The Ontology of Cyber Threats: A Comparison of the Cyber Security Law and the EU Framework

This article is the first in a series comparing Turkey's Cyber Security Law No. 7545 (hereinafter referred to as "CSL") with EU cyber security regulations from a legal perspective.

Introduction: The Transformation of Cyber Security in the Digital Age

The internet was a technology designed to facilitate our lives. However today, this network that forms the critical infrastructure of modern society has also become the source of major security vulnerabilities. This paradox forms the foundation of cyber security regulations. More than 15 million data breaches worldwide in 2023 strikingly demonstrate the importance of this issue. Attacks targeting critical infrastructure, ransomware, and nationwide cyber attacks are now among the main concerns not only of technology companies but also of nation-states.

Cyber security legislation has become the defense weapon of countries against these technological threats. However, each country adopts different approaches stemming from its historical, cultural, and institutional structure. This comparative analysis aims to be not only a technical or legal examination but also a philosophical investigation into the ontological basis of cyber security.

Questions such as "What are we protecting?", "What is the threat?", "What is the difference between security and resilience?" will be important for understanding the assumptions underlying different regulatory frameworks.

Cyber Security: Not Just a Technical Problem, a Social Issue

Cyber space attacks are no longer viewed merely as technical threats to computer systems. Both the CSL and EU regulations position cyber security as a fundamental component of social security. However, there are significant philosophical differences between these two approaches.

The question "What is cyber security?" may seem simple, but definitions in legal texts reveal the philosophical assumptions underlying regulatory frameworks. Cyber security is defined in Article 3 of Law No. 7545 as:

> *"Cyber security: The set of activities encompassing the protection of information systems that make up cyber space from attacks, ensuring the confidentiality, integrity, and accessibility of data processed in this environment, detection of attacks and cyber incidents, activation of response and alarm mechanisms against these detections, and restoration to the pre-cyber incident state."*

This definition positions cyber security as a *reactive* defense against attacks, while the EU's NIS2 Directive and Cyber Resilience Act (CRA) approach cyber security with a more *proactive* approach focused on system resilience.

When examining the definition in the CSL, we see that expressions such as "protection from attacks," "detection," "response," and "restoration" stand out. These expressions reflect a reactive understanding that anticipates action after an attack has occurred. This approach positions cyber security within a military defense logic, adopting the metaphor of protecting a fortress targeted by an attacker. Although the term "cyber resilience" appears among the duties of the Presidency in Article 5 of the Law, this concept remains a secondary element, and the law as a whole is based on a reactive security understanding.

EU regulations, on the other hand, center on the concept of resilience. The NIS2 Directive of 2022 aims to increase the cyber resilience of organizations by introducing stricter security requirements to a wider range of sectors. NIS2 mandates not just defense, but proactive measures for organizations to strengthen their digital infrastructures. This approach aims to contribute not only to their own security but to collective cyber resilience across the EU.

This resilience approach is further strengthened by the Critical Entities Resilience Directive (CER). CER requires critical organizations to conduct regular risk assessments (Article 10) and take appropriate and proportional technical and organizational measures to ensure their resilience (Article 11). Organizations must also define these measures in a resilience plan or equivalent document.

The Cyber Resilience Act (CRA) adopts a product-oriented approach, imposing responsibilities on manufacturers with the "security-by-design" principle for products containing digital components. Finally, the Cyber Solidarity Act (Regulation (EU) 2025/38) centers on collective security by creating a system built on three main components: the pan-European Security Operations Center infrastructure (European Cyber Shield), the Cyber Emergency Mechanism, and the European Cyber Security Incident Investigation Mechanism.

To concretize the difference between them, consider this example: In the case of a cyber attack on an energy grid, the CSL approach would primarily focus on identifying the attacker, stopping the attack, and restoring the system to its previous state. The EU approach, however, emphasizes pre-designing resilience measures such as alternative routes, backup systems, and automatic isolation mechanisms so that critical services can continue uninterrupted even if an attack occurs.

