UDC 327.51:004.056(520)
IRSTI 11.25.91
https://doi.org/10.48371/ISMO.2026.64.2.002

ACTIVE CYBER DEFENSE AND CONSTITUTIONAL DETERRITORIALIZATION: CONSTRUCTING NORMATIVE EXCEPTIONS IN JAPAN (2022-2025)

* Kairolla A.B.[1], Absattarov G.R.[2]
*[1,2] Kazakh Ablai Khan University of International Relations and World Languages, Almaty, Kazakhstan

Abstract. In the context of escalating cyber threats, the protection of critical infrastructure has acquired particular significance for Indo-Pacific states. In May 2025, the Japanese Parliament adopted the Active Cyber Defense Act, for the first time granting the government authority for preventive monitoring of communications metadata, remote access to attacker infrastructure, and neutralization of malicious servers abroad. The adoption of the law was preceded by a five-year cyber espionage campaign by the Chinese group MirrorFace, which conducted over 200 attacks against the Ministry of Foreign Affairs, the Ministry of Defense, the Japan Aerospace Exploration Agency, and a number of politicians. The present study examines this law not as a linear expansion of defense powers, but as a structural rupture in which cyberspace is constructed as a domain beyond constitutional constraints. The novelty of the research lies in analyzing the law through the prism of the Copenhagen School securitization theory and the cyber-securitization concept of Hansen and Nissenbaum. The article employs methods of discourse analysis, process-tracing, and comparative analysis of the four pillars of the law. The results demonstrate that the technification of threat serves as the key mechanism of depoliticization, enabling the removal of preventive cyber operations from the jurisdiction of Article 9 without formal constitutional revision, thereby creating a precedent for analogous processes in other technological domains. The practical significance of the findings lies in identifying a model of constitutional transformation applicable to the analysis of emerging security challenges in cyberspace, autonomous weapons systems, and electromagnetic spectrum operations.

Keywords: Japan, active cyber defense, securitization, constitutional deterritorialization, normative exception, Article 9, Copenhagen School, cyberspace, MirrorFace, technification, latent securitization, Indo-Pacific

Introduction

On May 16, 2025, the House of Councillors of Japan, with the support of both the ruling coalition and the main opposition parties, adopted a package of two laws: the Act on Strengthening Cyber Response Capabilities (サイバー能力化法) and an accompanying act amending related legislation. Collectively

known as the Active Cyber Defense Act (能動的サイバ┌防御法), these legal acts, published on May 23, 2025 and entering into force in stages during 2026–2027, grant the government three fundamentally new powers: monitoring of international traffic metadata for early threat detection, remote access to attacker infrastructure, and neutralization of malicious servers abroad [1].

The adoption of this law became the culmination of a three-year legislative process initiated by the National Security Strategy (┌家安全保障┌略) of December 16, 2022, which for the first time set the objective of Japan achieving cyber capabilities "equal to or exceeding those of leading Western states" [2, p. 22]. The immediate stimulus was provided by the results of a five-year investigation by the National Police Agency (NPA) into the cyber espionage campaigns of the MirrorFace group (also known as Earth Kasha), a subgroup of the Chinese APT10, which from December 2019 to 2024 conducted over 200 cyberattacks against the Ministry of Foreign Affairs, the Ministry of Defense, the Japan Aerospace Exploration Agency (JAXA), semiconductor companies, think tanks, and individual politicians [3].

From the standpoint of Japan's postwar constitutional order, this event holds fundamental significance. Article 9 of the 1947 Constitution, which enshrined the renunciation of war as a sovereign right and the prohibition on maintaining armed forces, has functioned for 78 years not merely as a legal constraint but as a constitutive element of the state's strategic identity. As demonstrated by Berger [4] and Katzenstein [5], the antimilitarist identity generated a specific model of strategic behavior: the impossibility of a conventional military response stimulated the development of economic diplomacy, institutional building, and technological innovations in the security sphere.

The central argument of this article holds that the Active Cyber Defense Act constitutes not an incremental adaptation of the constitutional order but a constitutional deterritorialization: cyberspace is constructed as a domain in which the constraints of Article 9 are discursively marked as irrelevant. It is necessary to specify the epistemological status of this argument. The present study does not advance a legal thesis regarding the unconstitutionality of the law, as that falls within the competence of constitutional adjudication. The argument is sociological in nature: drawing on the constructivist theory of securitization, the article analyzes how the government's discursive practices weaken the constitutive function of Article 9 in a new technological domain without affecting its formal legal status. What is at issue is not a violation of the norm, but the creation of a space in which the norm ceases to structure state behavior.

