Affairs and Communications. (2013, January). *National Cybersecurity Strategy and 2013-2014 Action Plan*. https://afyonluoglu.org/PublicWebFiles/Reports-TR/2013-2014%20Ulusal%20Siber%20G%C3%BCvenlik%20Stratejisi%20ve%20Eylem%20Plan%C4%B1.pdf

Moynihan, H. (2019). *The application of international law to state cyberattacks: Sovereignty and non-intervention*. Chatham House. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace

Ning, S., & Wu, H. (n.d.). *Generative AI and cyber risk in China*. ICLG. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/01-generative-ai-and-cyber-risk-in-china

Presidential Decree, Decree No: 77. (2025, January 8). *Official Gazette* (No. 32776). https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. https://doi.org/10.1017/9781316822524

State Planning Organisation. (2006). *Information Society Strategy Action Plan 2006-2010*. https://ms.hmb.gov.tr/uploads/2019/01/Bilgi-Toplumu-Stratejisi-Eylem-Plani-2006-2010.pdf

Turkish Penal Code, Law No. 5237, Official Gazette No. 25611. Republic of Türkiye. (2004). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5

Tufan, S. (2025, January 9). Siber güvenlik başkanlığı kuruldu. *Marketing Türkiye*. https://www.marketingturkiye.com.tr/haberler/siber-guvenlik-baskanligi-kuruldu/

UN General Assembly. (2009). *Resolution 64/211: The rule of law at the national and international levels* (A/RES/64/211). https://undocs.org/A/RES/64/211

UN General Assembly. (2018). *Resolution 73/27: Advancing responsible state behaviour in cyberspace in the context of international security* (A/RES/73/27). https://undocs.org/A/RES/73/27

United Nations General Assembly. (2021, July 14). *Group of governmental experts on advancing responsible state behaviour in cyberspace in the context of international security* (A/76/135). https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

Yılmaz, A. (2025, January 10). Siber güvenlik kanunu teklifi TBMM'de. *Anadolu Agency*. https://www.aa.com.tr/tr/gundem/siber-guvenlik-kanunu-teklifi-tbmmde-/3447212

TRT WORLD
research centre

TRTWORLD
research
centre