The Nature of Cyber Existence: Impact from Technical Infrastructure to Society

The CSL's definition of "cyber space":

> *"Cyber space: The environment consisting of all information systems that are directly or indirectly connected to the internet, electronic communications, or computer networks, and the networks that connect them to each other,"*

This definition views cyber space primarily as a technical infrastructure, while the EU approach treats cyber space as a socio-technical ecosystem. The EU's Cyber Resilience Act conceptualizes cyber space not just as a technical system but as a social environment.

When examining the CSL's definition, it emphasizes the physical and technical components of cyber space (computer networks, information systems, electronic communications). This definition frames cyber space as a form of specific technology and shapes its protection approach largely around technical measures.

The EU's approach, on the other hand, has undergone a significant transformation over time. In its first Cyber Security Strategy in 2013, the EU essentially adopted a risk-based security logic. This strategy emphasized safety alongside security and acknowledged that cyber incidents could come from various sources, including criminal, politically motivated, terrorist or state-sponsored attacks, as well as natural disasters and unintentional errors. This all-hazards approach provided a framework encompassing both antagonistic and non-antagonistic threats and risks.

However, in the 2020 strategy, the EU noticeably shifted toward a threat-based security logic. The new strategy focuses on protecting people, businesses, and institutions from cyber threats rather than creating a secure online environment, and in the introduction section, it only refers to cyber attacks related to malicious targeting. As one expert put it, the EU has moved from an approach focused on ensuring availability and reliability to one focused on actor-oriented threats and active protection.

This change has not only remained at the rhetorical level but has also been institutionalized with concrete institutional changes. The 2020 strategy proposes the creation of a European Cyber Shield to provide technical/operational defense capabilities and a Joint Cyber Unit to send experts/equipment to member states. It also introduces new measures such as a "cyber diplomacy toolbox" for joint EU diplomatic response to malicious cyber activities and an EU cyber deterrence posture to develop attribution capabilities.

Importantly, the EU's 2020 strategy has not completely abandoned the previous risk-based approach but has added a threat-based logic on top of it. Therefore, both approaches currently coexist, but some experts are concerned that the increased focus on antagonistic attacks could divert attention and resources from managing other common causes of cyber incidents, including malfunctions and errors.

Similarly, the NIS2 Directive defines cyber space not just as a structure consisting of networks and information systems, but as a broad social space that includes users of these systems and other individuals affected by cyber incidents.

The Cyber Solidarity Act (CSA) takes this holistic approach even further, emphasizing that cyber security is not solely a government responsibility, but that the private sector also plays a vital role against threats. This approach views cyber space as a collective responsibility area where various actors interact.

The practical consequences of this difference are important. While cyber space is defined in the CSL as an area where elements of national power need to be protected, in EU texts it is addressed together with the economic dimension as part of the digital single market. This difference also shapes the philosophical foundations of measures taken against cyber threats.

While the EU's Cybersecurity Act sets forth a vision of an open, secure, free, and peaceful cyber space, the CSL similarly provides a comprehensive certification framework. In Article 5(ğ) of the CSL, "carrying out testing and certification processes for software, hardware, products, systems, and services related to the cyber security field" is listed among the duties of the Presidency. Article 6 of the Law grants the Presidency the authority to "determine the minimum security criteria for cyber security software, hardware, products, and services" and "manage certification, authorization, and documentation processes." The Law also mandates in Article 7 the use of "products and services authorized and certified by the Presidency" for public institutions and critical infrastructures. Both regulations aim to build trust in the digital ecosystem.

The evolution of EU regulations is also documented by the increasing frequency of terms reflecting threat-based logic and the introduction of new concepts such as deterrence and diplomacy that were not previously found in strategy documents. While these terms are also found in the CSL, the CSL's approach is more focused on protection

at the national level, while the EU's approach offers a more comprehensive strategy coordinated across the European Union.