The theoretical framework of the present study is the securitization theory of the Copenhagen School. Barry Buzan, Ole Wæver, and Jaap de Wilde in their monograph "Security: A New Framework for Analysis" [6] developed an analytical framework in which security is viewed not as an objective condition but as a performative speech act, that is, the transfer of an issue from the sphere of "normal politics" to the regime of "extraordinary measures." This approach

enables investigation of how states construct certain phenomena as existential threats to justify the expansion of powers.

With regard to the cyber domain, Lene Hansen of the University of Copenhagen and Helen Nissenbaum of New York University, in their article "Digital Disaster, Cyber Security, and the Copenhagen School" [7], identified three modalities of cyber-securitization: hypersecuritization, technification, and the securitization of everyday practices. Their concept of technification, that is, the depoliticization of securitizing discourse through appeal to technical expertise, holds particular interest for analyzing the Japanese case, where technical language is systematically employed to remove cyber operations from constitutional jurisdiction. Myriam Dunn Cavelty of ETH Zurich, in the work "From Cyber-Bombs to Political Fallout" [8], analyzed how discursive representations of cyber threats shape political consequences, concluding that the exaggeration of cyberattacks' destructive potential is used to legitimize the strengthening of state control.

The constitutional dimension of Japan's security has been thoroughly investigated in the works of several schools. Thomas Berger of Boston University in the monograph "Cultures of Antimilitarism" [4], and Peter Katzenstein of Cornell University in the work "Cultural Norms and National Security" [5], convincingly demonstrated that the antimilitarist identity of postwar Japan is not merely a legal constraint but a structural condition shaping the entire field of strategic behavior. Andrew Oros of Washington College, in the monograph "Japan's Security Renaissance," analyzed the transformation of Japanese security policy in the 21st century and demonstrated how the gradual revision of security identity occurs while the antimilitarist core is preserved [9]. Christopher Hughes of the University of Warwick, in the work "Japan's Foreign and Security Policy Under the Abe Doctrine," investigated in detail the bureaucratic mechanisms of defense policy transformation under the Abe administration, revealing the key role of the interaction between Liberal Democratic Party "tribal" Diet members and Ministry of Economy, Trade and Industry bureaucrats in shaping economic security policy [10].

Jef Huysmans of Queen Mary University of London, in the work "Security Unbound," developed the argument regarding the democratic limits of securitization, which bears direct relevance to the Japanese case, where the constitutional order sets institutional boundaries of permissible securitization [11].

The Active Cyber Defense Act of 2025 itself has become the subject of expert analysis. The analytical firm GR Japan, in the review "Japan's Active Cyber Defense Act," thoroughly examined the legislative history, institutional design, and strategic implications of the law, drawing attention to its four-component structure [12]. The ESET cybersecurity company, in the report "Operation AkaiRyū," confirmed MirrorFace's affiliation with APT10 and documented the resumption of the ANEL backdoor, previously considered abandoned since 2018,

indicating institutional continuity of cyber espionage operations [13]. Questions of Japan's national security in a broader context are also examined by Kazakhstani researchers. German Kim, Shynar Seitnur, and Vladislav Pishchalin, in their article "On the Political Realism of Japan's New National Security Strategy," published in the present journal, analyzed the 2022 National Security Strategy through the prism of political realism theory [14]. Their analysis, although focused on the conventional dimension of security, identifies the same starting point from which the present study proceeds: the 2022 Strategy, which first articulated the objective of achieving "active cyber defense."

Thus, existing research thoroughly analyzes both the theoretical frameworks of securitization and conventional aspects of the transformation of Japan's defense policy. However, the constitutional dimension of cyber-securitization, the mechanism by which cyberspace is constructed as a domain beyond the reach of Article 9, remains insufficiently studied. The present article fills this gap by integrating the Copenhagen School's securitization theory with the analysis of constitutional transformation.

Description of Materials and Methods

The study of Japan's Active Cyber Defense Act encompasses the analysis of key legal and strategic documents as well as actual changes in the country's cybersecurity institutional architecture. The article is based on a corpus of Japanese-language sources, including the National Security Strategy (December 2022), the final proposals of the Expert Council on Cybersecurity (有識者┌議提言, November 2024), explanatory documents of the Cabinet Secretariat (March 2025), the NPA and NISC alert on MirrorFace activities (January 2025), and materials from parliamentary debates during the bill's passage (February-May 2025).

Discourse analysis of these documents reveals the structure of the securitizing discourse, identifying who acts as the securitizing actor, what is constructed as an existential threat, and how the necessity of extraordinary measures is justified. For the reconstruction of the sequence from threat identification to legislative response, the method of process-tracing is applied, productively employed in studies of Japanese security policy [9; 10]. This method enables tracing how the five-year MirrorFace cyber espionage campaign led to public attribution by the NPA, the work of the Expert Council, Cabinet approval of the bill, and its ultimate adoption by Parliament. A comparative approach differentiates the four pillars of the law by their degree of constitutional significance, separating incremental elements from those producing a structural rupture. Tables and diagrams are used for systematization and visualization of empirical material.

