frontiers | Frontiers in Political Science

TYPE Original Research
PUBLISHED 12 January 2026
DOI 10.3389/fpos.2025.1749390

OPEN ACCESS

EDITED BY
Luiz Rogério Franco Goldoni,
Brazilian Army Command and General Staff College, Brazil

REVIEWED BY
Zhamilia Klycheva,
TransResearch Consortium, United States
Małgorzata Krystyna Kamola-Cieślik,
University of Szczecin, Poland

*CORRESPONDENCE
Roland Kelemen
✉ kelemen.roland@ga.sze.hu

RECEIVED 18 November 2025
REVISED 07 December 2025
ACCEPTED 08 December 2025
PUBLISHED 12 January 2026

CITATION
Kelemen R, Bucko B, Mazuch M, Squillace J, Cappella J and Szabó H (2026) The service doctrine: How intelligence mandates shape national cybersecurity ecosystems?
Front. Polit. Sci. 7:1749390.
doi: 10.3389/fpos.2025.1749390

The service doctrine: How intelligence mandates shape national cybersecurity ecosystems?

Roland Kelemen[1]*, Boris Bucko[2], Martin Mazuch[3], Joseph Squillace[4], Justice Cappella[5] and Hedvig Szabó[1]

[1]Modern Technologies and Cybersecurity Law Department, Deak Ferenc Faculty of Law, Széchenyi István University, Győr, Hungary, [2]The Ministry of Education, Research, Development and Youth of the Slovak Republic, Bratislava, Slovakia, [3]Faculty of Management Science and Informatics, University of Žilina, Žilina, Slovakia, [4]Cybersecurity Analytics and Operations, Penn State University, University Park, PA, United States, [5]Business Management and Marketing, Penn State University, University Park, PA, United States

This study provides a structured comparative analysis of how democratic and authoritarian regimes integrate cybersecurity into their national security architectures, with particular attention to the severely under-researched Central-Eastern European EU member states (Hungary and Slovakia). Using a most-different-systems design, the article contrasts the multi-stakeholder, cooperative model of a major rule-of-law democracy (United States) with the centralized, digital-sovereignty-driven approaches of three major authoritarian powers (China, Russia, Iran) and two smaller EU members. In addition to institutional structures and oversight mechanisms, the analysis explicitly incorporates public trust dynamics as a critical variable of cybersecurity resilience. Findings show that democratic systems generate higher legitimacy but slower operational tempo, whereas authoritarian models achieve rapid capability integration at the expense of societal trust and private-sector autonomy. In the Central-Eastern European cases, the interplay of NIS2 obligations and pronounced centralizing tendencies produces distinctive governance patterns that deviate from both the classic "cooperating cyberfare state" and the "smart total-control" archetypes. The study demonstrates that sustained public trust—fostered through transparent communication, accountable institutions and meaningful societal inclusion—acts as a force multiplier for cybersecurity resilience across all regime types. By filling three identified gaps (small EU member states, cross-regime empirical depth, and public-trust integration), the article advances both the comparative politics of cybersecurity governance and practical policy recommendations for strengthening transatlantic and intra-EU cyber resilience.

KEYWORDS

central-eastern Europe, cooperative vs. monocratic cybersecurity, cybersecurity governance, digital sovereignty, most-different-systems design, national security, public trust

1 Introduction

In the 21st-century security environment, public trust in national security institutions has emerged as a cornerstone of sustainable security. This trust is a multifaceted concept, encompassing both diffuse institutional trust in the legitimacy of state actors and specific, sector-level confidence in their competence and integrity. The absence of either dimension directly undermines the credibility of state security policy, the societal acceptance of defence operations, and the effectiveness of strategic communication, a relationship explored in detail

in Kelemen et al. (2024a). Recent analyses of contemporary crises, including pandemics, democratic backsliding, and domestic extremism, consistently highlight that national security actors—from intelligence services to armed forces—are increasingly dependent on active societal cooperation to achieve desired outcomes (Jones, 2025). This interdependence is particularly pronounced within the social pillar of the United Nations Sustainable Development Goals (SDGs), especially SDG 16 (Peace, Justice and Strong Institutions), where rule-of-law-based, transparent, and accountable institutions generate high levels of public trust, which in turn enable the long-term implementation of complex security strategies, including those addressing climate change, energy security, and hybrid threats (United Nations, 2021).