The underlying idea of the EU's adopted approach is that cyber threats are inherently borderless, and therefore effective defense is only possible through international cooperation. As stated in the EU Commission's cyber security strategy, member states need to develop collective response mechanisms to be greater than the sum of their parts in combating cyber threats. Cyber security is no longer viewed solely as a national issue but as a component of shared sovereignty. This understanding forms the infrastructure of the EU's efforts to develop joint defense capabilities, cyber diplomacy, and deterrence strategies.

Cyber Sovereignty in Turkey's Approach

Another notable feature of the CSL is its definition of cyber space within the sphere of national sovereignty and its treatment within the framework of national power elements. The purpose stated in Article 1 of the law is explained as "detecting and eliminating current and potential threats directed from inside and outside against all elements that constitute the national power of the Republic of Turkey in cyber space."

This approach parallels the concept of cyber sovereignty advocated by countries such as China and Russia in recent years. Cyber sovereignty argues that the internet and digital technologies should be regulated on the basis of national security concerns and state control. This perspective views the internet as an area that can be divided by national borders and suggests that states should have full control over their cyber territories.

This approach of the CSL is concretized especially with the broad powers given to the Cyber Security Presidency. The Presidency has the authority to inspect, regulate, and intervene in almost all critical infrastructures to ensure cyber security, which is defined as an integral part of national security.

Digital Single Market and Cooperation in the EU Approach

While the EU addresses cyber space with an economic dimension, within the framework of the digital single market concept, it also relates it to strategic autonomy and digital leadership goals. In its conclusion declaration adopted in 2021, the EU Council emphasized that cyber security is necessary to build a resilient, green, and digital Europe and especially the importance of achieving strategic autonomy to strengthen the EU's digital leadership.

The EU's approach treats cyber security not only as a factor supporting economic prosperity but also as a holistic issue with security, diplomatic, and geopolitical dimensions. The joint communication published by the European Commission and the

External Relations Service (EEAS) aims to strengthen the EU's capabilities to prevent, deter, and respond to cyber threats. The EU's cyber security approach also includes diplomatic and security dimensions such as the cyber diplomacy toolbox and cyber deterrence posture.

This multifaceted approach shapes the EU's cyber security regulations. Structures such as the EU Cyber Security Agency (ENISA), the Computer Incident Response Teams Network (CSIRTs Network), and the NIS Cooperation Group, as well as new mechanisms proposed by the Council such as the joint cyber unit and the cyber intelligence working group of member states, aim to create a cyber security architecture that transcends national borders.

The EU's digital single market strategy aims to remove virtual borders and facilitate consumer access to cross-border online content across European industry. The main goal of this strategy was harmonization instead of fragmentation. With the Cybersecurity Act, the EU aims to create a more secure digital space within the EU by establishing a European Cyber Security Certificates framework for products, processes, and services.

The EU's cyber security strategy centers on international cooperation. The EU's aim is to create a global framework for conflict prevention and stability in cyber space. The foundation of this framework lies in a common understanding based on states behaving in cyber space as they do in other areas and applying existing international law. The EU also supports the implementation of cyber security confidence-building measures to reduce the risk of misperception, escalation, and conflict.

The Triple Conceptual Framework: Confidentiality, Integrity, Accessibility

Both the CSL and EU regulations are based on the conceptual triad of confidentiality, integrity, and accessibility, which are the three fundamental elements of cyber security. This triad forms a universal framework for cyber security.[2]

However, we see significant differences in the application of this triad:

- **CSL** addresses this triad from an attack-oriented perspective while
- **EU regulations** position it within a risk management perspective

Origins and Importance of the CIA Triad

The confidentiality, integrity, and availability (CIA) triad is a fundamental paradigm in the field of information security. This conceptual framework, which emerged during the

development of ARPANET security protocols in the late 1970s, forms the basis of almost all cyber security regulations and standards today (ISO 27001, NIST, etc.).

These three concepts define the basic values that information security aims to protect:

1. **Confidentiality**: Information being accessible only to authorized persons
2. **Integrity**: Information not being modified without authorization or accidentally, maintaining its consistency
3. **Availability**: Information being available when needed

This triad provides a universal language for identifying, classifying, and prioritizing cyber security problems. For example, a ransomware attack primarily threatens availability, a data leak threatens confidentiality, and a database manipulation threatens integrity.