Results

Cyber espionage and the formation of securitizing discourse. The legislative process between 2022 and 2025 cannot be understood outside the context of

specific cyber incidents that provided the material basis for the securitizing discourse. The central element of this basis was the activity of the MirrorFace group. The NPA, jointly with the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), in January 2025 publicly attributed its actions as "systematic cyberattacks linked to China, directed primarily at the theft of information pertaining to Japan's national security and advanced technologies" [3]. The following table systematizes the three identified campaigns (see Table 1).

Table 1. MirrorFace campaigns according to NPA data (2019-2024)

Campaign	Period	Targets	Methods	Malware
A	Dec. 2019 - Jul. 2023	Think tanks, MFA, politicians, media	Spear-phishing (themes: «Japan-US alliance,» «Taiwan Strait,» «FOIP»)	**LODEINFO, NOOPDOOR, LilimRAT**
B	Feb. - Oct. 2023	Semiconductors, aerospace, ICT, JAXA	Exploitation of VPN vulnerabilities (Array Networks, Fortinet, Citrix)	**Cobalt Strike, LODEINFO, NOOPDOOR**
C	From Jun. 2024	University researchers (security, IR), think tanks, politicians, media	Spear-phishing with links; Visual Studio Code tunnels; Windows Sandbox	**ANEL (UPPERCUT), AsyncRAT**

Note: compiled by the author based on NPA and NISC data [3] and the ESET Research report [13]

Several aspects of this picture merit analytical attention. First, the trajectory of target development: from political (Campaign A: politicians, media) to technological (Campaign B: semiconductors, aerospace) and back to political (Campaign C). This pattern indicates a dual objective: technology theft and intelligence collection. Second, the phishing email themes of Campaign A evidence the deliberate exploitation of key nodes in Japan's strategic discourse. Third, ESET in March 2025 confirmed that MirrorFace is a subgroup of APT10, and that ANEL, a backdoor previously considered abandoned since 2018, was returned to the arsenal with minimal version updating (5.5.0 to 5.5.4), indicating institutional continuity of operations [13].

In parallel with MirrorFace's activities, two incidents documented in open sources served as catalysts for the legislative process. In the fall of 2020, the U.S. National Security Agency discovered that Chinese military hackers had penetrated Japan's classified defense networks. According to the assessment of American officials, the data breach regarding Japan's military capabilities jeopardized intelligence sharing between the Pentagon and Japan's defense establishment. In 2023, a large-scale breach of Tokyo's defense networks was revealed, characterized as the most damaging hacking incident in the country's modern history [15].

The constitutive function of Article 9 as the initial analytical framework. To understand the mechanism of deterritorialization, it is necessary to articulate

the logic that this mechanism overcomes. Article 9 is interpreted in three registers: juridical (a norm constraining military potential), strategic (a limitation compelling alternative strategies), and constitutive (the foundation of strategic identity). It is the third register that generates the constitutive paradox, as the constraint functions not as a barrier but as a productive condition.

The practical manifestations of the constitutive paradox can be traced in the institutional innovations of recent years. The Economic Security Promotion Act (経済安全保障推進法, May 2022), with its four pillars (supply chain resilience, reliability of basic infrastructure, support for key technologies, and classified patents), represents a characteristic product of the constitutive paradox. The strong industrial orientation combined with a weak defense dimension is explained by the interaction of two factors: the antimilitarist identity as a structural constraint and the dominance of LDP "tribal" Diet members (族議員) and METI bureaucrats as key agents [10].

In the terms of the Copenhagen School, the constitutive paradox functioned as a built-in mechanism of desecuritization. Every attempt to transfer an issue from "normal politics" to the regime of "extraordinary measures" encountered the constitutional threshold. In the Japanese case, the constitutional order systematically prevented the completion of this performative act: the threat could be articulated, but extraordinary measures encountered a constitutional constraint [6; 16, p. 56].

Securitization trajectory: from threat to law. Process-tracing reveals six nodes in the sequence that led to the adoption of the law. The following figure visualizes this sequence (see Figure 1).