Public trust is not merely a normative ideal but an operational necessity. Without it, populations resist restrictive measures, withhold cooperation with authorities, and become more vulnerable to disinformation campaigns. NATO member states have increasingly recognized this linkage, integrating sustainability considerations into their national security strategies on the understanding that social stability, economic well-being, and security resilience are inseparable (NATO, 2022). The NATO Climate Change and Security Action Plan, for instance, explicitly frames climate change as a "defining challenge" that requires enhanced societal trust and cross-sectoral collaboration to achieve effective mitigation and adaptation (NATO, 2021). Sustaining public trust therefore demands continuous, two-way, transparent communication, institutional accountability, and the meaningful involvement of societal stakeholders.

The significance of public trust is amplified in the cybersecurity–national security nexus, where threats are largely invisible, protective measures are frequently classified, and the role of the private sector is indispensable. These characteristics render societal trust particularly fragile (Barrinha and Renard, 2020). Democratic regimes, with their emphasis on transparency and multi-stakeholder cooperation, tend to foster greater public legitimacy yet often experience slower decision-making and coordination challenges due to voluntary private-sector participation and stringent oversight requirements (Manjikian, 2023). In contrast, authoritarian systems, guided by the ideology of digital sovereignty, establish highly centralized, monocratic structures in which private actors are subordinated to or co-opted by the state, enabling rapid integration of offensive and defensive cyber capabilities into the national security apparatus (Conduit, 2023; Santaniello and Barbieri, 2024). Empirical studies confirm that authoritarian regimes achieve greater operational agility across the full spectrum of cyber warfare, whereas democratic systems, bound by rule-of-law constraints and private-sector autonomy, frequently face delayed responses and fragmented implementation (Whyte, 2020; Egloff and Smeets, 2023; Saeed et al., 2023).

Within the European context, the implementation of the NIS2 Directive reveals stark divergences in governance models among member states, producing fragmentation rather than convergence (Veigurs et al., 2024; Santaniello and Barbieri, 2024). Public–private cooperation ranges from the predominantly voluntary US model, through mandatory reporting regimes in several EU states, to the subordinate "patriotic hacker" arrangements observed in authoritarian systems (Huang et al., 2021; Conduit, 2023). The dual-use nature of cyber capabilities creates novel dilemmas in both regime types: democratic societies expose private actors to geopolitical pressure, while authoritarian regimes, by incorporating proxy actors, simultaneously enhance resilience and risk erosion of centralized control (Shah et al., 2023; McIntosh et al., 2023).

A conspicuous gap in the literature is the near-total under-representation of smaller and medium-sized Central-Eastern European EU member states (e.g., Hungary and Slovakia) in comparative cybersecurity governance research. Most studies focus either on major democracies (United States, Germany, France) or on major authoritarian powers (China, Russia, Iran), rarely employing a "most different systems" design that would place these two extremes and Central-Eastern European cases within a single analytical framework (Veigurs et al., 2024; Santaniello and Barbieri, 2024; Shah et al., 2023). Empirical analysis is also lacking on how the "national security exception" in democratic systems erodes rule-of-law oversight mechanisms (prior judicial authorisation, proportionality), and on the extent to which the authoritarian "smart total-control" logic is exportable or adaptable to EU member states in the region. Finally, there is a striking scarcity of in-depth, cross-regime comparative studies examining the actual effectiveness—rather than merely the formal regulation—of public–private cooperation, particularly along the voluntary versus mandatory reporting dimension (Saeed et al., 2023; Arroyabe et al., 2024).