Different Implementation Approaches: Attack-Oriented vs. Risk Management

In the CSL's attack-oriented approach, the CIA triad is treated as values targeted by threat actors. The law defines attempts to eliminate these three values and proposes protection mechanisms against them. In this approach, the cyber security problem is primarily framed as an attacker-defender relationship.

In the EU's risk-focused approach, this triple framework is evaluated within a broader spectrum of risks. EU regulations recognize not only deliberate attacks but also system failures, human errors, natural disasters, and other accidental events as threats to these three values. Therefore, the EU approach focuses more on risk assessment, risk mitigation, and risk management processes.

However, it should also be noted that in EU regulations, this triad is applied in a worryingly inconsistent manner.[3] For example, Article 5(1)(f) of the GDPR does not explicitly mention data availability. This situation reflects the coordination difficulties experienced among the EU's numerous regulatory institutions and frameworks.

In recent years, it has been discussed that the CIA triad cannot cover all dimensions of cyber security. Particularly concepts such as privacy, authentication, and non-repudiation are gaining importance in addition to this triad.

Actor-Threat Relationship: Attacker-Oriented and Risk-Oriented Approaches

The CSL addresses cyber threats with an actor-focused approach. Article 3 of the law defines "cyber attack" as follows:

> *"Cyber attack: Operations deliberately carried out against persons or information systems anywhere in cyber space, with the aim of eliminating the confidentiality, integrity, or accessibility of data processed by information systems that make up cyber space,"*

This definition frames cyber threats as the actions of a deliberate attacker. On the other hand, in the EU's 2023 Cyber Resilience Act, threats are positioned more in terms of risks in the system itself - including deliberate attacks as well as accidents and natural disasters.

This difference reflects the distinction between risk-based and threat-based security logics.[4] While Turkey's approach is more threat-based, the EU has adopted an approach that combines both risk and threat logics.

Threat-Based Security: Motivations and Capabilities of Attackers

Threat-based security logic focuses on the identities, motivations, and capabilities of potential attackers. In this approach, the primary task of cyber security is to detect, deter, and neutralize the actions of hostile actors (nation-states, cyber crime organizations, hacktivists, etc.).

The expression "deliberately carried out operations" in Article 3 of the CSL clearly reveals this attacker-oriented perspective. The cyber security problem is fundamentally seen as the conscious and malicious actions of an actor. Therefore, security strategies developed under the CSL take shape around the detection of attackers, attribution of attacks, and deterrent measures against attackers.

This approach can be seen in Turkey's response to the WannaCry ransomware attack in 2017. Turkey's reaction primarily focused on identifying the actors who carried out the attack and on defense measures that could be taken to prevent similar attacks.

Risk-Based Security: System Vulnerabilities and Resilience

Risk-based security logic, on the other hand, focuses on vulnerabilities in the system and potential impacts if these vulnerabilities are exploited, rather than on the intentions and capabilities of attackers. In this approach, the basic question is not "who can attack?" but "what can go wrong?" and "what are the effects of this?"

The EU's NIS2 Directive and CRA place strong emphasis on risk assessment and risk management processes. Under these regulations, organizations are obligated to conduct regular risk assessments, develop risk mitigation plans, and document remaining risks. In the EU approach, cyber incidents can originate not only from deliberate attacks but also from technical failures, software bugs, human errors, natural disasters, or other unexpected events.

The EU's response to the WannaCry attack, in addition to trying to identify those who carried out the attack, focused on increasing the resilience of systems to mitigate the impact of such attacks. Accordingly, the NIS2 Directive was developed to mandate the use of up-to-date software and security patches by companies.