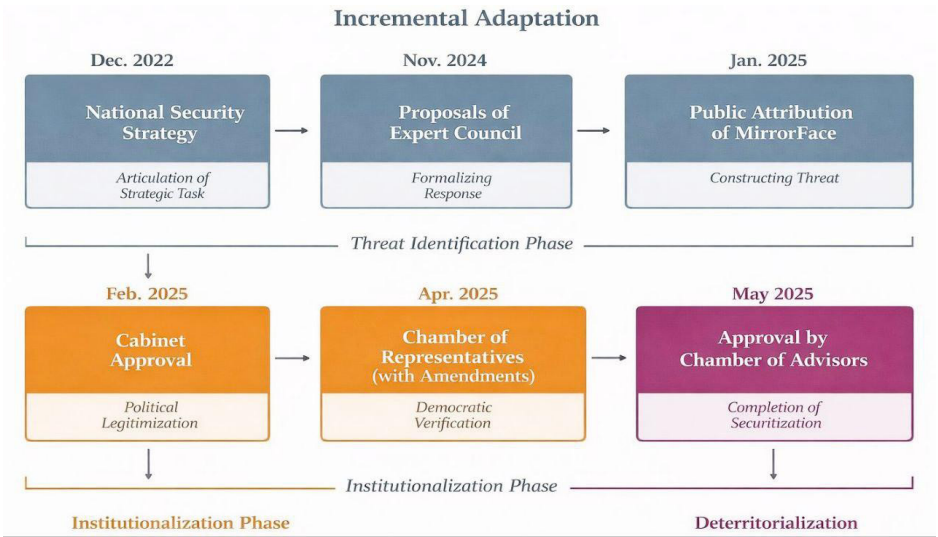

Figure 1. Sequence of transition from threat identification to law adoption (2022–2025).

Compiled by the author based on government documents and parliamentary materials.

This sequence demonstrates three significant patterns. The first is acceleration: from the articulation of the objective (December 2022) to the adoption of the law (May 2025), fewer than three years elapsed, an extraordinarily short period for the Japanese legislative process. For comparison, the debates on the reinterpretation of collective self-defense took more than two years (July 2014 to September 2015) with a significantly narrower scope of powers. The second pattern is institutional inheritance. The architecture of the law builds upon the infrastructure of the 2022 Economic Security Act: the category of "critical infrastructure" (基幹インフラ), covering 15 sectors and approximately 257 operators as of July 2025, is directly borrowed from the economic security regime. The third pattern is institutional mimicry. The creation of the NCO (National Cybersecurity Office, 「家サイバ「統括室), the formation of the Cyber Threat Information Sharing Council, and the integration of a security clearance system are all institutional calques of Western prototypes (USCYBERCOM, NCSC). Nevertheless, beneath the external isomorphism, the internal logic differs: the NCO reports to the Cabinet Secretariat rather than the Ministry of Defense.

Four pillars: differentiating incrementalism and deterritorialization. Structural analysis of the four pillars of the law reveals their heterogeneous constitutional nature. The following figure visualizes this distinction (see Figure 2).

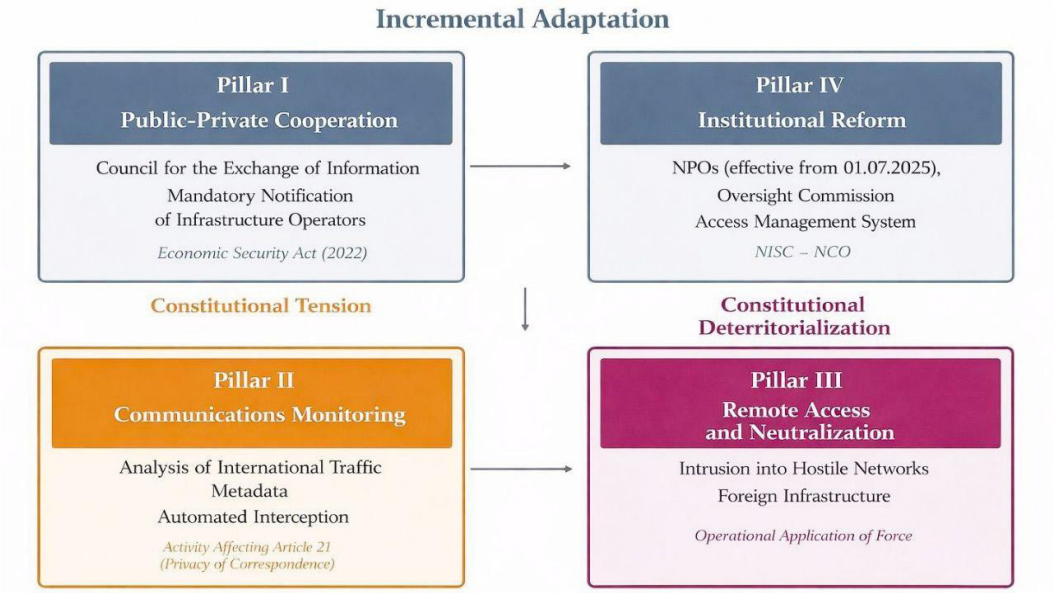

Figure 2. Constitutional significance of the four pillars of the Active Cyber Defense Act.
Compiled by the author.