The present study addresses these three critical gaps by (1) incorporating Central-Eastern European EU member states (Hungary and Slovakia), (2) simultaneously analyzing a major democracy (United States) and major authoritarian powers (China, Russia, Iran) within a "most different systems" framework, and (3) conducting an in-depth examination of the practical functioning of oversight mechanisms, public–private relationships, and public trust dynamics, moving beyond formal legal texts.

To address these gaps systematically, this study is guided by three central research questions:

1. How do the underlying logics of cybersecurity governance models in rule-of-law democracies and authoritarian regimes differ, particularly concerning the integration of national security frameworks and cybersecurity institutions?
2. In what ways does public trust function as a critical variable for national cybersecurity resilience, and how does its role vary across these different political systems?
3. What specific governance patterns emerge in Central-Eastern European EU member states at the intersection of supranational legal requirements, such as the NIS2 Directive, and national centralizing tendencies?

This article argues that while democratic and authoritarian states converge in establishing dual legal-institutional structures, these frameworks diverge fundamentally in their function and purpose. We posit that democratic models are defined by an inherent structural tension between security imperatives and fundamental rights, which creates persistent legitimacy challenges (Santaniello and Barbieri, 2024), whereas authoritarian models achieve a seamless synergy for state control at the expense of societal trust and long-term innovative capacity (Conduit, 2023). The analysis demonstrates that public trust acts as a critical force multiplier for cybersecurity resilience across all regime types, and its erosion—whether through over-surveillance in democracies or coercion in autocracies—directly undermines a nation's defensive capabilities (Park and Kwon, 2024). Finally, the Central-Eastern

European cases reveal the formation of a distinctive subtype within the broader cooperative model, featuring governance patterns that deviate from the classic archetypes and offering crucial insights for strengthening intra-EU and transatlantic cyber resilience.

2 Methodology and analytical framework

This study employs a qualitative, comparative analytical methodology designed to capture the structural logics through which different political regimes integrate cybersecurity into their national security architectures. The aim is not merely to describe institutional arrangements, but to identify the underlying governance principles, patterns of authority concentration, and mechanisms of democratic or non-democratic control that shape the cybersecurity–national security nexus.

2.1 The structure of the inquiry

The research follows a structured, focused comparison across six country cases—Hungary, Slovakia, the United States, China, Russia, and Iran—selected on the basis of two criteria. First, each represents a mature or consolidating cybersecurity governance system with established national security linkages. Second, they collectively capture the principal regime types relevant to contemporary cyber governance: rule-of-law democracies and authoritarian cyber-sovereignty models. This design enables the identification of convergent institutional structures as well as divergent political logics.

2.2 Sources and data

The analysis is based on a triangulation of (1) national cybersecurity and national security legislation; (2) institutional documents, strategies, and publicly available oversight records; (3) relevant case law, particularly from the European Court of Human Rights; and (4) peer-reviewed academic literature on cybersecurity governance, surveillance oversight, and state–society relations. This multilayered source base allows the comparison to move beyond formal legal texts and incorporate the practical functioning of institutions.

2.3 Analytical perspectives on the cyber–national security nexus

To ensure comparability across diverse political systems, the study applies three analytical dimensions derived inductively from the literature and the preliminary case mapping:

1 The logic of dual governance structures—examining how cybersecurity legislation and national security frameworks interact, whether in tension or synergy, and how this relationship shapes the distribution of authority.
2 The effectiveness of independent oversight—assessing parliamentary, judicial, and administrative checks on national security powers related to cybersecurity, with particular attention to prior authorization, transparency, and proportionality standards.
3 Civil–state relations in the cybersecurity ecosystem—evaluating whether cooperation with private actors and civil society reflects voluntariness, regulated partnership, or legally enforced subordination.