Critical Infrastructure Concept: Cyber Space as Meta-Infrastructure

The CSL defines critical infrastructure as:

> *"Critical infrastructure: Infrastructures hosting information systems that are necessary for national, social, or economic activities to continue and which, if their confidentiality, integrity, or accessibility of the information/data they process is compromised, could lead to loss of life, large-scale economic damage and security vulnerabilities, or disruption of public order,"*

This definition places critical infrastructure in a legal framework in terms of information systems with physical impact potential. The EU approach, on the other hand, more reflects the concept of the critical infrastructure of critical infrastructures - the idea that cyber space is a meta-infrastructure that supports all other critical infrastructures.[5]

Historically, the concept of critical infrastructure primarily referred to physical systems (power plants, dams, bridges, etc.). However, with digital transformation, these infrastructures have increasingly become cyber-physical systems - structures where physical components are intertwined with digital control systems.

The CSL's definition of critical infrastructure bears traces of this transition period. The definition primarily focuses on digital systems with physical effects. Expressions such as "loss of life," "large-scale economic damage," and "disruption of public order" emphasize the physical world impacts of cyber security breaches. This approach essentially positions cyber security as an extension of physical security.

Within this definition framework, the CSL also provides comprehensive standards and certification mechanisms to ensure the security of critical infrastructures. Article 5(g) of the Law assigns the Cyber Security Presidency the duty to "prepare standards related to

the field of cyber security, examine standards prepared by other persons or organizations, give opinions on them, adopt them as standards if deemed appropriate, publish them, and monitor their implementation." Additionally, according to Article 6(1), the Presidency "determines the minimum security criteria for cyber security software, hardware, products, and services" and manages certification processes for compliance with these criteria.

The obligation to comply with these standards is explicitly stated in Article 7(c). According to this provision, "public institutions and organizations, as well as critical infrastructures, are obligated to procure cyber security products, systems, and services from cyber security experts, producers, or companies authorized and certified by the Presidency." Temporary Article 1 imposes an obligation on all organizations operating in the field of cyber security to complete certification and documentation processes.

In the EU's approach, as seen particularly in the relationship between the Critical Entities Resilience Directive and the CRA, cyber space is conceptualized as the critical infrastructure of critical infrastructures. In this perspective, cyber security is viewed as a fundamental infrastructure that supports all other critical infrastructures. All sectors such as energy, transportation, health, and finance are now dependent on digital systems, and the security of these systems is a prerequisite for the security of all other infrastructures.

Although both the CSL and EU regulations offer comprehensive security standards, there is a distinct difference in their philosophical foundations. While the CSL addresses the protection of critical infrastructures from a national security perspective by positioning cyber security as an inseparable part of national security, the EU approach views cyber security as a meta-infrastructure supporting all sectors and evaluates it in the context of economic integration and cross-border cooperation.

From Critical Services to Critical Entities

As a notable development, both the CSL and EU regulations are showing a transformation from the concept of critical infrastructure to the concepts of critical services or critical entities. This transformation reflects the understanding that what needs to be protected is not only physical systems but also the services provided through these systems and their societal functions.

The concept of "critical public service" defined in Article 3(e) of the CSL is an example of this trend:

> *"Critical public service: A service that is necessary for national, social, or economic activities to continue and that, if interrupted or damaged, could have a significant impact on national security, the country's social or economic welfare, public order or health, or the*

> *provision of other services, provided nationwide with monopoly or limited substitution,"*

Similarly, the EU's CER Directive defines the concept of critical entity as entities necessary for the provision of essential services and whose disruption would cause significant societal or economic impacts.

This transformation shows that the understanding of cyber security is evolving from the protection of technical systems to ensuring the sustainability of societal functions. This evolution is also an indication that cyber security is no longer a technical issue but has become a societal and political issue.

Cultural and Social Context Differences

When stating "basic principles" in Article 4 of the CSL, the following statement is included:

> *"Cyber security is an inseparable part of national security."*

This principle directly positions cyber security within the framework of national security. EU regulations, on the other hand, treat cyber security more as a multi-layered issue with economic, social, and political dimensions. The EU's approach can be explained by the concept of the Regulatory Security State - where regulatory authority is used directly as a security tool.[1]

In the CSL's approach, cyber security is evaluated in the same category as other security measures aimed at protecting the existence and integrity of the state. The CSL's establishment of a Cyber Security Board consisting of representatives from security institutions such as the Ministry of Interior, Ministry of National Defense, General Secretariat of the National Security Council, and National Intelligence Organization reflects this perspective.