Pillars I and IV are incremental in character. The creation of the Cyber Threat Information Sharing Council reproduces the coordination logic already

institutionalized in the economic security regime. The transformation of NISC into the NCO elevates the institutional status of cybersecurity but does not create fundamentally new powers. Pillar II, communications monitoring, creates constitutional tension, but predominantly along the axis of Article 21 (secrecy of correspondence) rather than Article 9. The law formally limits monitoring to international traffic metadata, excludes content interception, and provides for "automated machine selection" (自動的な方法による機械的情報の選別). The creation of the independent Communications Information Oversight Commission (サイバー通信情報監理委員会) institutionalizes an oversight mechanism.

Pillar III possesses a fundamentally different constitutional nature. Remote access to attacker infrastructure and neutralization of malicious servers abroad constitute proactive offensive cyber operations on the territory of foreign states. The police and Self-Defense Forces are granted powers to "access electronic computing machines used for carrying out attacks and take actions to eliminate the threat" (アクセス・無害化措置). From the standpoint of constitutional law, these powers create tension along two axes: Article 9, paragraph 1 (prohibition on "the threat or use of force as means of settling international disputes") and Article 21 (guarantee of secrecy of communications). In the comparative legal context, analogous powers are enshrined in the "defend forward" doctrine of U.S. Cyber Command (2018) and the model of the United Kingdom's National Cyber Force (2020), and doctrinally grounded in the Tallinn Manual 2.0 [17], which distinguishes cyber operations below and above the threshold of \"use of force\" within the meaning of Article 2(4) of the UN Charter. The Japanese government positions Pillar III precisely as "countermeasures" (対抗措置) rather than "use of force" (武力行使). However, in a conventional military analogy, these actions are functionally equivalent to a preventive strike on adversary infrastructure.

Discussion

Technification as a mechanism of deconstitutionalization. The comparative legal analysis conducted above identifies a fundamental circumstance: Pillar III creates constitutional tension, yet this tension does not become the subject of constitutional discussion. Unlike the reinterpretation of collective self-defense by the Abe cabinet (July 2014), where the question was formulated explicitly ("Does Article 9 permit this action?"), in the case of the Active Cyber Defense Act, the constitutional problematic is discursively neutralized before it acquires public articulation. The mechanism of this neutralization is technification in the meaning given to this concept by Hansen and Nissenbaum [7].

In their conceptual framework, technification represents a modality of securitization in which the appeal to technical expertise depoliticizes the issue, removing it from the sphere of public discussion. In the Japanese case, this mechanism performs a specific and more radical function: it does not merely depoliticize the issue but removes it from constitutional jurisdiction as such. In other words, technification here is not an instrument of securitization in the

classical sense of the Copenhagen School but a mechanism of constitutional deterritorialization: the creation of a domain in which the constitutional norm is a priori marked as irrelevant.

The mechanism can be traced at three levels of discursive practice in government documents. At the level of nomination, the neutralization of a foreign server is designated not as "use of armed force abroad" (海外**における**武力行使) but as a "technical countermeasure" (技術的**な**措置). At the procedural level, automated data selection is constructed not as "state surveillance" (「家**による**監視) but as "machine filtering of metadata," a process in which "no person views the content of communications." At the level of goal-setting, remote access operations are framed as "elimination of malicious effects" (無害化) rather than "offensive cyber operations." In each case, the technical language performs the same function: it reclassifies the action so that the constitutional norm loses its applicability. Crucially, what is at issue is not argumentation (the government does not prove the compatibility of actions with Article 9) but categorization, whereby the action is placed in a domain where the question of Article 9's applicability does not arise.

This mechanism fundamentally differs from previous transformations of the constitutional order. The reinterpretation of collective self-defense operated within constitutional logic: the interpretation of Article 9 was expanded, but the article itself remained the referent norm. The Active Cyber Defense Act performs a different operation: the question of Article 9's applicability is discursively removed. The technical character of cyber actions is constructed as a basis for removing them from the constitutional domain, not through the argument "Article 9 permits this" but through the assertion "Article 9 does not apply to this." It is precisely at this point that the constitutive function of Article 9 loses its logic. The constitutional constraint ceases to structure the field of the permissible, not because it has been repealed or reinterpreted, but because an entire domain of state activity is constructed outside its jurisdiction.

The cross-party consensus in the vote indirectly confirms the effectiveness of this mechanism. The 2015 Security Laws were adopted amid fierce opposition resistance and mass protests, as the discourse was built in constitutional terms. The Active Cyber Defense Act, by contrast, was adopted with the support of the main opposition parties, as the technical framing depoliticized the constitutional dimension. In the terms of Balzacq [18, p. 182], this contrast demonstrates the success of the "perlocutionary" dimension of securitization: the effect on the audience is achieved not by the force of constitutional argument but by its technical opacity, which removes the issue from the sphere where constitutional argumentation is perceived as appropriate.