These dimensions provide a consistent lens for identifying regime-specific patterns and cross-cutting differences.

To ensure analytical rigor and facilitate the replicability of our findings, the qualitative assessments presented—particularly in the comparative synthesis table (Table 1)—were operationalized according to a consistent set of criteria. For instance, the 'Strength of Independent Oversight' was coded based on a composite evaluation of three factors: (1) the legal requirement for prior, independent (preferably judicial) authorization for intrusive surveillance measures; (2) the documented practical effectiveness of parliamentary committees, assessed through public records and academic literature; and (3) the availability of effective legal remedies for citizens against state overreach, as interpreted in relevant case law. Similarly, the 'Nature of Civil–State Relations' was categorized along a spectrum from 'Voluntary partnership' to 'Full subordination' based on whether legal frameworks emphasize incentives and self-regulation, mandate compliance through reporting and auditing requirements, or legally compel private actors to serve as direct instruments of state security.

2.4 Comparative structure of the inquiry

The study employs a "most different systems" logic within each regime cluster. Hungary, Slovakia, and the United States differ institutionally yet share rule-of-law constraints; China, Russia, and Iran diverge culturally and institutionally but converge in authoritarian cyber-sovereignty practices. This approach allows the analysis to isolate the role of political regime type as the main explanatory factor across cases.

2.5 Limitations of the approach

The comparison focuses on national-level legislation and institutional mechanisms rather than operational cyber capabilities or intelligence practices unavailable through open sources. While this constitutes an inherent limitation, the selected analytical dimensions are sufficient to reveal the constitutional and governance structures that define each country's approach to cybersecurity and national security integration.

Furthermore, the selection of country cases, while purposefully designed to contrast major democratic and authoritarian archetypes alongside under-researched Central-Eastern European states, introduces a potential selection bias. The findings may not be generalizable to other types of political systems, such as those with different historical trajectories or distinct rule-of-law traditions. Future research could build upon this study's framework by expanding the comparative analysis to include a wider range of country cases.

3 Results: comparative analysis of national cybersecurity governance frameworks

This chapter presents the empirical findings of the study by analyzing the legal and institutional frameworks governing the intersection of cybersecurity and national security in two distinct clusters of states. The first section examines models operating within a rule-of-law framework—Hungary, Slovakia, and the United States—highlighting their shared challenges in balancing security with democratic oversight and fundamental rights, alongside their divergent institutional solutions. The second section analyses authoritarian models—China, Russia, and Iran—where cybersecurity governance is primarily instrumentalized as a tool for state control, surveillance, and regime stability.

3.1 Rule-of-law models: balancing security imperatives and fundamental rights

Governance models in democratic states are characterized by a persistent tension between the need for effective security measures and the obligation to uphold the rule of law. These frameworks typically feature constitutionally limited powers, mechanisms for parliamentary and judicial oversight, and a complex ecosystem of public-private cooperation. However, as the cases of Hungary, Slovakia, and the United States demonstrate, significant variations exist in how this balance is struck. These differences are shaped by distinct legal traditions, national security priorities, and, in the European context, the influence of supranational legal frameworks like those of the European Union.