In the EU's Regulatory Security State approach, the state provides security indirectly by creating regulatory frameworks, rather than using direct military or police force. For example, the EU's NIS2 Directive makes certain cyber security standards mandatory for private sector organizations, turning these organizations into implementers of the state's security objectives.

Turkey's model, while containing regulatory elements, is closer to the concept of the Positive Security State. In this model, the state provides security directly through its own institutions. The broad intervention and supervision powers given to the Cyber Security Presidency in the CSL are an indication of this approach.

These differences in cyber security approaches are also related to broader cultural and institutional factors. The EU's multinational and federative structure necessitates regulatory approaches, as creating a common military or intelligence structure is politically difficult. Different security perceptions and priorities among member countries make creating a common regulatory framework more feasible than developing direct intervention mechanisms. In countries with strong central government traditions like Turkey, it is more common for the state to develop direct intervention and control mechanisms. Associating cyber security with national security encourages managing this area with traditional security institutions and approaches.

Practical Effects of Approach Differences

The philosophical differences in Turkish and EU cyber security approaches are also reflected in practical regulations. While Turkey's centralized, national security-focused approach is concretized with the broad powers given to the Cyber Security Presidency, the EU's distributed, risk-focused approach is divided among numerous regulatory tools and institutions.

The EU approach, characterized as an invasive forest,[6] creates challenges in terms of conceptual consistency, while Turkey's centralized, threat-focused approach raises questions in terms of flexibility and adaptability.

The institutional structure created by the CSL envisions cyber security being managed by a central authority. The Cyber Security Presidency is directly responsible for the cyber security of critical infrastructures and public institutions and is equipped with inspection, intervention, and sanction powers directed at these institutions. The biggest advantage of this central structure is that it provides rapid decision-making and coordinated intervention capability. Especially in national-scale cyber security crises, the intervention process under the coordination of a single authority can be faster and more consistent. For example, in the event of a cyber attack on critical infrastructure, the Cyber Security Presidency can coordinate all relevant institutions and create a national-level response.

However, this central structure also has some potential disadvantages. First, cyber threats are rapidly changing and evolving threats. There is concern that a central structure may be less flexible in keeping up with this change and developing innovative solutions. Additionally, expertise in the field of cyber security is globally distributed, and many innovative solutions come from the private sector and academia. A central structure may not benefit enough from these diverse sources of knowledge and expertise.

The EU's distributed governance model, on the other hand, envisions a multi-layered system where different actors (member states, EU institutions, private sector, civil society) interact with each other. Various institutions and platforms such as ENISA, the NIS Cooperation Group, CSIRTs Network, CyCLONe (EU Cyber Crisis Liaison Organization Network) have different roles in cyber security governance. The strength of this distributed model is its ability to benefit from various sources of expertise and encourage the development of innovative solutions. The participation of different actors ensures the development of policies that take into account the concerns and perspectives of a wider range of stakeholders. However, this approach can also have disadvantages such as coordination difficulties, authority ambiguities, and slowness in decision-making processes.

Effects on Innovation and Market Dynamics

The effects of cyber security regulations on innovation and market dynamics are also an important point of comparison. The EU's risk-focused and market-friendly approach generally aims to create an environment that fosters innovation. Regulations such as the NIS2 Directive and CRA focus on specific security outcomes and give companies flexibility on how to achieve these outcomes. This "outcome-based regulation" approach encourages companies to develop innovative solutions.

The EU also runs programs that directly support cyber security innovation. Programs such as Horizon Europe, Digital Europe, and Connecting Europe Facility provide billions of euros in funding for cyber security research and development projects. These programs particularly encourage small and medium-sized enterprises (SMEs) and start-ups to develop innovative cyber security solutions.