Bureaucratic dynamics: antimilitarist inheritance. The institutional architecture of the law reveals an additional paradox that reinforces the deterritorialization effect. The distribution of powers among agencies reproduces the pattern characteristic of Japanese security policy throughout the postwar

period: the dominance of civilian structures with the marginalization of the military. The NCO reports to the Cabinet through the Secretariat. The primary agent of neutralization is the police (警察), not the Self-Defense Forces. This institutional configuration reproduces the persistence of the antimilitarist culture identified by Berger and Katzenstein.

At the same time, it is precisely the civilian institutional design that paradoxically facilitates the expansion of the state's offensive potential. Powers that, if assigned to the Self-Defense Forces, would inevitably activate constitutional scrutiny are transferred to civilian agencies and thereby discursively removed from under the constitutional norm. The antimilitarist identity, therefore, does not impede the expansion of state powers but transforms its institutional form, creating an effect that may be conceptualized as "deconstitutionalization through antimilitarist institutional inheritance." It is necessary to specify the epistemological status of this observation. The present study does not claim that antimilitarist identity is instrumentally deployed; rather, it argues that deeply embedded institutional patterns, products of 78 years of constitutional practice, structure the form in which new capabilities are acquired, producing effects that are not necessarily intended by any single actor.

This dynamic permits a refinement of the study's theoretical framework. The Copenhagen School traditionally conceptualizes securitization as a binary transition: from "normal politics" to "extraordinary measures" and back. The Japanese case demonstrates a third modality: latent securitization, in which the expansion of state powers occurs without a public transition to the emergency regime. Technification depoliticizes the content of actions, and antimilitarist institutional inheritance depoliticizes their form. The aggregate effect is that the state acquires offensive cyber capabilities while formally remaining within the antimilitarist constitutional order.

Conclusion

The analysis of the Active Cyber Defense Act of 2025 through the prism of the Copenhagen School securitization theory and the cyber-securitization concept of Hansen and Nissenbaum allows us to assert that the adopted law constitutes a qualitatively different type of constitutional transformation compared to preceding stages of Japan's defense policy adaptation. The mechanism of this transformation is not constitutional revision but constitutional deterritorialization: the creation of a normative space in which the constraint ceases to structure state behavior.

The key role in this process is played by the technification of discourse. The reclassification of offensive cyber operations from the category of "use of force" to the category of "technical countermeasures" enables the state to acquire capabilities whose functional logic is comparable to preventive actions in the conventional military sphere without activating constitutional scrutiny. The civilian institutional design additionally depoliticizes the form of these actions. The antimilitarist identity, which for 78 years constrained the field of the

permissible, paradoxically transforms into an institutional resource ensuring the political acceptability of the expansion of offensive potential.

The theoretical significance of the study consists in identifying a modality of securitization not described in the existing literature on critical security studies. The binary model of the Copenhagen School presupposes the transfer of an issue from "normal politics" to the regime of "extraordinary measures." The Japanese case demonstrates a different mechanism: the expansion of state powers without a public transition to the emergency regime and without constitutional argumentation, through the discursive construction of an entire domain as a space to which the constitutional norm does not apply. This mechanism may have analytical significance for the study of processes in other technological domains, such as autonomous weapons systems, electromagnetic spectrum operations, and space operations.

In the regional context, the transformation creates a dual dynamic. For allies, the enhancement of Japan's cyber capabilities increases interoperability and strengthens the deterrence architecture. For regional adversaries, it may be interpreted as covert remilitarization masked by a civilian institutional shell. The law enters into force in stages during 2026–2027, and the question of the possibility of desecuritization, the return of the cyber domain to the regime of constitutional control, remains open and requires further research as the new regime undergoes institutional consolidation.

REFERENCES

[1] ┌閣官房サイバ┌安全保障体制整備準備室 [Naikaku Kanbō Saibā Anzen Hoshō Taisei Seibi Junbishitsu]. サイバ┌┌┌能力┌化法案及び同整備法案について [Regarding the Bill to Strengthen Cyber Response Capabilities and the Related Development Bill] [Electronic resource]. – 2025. – March. – https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/index.html (Date of access: 15.01.2026).

[2] ┌閣官房┌家安全保障┌議 [Naikaku Kanbō Kokka Anzen Hoshō Kaigi]. ┌家安全保障┌略 [National Security Strategy] [Electronic resource]. – 2022. – Dec. 16. – https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-j.pdf (Date of access: 15.01.2026).

[3] ┌閣官房警察┌┌┌閣サイバ┌セキュリティセンタ┌ [Naikaku Kanbō Keisatsuchō, Naikaku Saibā Sekyuriti Sentā]. MirrorFaceによるサイバ┌攻┌について（注意喚起） [Regarding Cyberattacks by MirrorFace (Alert)] [Electronic resource]. – 2025. – Jan. 8. – https://www.cyber.go.jp/pdf/news/press/20250108_MirrorFace.pdf (Date of access: 15.01.2026).