3.1.1 The Hungarian hybrid model: state-centric control with EU overlays

According to the European Union Agency for Cybersecurity, the goal of cyber governance is to increase societal participation and cooperation in cyber-related measures, considering international agreements, strategies, and standards based on "good practices" [European Union Agency for Cybersecurity (ENISA), 2023]. Experience from recent decades confirms that a comprehensive governmental approach integrating all critical sectors is necessary in the field of cybersecurity (Cavelty and Egloff, 2019). Hungary, like other European states, treats cyberspace protection as a national security issue due to the all-of-society risk (Government resolution 1089/2025 (III. 31.) on Hungary's cybersecurity strategy 2025), resulting in regulations and an institutional structure that has led to the convergence of cybersecurity and national security tasks. Hungary's cybersecurity governmental approach operates through a dual regulatory structure that combines the traditional legal environment for national security with cybersecurity legislation. Hungarian cybersecurity regulations align with European Union directives and NATO cybersecurity principles (Pijpers et al., 2021). Act LXIX of 2024 on Hungary's cybersecurity (n.d.) defines the state framework for cybersecurity, regulating the protection of electronic information systems, as well as the tasks, competencies, procedures, and incident management rules for essential and important organizations. The legal status and powers of national security services, however, are established by the Act CXXV of 1995 on the National Security Services, 1995, which includes provisions for intervention in information systems to counter threats from cyberspace. These two pieces of legislation complement each other in delineating cyber defence authority-coordination functions from more traditional national security tasks.

The Hungarian cybersecurity model is hybrid and collaborative, with implementation built on three pillars (Liebetrau, 2022). In the civilian national security sector, the National Cyber Security Center (NCSC), operating within the National Security Special Service, performs general cyber authority and national incident response functions. In the defence sector, the defence cybersecurity authority is vested in the minister responsible for defence, while the defence cyber incident response center is operated by the Military National Security Service, which is also responsible for supporting military cyber operations. In civilian public administration, the Supervisory Authority for Regulatory Affairs oversees the cybersecurity certification of digital products and services. While this structure serves functional specialization, it simultaneously concentrates information gathering and intervention powers, which presents risks that need to be managed from the perspective of democratic control and the rule of law. Democratic oversight forms the basis for the legitimate operation of the national security system. In Hungary, the services' activities are subject to parliamentary committee control; however, this mechanism is often formal in practice and provides limited substantive oversight of sensitive areas of cybersecurity activities, such as monitoring electronic communications network traffic and taking measures necessary to interrupt cyberattacks. From a rule of law perspective, the greatest challenge is ensuring the proportionality and necessity of covert measures and state interventions in cyberspace (Soesanto and Smeets, 2021).

Hungarian regulation recognizes an active (and in some cases repressive) toolkit that goes beyond prevention. The Act on National Security Services expressly authorizes national security services to "intervene in information systems for the purpose of countering threats from cyberspace," within a covert information gathering framework subject to external authorization. In parallel, the Act on Cybersecurity makes it the task of the National Cyber Security Center to, among other things, analyze electronic communications network traffic without content for threat and attack detection, and further stipulates that the NCSC "executes or initiates" the measures necessary to interrupt an attack. Only a person designated by the Government may decide on the execution of the interruption. The measures must be necessary and proportionate, and must be consistent with national security, defence, law enforcement, and foreign policy interests as a tool of cyber deterrence (Soesanto and Smeets, 2021). From the perspective of the democratic legitimacy of measures, the supervisory and authorization procedures applied in these measures are crucial. In the case of Szabó and Vissy (2016), the European Court of Human Rights (ECtHR) found that the Hungarian framework for national security secret surveillance provides too broad authorization and lacks adequate guarantees of prior independent authorization and effective remedies, which is particularly relevant for the democratic control of network-level detection and system-level intervention. This standard was further refined in Big Brother Watch and Others v. the United Kingdom (Grand Chamber, 2021) and Centrum för rättvisa v. Sweden (Centrum för rättvisa v. Sweden, grand chamber, app. No. 35252/08 (European court of human rights, 25 June 2021), n.d.): bulk techniques and covert surveillance systems are only compatible with Article 8 of the Convention with "end-to-end" safeguards (preferably judicial, prior authorization; narrow, foreseeable purpose and category system;