The CSL's approach, on the other hand, focuses more on compliance and standardization rather than innovation. Article 5 of the Law gives the Cyber Security Presidency the authority to determine standards in the field of cyber security:

> *"To prepare standards related to the field of cyber security, examine standards prepared by other persons or organizations, give opinions on them, adopt them as standards if deemed appropriate, publish them, and monitor their implementation."*

The obligation to comply with these standards, while guaranteeing a minimum level of security on one hand, may restrict innovation on the other. In particular, the requirement for Presidency approval for the sale of cyber security products abroad, as specified in Article 18 of the CSL, may affect the global market competitiveness of domestic cyber security companies.

However, Article 4(ğ) of the CSL contains the statement, "Work aimed at increasing the qualified human resource capability and capacity in the field of cyber security is

encouraged," which can be seen as a commitment to supporting innovation through human resource development.

Conclusion: Towards a Synthesis?

The philosophical differences in Turkish and EU cyber security approaches are also reflected in practical regulations. While Turkey's centralized, national security-focused approach is concretized with the broad powers given to the Cyber Security Presidency, the EU's distributed, risk-focused approach is divided among numerous regulatory tools and institutions.

It is evident that the Cyber Security Law is an important step towards strengthening the national cyber security framework. The Law creates a comprehensive framework by establishing the Cyber Security Presidency and aiming to increase the cyber resilience of critical infrastructures. However, this basic framework can be further strengthened with secondary regulations. In particular, integrating the strengths of EU regulations such as the NIS2 Directive, Cyber Resilience Act, and Cyber Solidarity Act can make Turkey's cyber security approach more effective.

Cyber resilience, proactive cyber defense and deterrence, human-centered approach, secure technology use, domestic and national technologies, and an active role in cyber diplomacy, which are among the six main goals stated in Turkey's 12th Development Plan, contain many elements consistent with the EU's approach. In secondary regulations, leveraging the EU's experiences, especially in cross-sectoral standardization, risk assessment, and international cooperation, can increase the effectiveness of the law.

The regular cyber security assessments and penetration tests introduced by the new Cyber Security Law already include some elements of the EU's risk-based approach. Further strengthening this approach and developing flexible solutions under the coordination of the Presidency that meet the unique needs of different sectors can increase the implementation effectiveness of the law.

The constantly evolving nature of cyber threats requires regulatory frameworks to be continuously updated and developed. Therefore, it is important that cyber security regulations are designed not as static rules but as dynamic and learning systems.

Finally, it should not be forgotten that cyber security is not only a technical issue but also a societal, economic, and political issue. The most effective cyber security strategies are holistic approaches that include not only technical measures but also institutional capacity building, awareness raising, education, and international cooperation. While Turkey's new Cyber Security Law provides a strong foundation focused on national security, supporting it with secondary regulations that integrate the

best practices of the EU's resilience and cooperation-focused approach can significantly increase the country's resilience against cyber threats. In this context, it is critically important that the cyber security approaches of both Turkey and the EU are continuously evaluated and developed in the face of technological developments and the changing threat environment.

[1]: Mügge, D. (2023). Securitizing tech-regulation: the European Union as regulatory security state in cyberspace. Journal of European Public Policy, 30:7, 1431-1442.

[2]: Olejnik, L., Kurasiński, A. (2024). Cybersecurity Philosophical Framework: A Comprehensive Approach to Cyber Threat Analysis. Journal of Cybersecurity Theory and Practice, 15:2, 3-14.

[3]: Bygrave, L. (2025). EU Cybersecurity Law: Evolution, Challenges, and Metaphorical Analysis. European Law Review, 40:1, 6.

[4]: Backman, S. (2023). Risk vs. threat-based cybersecurity: the case of the EU. European Security, 32:1, 85-103.

[5]: Hubbard, G.A. (2023). State-level Cyber Resilience: A Conceptual Framework. ACIG, 2:1, 216.

[6]: Bygrave, L. (2025). EU Cybersecurity Law: Evolution, Challenges, and Metaphorical Analysis. European Law Review, 40:1, 7.