[4] Berger T. U. Cultures of Antimilitarism: National Security in Germany and Japan. – Baltimore : Johns Hopkins University Press, 1998. – 256 p.

[5] Katzenstein P. J. Cultural Norms and National Security: Police and Military in Postwar Japan. – Ithaca, NY : Cornell University Press, 1996. – 307 p.

[6] Buzan B. Security: A New Framework for Analysis / B. Buzan, O.

Wæver, J. de Wilde. – Boulder : Lynne Rienner Publishers, 1998. – 239 p.

[7] Hansen L., Nissenbaum H. Digital Disaster, Cyber Security, and the Copenhagen School // International Studies Quarterly. – 2009. – Vol. 53, № 4. – P. 1155–1175.

[8] Dunn Cavelty M. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse // International Studies Review. – 2013. – Vol. 15, № 1. – P. 105–122.

[9] Oros A. L. Japan's Security Renaissance: New Policies and Politics for the Twenty-First Century. – New York : Columbia University Press, 2017. – 320 p.

[10] Hughes C. W. Japan's Foreign and Security Policy Under the 'Abe Doctrine': New Dynamism or New Dead End? – London ; Basingstoke : Palgrave Pivot, 2015. – 114 p.

[11] Huysmans J. Security Unbound: Enacting Democratic Limits. – London : Routledge, 2014. – 224 p.

[12] GR Japan. Japan's Cybersecurity Turning Point: Active Cyber Defense Act and the National Cybersecurity Office [Electronic resource]. – 2025. – https://grjapan.com/sites/default/files/content/articles/files/20250916%20GR%20Japan%20Industry%20Insight%20Cybersecurity.pdf (Date of access: 13.02.2026).

[13] ESET Research. Operation AkaiRyū: MirrorFace Invites Europe to Expo 2025 and Revives ANEL Backdoor [Electronic resource]. – 2025. – March 18. – https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/ (Date of access: 20.02.2026).

[14] German K., Seitnur Sh., Pishchalin V. On Political Realism of Japan's New National Security Strategy // Kazakhstan Oriental Studies. – 2025. – Vol. 13, № 1. – P. 143–157.

[15] Nakashima E. China Hacked Japan's Sensitive Defense Networks, Officials Say // The Washington Post. – 2023. – Aug. 7. – https://www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/ (Date of access: 20.01.2026).

[16] Wæver O. Securitization and Desecuritization // On Security / ed. by R. D. Lipschutz. – New York : Columbia University Press, 1995. – P. 46–87.

[17] Schmitt M. N., ed. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge : Cambridge University Press, 2017. – 30 p.

[18] Balzacq T. The Three Faces of Securitization: Political Agency, Audience and Context // European Journal of International Relations. – 2005. – Vol. 11, № 2. – P. 171–201.

БЕЛСЕНДІ КИБЕРҚОРҒАНЫС ЖӘНЕ КОНСТИТУЦИЯЛЫҚ ДЕТЕРРИТОРИАЛИЗАЦИЯ: ЖАПОНИЯДАҒЫ НОРМАТИВТІК ЕРЕКШЕЛІКТЕРДІҢ ҚАЛЫПТАСУЫ (2022–2025)

*Кайролла А.Б.[1], Абсаттаров Г.Р.[2]
*1,2 Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан

Аңдатпа. Киберқауіптердің үдеуі жағдайында критикалық инфрақұрылымды қорғау Үнді-Тынық мұхиты аймағы мемлекеттері үшін айрықша маңызға ие болды. 2025 жылғы мамырда Жапония Парламенті «Белсенді киберқорғаныс туралы» заңды қабылдады; бұл құжат үкіметке алғаш рет байланыс метадеректеріне алдын алу мониторингін жүргізу, шабуылдаушылардың инфрақұрылымына қашықтан қол жеткізу және шетелдік зиянды серверлерді бейтараптандыру өкілеттігін берді. Заңның қабылдануына Қытайдың MirrorFace тобы тарапынан бес жыл бойы жүргізілген кибертыңшылық науқаны негіз болды; аталған топ Сыртқы істер министрлігіне, Қорғаныс министрлігіне, Жапонияның аэроғарыштық зерттеулер агенттігіне және бірқатар саясаткерлерге қарсы 200-ден астам шабуыл ұйымдастырған. Бұл зерттеу аталған заңды қорғаныс өкілеттіктерінің жай ғана сызықтық кеңеюі емес, киберкеңістікті конституциялық шектеулерден тыс аймақ ретінде айқындайтын құрылымдық үзіліс ретінде қарастырады. Зерттеудің ғылыми жаңалығы заңды Копенгаген мектебінің «қауіпсіздендіру» теориясы мен Хансен және Ниссенбаумның «киберқауіпсіздендіру» тұжырымдамасы аясында талдауында жатыр. Мақалада дискурс-талдау, процесс-трейсинг және заңның «төрт тірегін» салыстыру әдістері қолданылады. Нәтижелер көрсеткендей, қауіптің технификациясы саясиландырудан арылудың негізгі механизмі болып табылады. Бұл превентивті кибер-операцияларды формалды конституциялық реформасыз-ақ 9-баптың юрисдикциясынан шығаруға мүмкіндік беріп, өзге технологиялық салалардағы ұқсас процестер үшін прецедент қалыптастырады. Зерттеудің практикалық маңызы киберкеңістіктегі, автономды қару жүйелеріндегі және электромагниттік спектр операцияларындағы жаңа қауіпсіздік сын-тегеуріндерін талдауда қолданылатын конституциялық трансформация моделін анықтауында.