strict selection and access rules; continuous independent supervision; detailed logging; substantive ex post control; and—where possible—delayed notification; Zalnieriute, 2022). These standards were confirmed in Ekimdzhiev and others v. Bulgaria, app. Nos. 70078/12 and 5 others (European court of human rights, 11 January 2022) (2022). These standards, applied to the Hungarian hybrid, collaborative model, require that alongside the concentration of service and defence cyber operational powers and network monitoring, truly independent ex ante authorization, external and ex post control ensure the enforcement of fundamental rights. These requirements are not merely legal-technical guarantees but minimum conditions for the democratic legitimacy of state cybersecurity intervention in a multi-actor ecosystem, as they delineate the "constitutional interface" through which the state's monopoly on coercion can be reconciled with the involvement of market, academic, and civil capacities. The acceptability of intervention stems not only from the severity of the threat but from accountability, which creates the basis of trust for cooperation.

The integration of cybersecurity into the Hungarian legal system stems partly from the state's defence function in the Hobbesian sense, thus guaranteeing security remains the exclusive task of the state. However, in the digital sphere, this responsibility is shared: alongside the state, economic actors, universities, and civil society are also participants in the cyber defence ecosystem (Kianpour et al., 2025). The Hungarian cybersecurity ecosystem includes the civil, economic, and scientific spheres, as university and industry actors also participate in strategic planning through the National Cybersecurity Forum. However, cooperation is typically consultative, not decision-making, so the role of civil control is limited. This operational model aligns with broader trends in the country's governance, where indicators measuring the accountability of executive and legislative branches have shown a significant decline over the past two decades (Freedom House, 2024). In such an environment, fostering trust-based, strategic partnerships in sensitive security areas becomes inherently challenging. Civil-state partnership is not merely a technical but a constitutional issue; the rule of law can only be enforced in cyberspace if society is part of shaping security decisions. International experience (Jardine et al., 2024) shows that civil involvement does not reduce the state's capacity for action but increases public trust and resilience. Actualizing social control would require regular public reports of decision-making processes and the expansion of citizen remedy channels, the latter is currently absent in practice. During the management of cybersecurity crisis situations, the Operational Task Force and the National Cybersecurity Working Group receive a directing role, but their decision-making is not public, and there are no mandatory transparency requirements for civil feedback. The level of democratic oversight in Hungary is limited: although parliamentary control formally exists, due to the overlap of cybersecurity and national security functions, decision-making remains within the closed circles of the executive branch, without parliamentary control.

3.1.2 The Slovak centralized model: aligning with the EU'S NIS directive

The legal and institutional framework forms the backbone of Slovakia's approach to cybersecurity as a dimension of national security. It determines the distribution of competences, the scope of obligations imposed on public and private actors, and the mechanisms of coordination among state institutions. Understanding this framework is therefore essential to evaluate how Slovakia integrates cybersecurity into its broader national security strategy and how effectively democratic oversight and rule-of-law safeguards are embedded within it.

The cornerstone of Slovak cybersecurity legislation is Act No. 69/2018 Coll. on Cybersecurity, which established obligations for operators of essential and digital services, defined risk management principles, and required incident reporting to the NBÚ SR (Act no. 69/2018 Coll. On cybersecurity, 2018). This Act transposed Directive (EU) 2016/1148 [Directive (EU) 2016/1148, 2016], integrating cybersecurity into national security and critical infrastructure protection. In December 2024, Act No. 366/2024 Coll. was adopted, amending the Cybersecurity Act to transpose Directive (EU) 2022/2555 (NIS2) into Slovak law (Act no. 366/2024 Coll. Amending act no. 69/2018 Coll, 2024). The reform transformed the Slovak system into a risk-based model emphasizing accountability, executive liability, and modernized sanction mechanisms [NBÚ SR (National Security Authority), 2024]. According to the Ministry of Investment, Regional Development and Informatization (MIRRI SR), this amendment represents a 'full functional transposition of NIS2' [MIRRI SR (Ministry of Investment, Regional Development and Informatization), 2024]. However, transitional provisions delay certain obligations, such as the establishment of sectoral CSIRTs and staff certification, until 2026 (Government Office SR, 2024). The NBÚ SR's 2023 report indicated that around 50% of obligated entities had not met audit and reporting requirements, revealing capacity gaps rather than legislative deficiencies [NBÚ SR (National Security Authority), 2023]. Despite these implementation challenges, Slovakia's legislative framework demonstrates a high degree of alignment with EU standards and establishes a solid legal foundation for the institutional system that underpins national cybersecurity governance. The gradual shift from formal compliance to proactive risk management reflects the country's effort to balance technical regulation with strategic resilience objectives.

Slovakia's cybersecurity governance combines functional centralization with sectoral specialization. The National Security Authority (NBÚ SR) acts as the national competent authority, overseeing compliance and certification, and operates the National Cybersecurity Center SK-CERT, which handles incidents of national and strategic relevance. Concurrently, the Ministry of Investment, Regional Development and Informatization (MIRRI SR) manages the governmental CSIRT. SK team, responsible for cybersecurity incidents within public administration and e-government systems (Smernica, 2024). Other ministries contribute complementary roles: the Ministry of Defence directs military cyber operations (Ministry of Defence SR, 2024), the Ministry of Interior investigates cybercrime, and the Ministry of Foreign and European Affairs coordinates cyber diplomacy (Government of the Slovak Republic, 2021).

Democratic oversight of cybersecurity governance in Slovakia continues to develop within the existing legal framework. The National Council's Committee on Defence and Security holds the mandate to review the activities of the National Security Authority (Národný bezpečnostný úrad—NBÚ SR), although access to classified operational information is naturally restricted due to confidentiality requirements (National Council of the Slovak Republic, 2023). Consequently, parliamentary scrutiny primarily focuses on legislative and strategic aspects rather than detailed operational oversight.

However, this oversight is hampered by significant structural weaknesses. The Act on Cybersecurity grants the NBÚ SR broad powers to block harmful content in cyberspace without prior judicial authorization (Sokol and Rózenfeldová, 2025). Furthermore, the legal framework lacks a mandate for systematic ex-post parliamentary oversight of such interventions, creating a significant democratic accountability gap (West, 2023; Kovanič and Coufalova, 2020; Chovancová, 2016).

This institutional configuration reflects a broader European effort to balance national security imperatives with rule-of-law safeguards. In Slovakia, independent judicial authorization for cybersecurity measures is still being refined within the national legal system, while constitutional guarantees under Articles 19 and 22—protecting privacy and the secrecy of correspondence—continue to serve as a guiding principle. Relevant case law of the European Court of Human Rights, particularly Szabó and Vissy v. Hungary (2016) and Big Brother Watch v. United Kingdom (2021), highlights the importance of prior independent oversight of digital surveillance (European Court of Human Rights, 2016, 2021). However, the effectiveness of prior judicial approval for the most intrusive measures is undermined by systemic challenges to judicial independence and impartiality, an issue previously highlighted in ECtHR critiques of the Slovak legal system (Hron and Illýová, 2025; Vaško, 2022; Knutelská, 2011; Lukáč et al., 2025). The European Union Agency for Fundamental Rights (FRA) has noted that several EU Member States, including Slovakia, continue to develop more comprehensive oversight mechanisms [FRA (European Union Agency for Fundamental Rights), 2022]. Overall, Slovakia's approach demonstrates substantial alignment with European legal standards, while offering scope for the gradual enhancement of parliamentary and judicial oversight to further strengthen democratic accountability in cybersecurity governance.