Тірек сөздер: Жапония, белсенді киберқорғаныс, қауіпсіздендіру, конституциялық детерриториалдау, нормативтік ерекшелік, Копенгаген мектебі, киберкеңістік, MirrorFace, технификация, латентті қауіпсіздендіру, Үнді-Тынық мұхиты аймағы

АКТИВНАЯ КИБЕРЗАЩИТА И КОНСТИТУЦИОННАЯ ДЕТЕРРИТОРИАЛИЗАЦИЯ: СОЗДАНИЕ НОРМАТИВНЫХ ИСКЛЮЧЕНИЙ В ЯПОНИИ (2022-2025 гг.)

*Кайролла А.Б.[1], Абсаттаров Г.Р.[2]
[*1,2] Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан

Аннотация. В условиях нарастания киберугроз вопросы защиты критической инфраструктуры приобретают особую значимость для государств Индо-Тихоокеанского региона. В мае 2025 года Парламент Японии принял Закон об активной киберзащите, впервые наделивший правительство полномочиями по превентивному мониторингу метаданных коммуникаций, удалённому доступу к инфраструктуре атакующих и нейтрализации вредоносных серверов за рубежом. Принятию закона предшествовала пятилетняя кампания кибершпионажа со стороны китайской группировки MirrorFace, осуществившей более 200 атак против Министерства иностранных дел, Министерства обороны, Японского агентства аэрокосмических исследований и ряда политиков. Настоящее исследование рассматривает данный закон не как линейное расширение оборонных полномочий, а как структурный разрыв, при котором киберпространство конструируется как домен за пределами конституционных ограничений. Новизна исследования состоит в анализе закона через призму теории секьюритизации Копенгагенской школы и концепции кибер-секьюритизации Хансена и Нисенбаума. В статье использованы методы дискурсивного анализа, процесс-трассировки и компаративного анализа четырех столпов закона. Результаты исследования демонстрируют, что технификация угрозы выступает ключевым механизмом деполитизации, позволяющим вывести превентивные кибероперации из-под юрисдикции девятой статьи без формальной конституционной ревизии, что создаёт прецедент для аналогичных процессов в других технологических сферах. Практическая значимость полученных результатов заключается в выявлении модели конституционной трансформации, применимой к анализу возникающих вызовов безопасности в киберпространстве, сфере автономных систем вооружения и операций в электромагнитном спектре.

Ключевые слова: Япония, активная киберзащита, секьюритизация, конституционная детерриториализация, нормативное исключение, Копенгагенская школа, киберпространство, MirrorFace, технификация, латентная секьюритизация, Индо-Тихоокеанский регион

Received / Мақала түсті / Статья поступила: 27.03.2026.
Accepted / Жариялауға қабылданды / Принята к публикации: 26.06.2026

Information about the authors:

Kairolla Adil Bauyrzhanovich – Master's student, Kazakh Ablai Khan University of International Relations and World Languages, Almaty, Kazakhstan, ORCID ID: 0009-0002-4143-4799, e-mail: arkito.a@protonmail.com

Absattarov Galymzhan Raushanbekovich – Candidate of Political Sciences, Associate Professor, Ablai Khan Kazakh University of International Relations and World Languages, Almaty, Kazakhstan, e-mail: abusattar@mail.ru

Авторлар туралы мәлімет:

Кайролла Адиль Бауыржанович – магистрант, Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан, ORCID ID: 0009-0002-4143-4799, e-mail: arkito.a@protonmail.com

Абсаттаров Галымжан Раушанбекович – саяси ғылымдар кандидаты, қауымдастырылған профессор, Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан, e-mail: abusattar@mail.ru

Сведения об авторах:

Кайролла Адиль Бауыржанович - магистрант, Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан, ORCID ID: 0009-0002-4143-4799, e-mail: arkito.a@protonmail.com

Абсаттаров Галымжан Раушанбекович - кандидат политических наук, ассоциированный профессор, Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан, e-mail: abusattar@mail.ru