Cooperation between the state and private operators forms a key component of Slovakia's cybersecurity system. Private providers of essential and digital services are required to report incidents and conduct regular cybersecurity audits under the supervision of the National Security Authority (Národný bezpečnostný úrad—NBÚ SR; Act no. 69/2018 Coll. On cybersecurity, 2018). However, the relationship remains largely confined to compliance-driven mechanisms rather than strategic, trust-based collaboration. This deficit is rooted in significant legal, cultural, and economic barriers. Culturally, a pervasive 'compliance-driven' mindset, often stemming from a post-communist legacy of state-centric control, and a mutual 'blaming culture' discourage the open information sharing essential for effective partnership (Calcara et al., 2022; Pollini et al., 2022). This underlying trust deficit is empirically evidenced by the National Security Authority's (NBÚ SR) 2023 report, which found that approximately 50% of obligated entities failed to meet their mandatory audit requirements—a figure that points not only to capacity gaps but also to a fundamental lack of proactive engagement from the private sector [NBÚ SR (National Security Authority), 2023]. Economically, significant resource constraints also hamper the capacity of both state and private actors to engage in more robust joint activities (Mishra et al., 2022). The structured involvement of private entities in strategic cybersecurity policy-making is gradually developing, offering opportunities to deepen public–private collaboration. Data exchange between state authorities and private operators is primarily based on bilateral arrangements, while aggregated statistical insights are shared selectively. Continued improvements in transparency and communication can further reinforce societal trust and participatory governance.

In comparison, several EU Member States—such as Estonia and the Netherlands—have adopted more inclusive models by institutionalizing dialog through Information Sharing and Analysis Centers (ISACs) and National Cybersecurity Forums (Jardine et al., 2024). In Slovakia, cooperation is formalized in the National Cybersecurity Strategy 2021–2025, which provides for a Steering Committee to coordinate implementation of the Action Plan, involving all stakeholders and conducting annual reviews; Act No. 69/2018 Coll. likewise obliges the Authority to cooperate with other state bodies, CSIRT units and operators of essential services (Act no. 69/2018 Coll. On cybersecurity, 2018; Government of the Slovak Republic, 2021).

3.1.3 The US decentralized model: public-private partnership and advisory governance

The United States operates the world's most sophisticated yet deeply paradoxical cybersecurity governance system. It simultaneously projects two contradictory faces to domestic and international audiences: a highly visible, liberal-market-oriented public-private partnership model that celebrates voluntary cooperation and industry self-regulation, and a largely invisible, constitutionally contested national-security surveillance apparatus that relies on compulsory bulk collection and secret legal authorities (Atkins and Lawson, 2021; Weiss and Krieger, 2025). This duality is not accidental but structurally embedded, reflecting both ideological commitment to limited government intervention in the economy and an uncompromising post-9/11 interpretation of national security imperatives.

The "public face" is built on advisory coordination and voluntary frameworks rather than binding regulation. The Cybersecurity and Infrastructure Security Agency (CISA), established in 2018 under the Department of Homeland Security, is the principal civilian coordinator for critical infrastructure protection. Despite its ambitious mandate, CISA's authority remains largely advisory: it issues alerts, deploys detection tools, coordinates incident response, and can issue Binding Operational Directives—yet these are mandatory only for federal civilian agencies, not private operators of critical infrastructure (CISA, 2015). Similarly, the widely respected NIST Cybersecurity Framework (CSF 2.0 as of 2024) and Special Publication 800–53 remain strictly voluntary standards that private entities adopt only when market forces, insurance requirements, or contractual obligations demand it (NIST, 2020; NIST, 2024).

The flagship legislative attempt to institutionalize cooperation—the Cybersecurity Information Sharing Act of 2015 (CISA, 2015)—aimed to remove legal and liability barriers to voluntary threat-indicator sharing between government and industry. Despite initial optimism, participation has been persistently underwhelming. Empirical studies of the financial services sector, long considered the most advanced example of US public-private partnership through the FS-ISAC, reveal enduring trust deficits, asymmetric information flows, and competitive disincentives that severely limit timely bidirectional sharing (Atkins and Lawson, 2021; Ullah et al., 2024). Firms fear reputational damage, regulatory second-order effects, and potential misuse of shared data by government agencies, while the absence of mandatory reporting requirements creates classic collective-action problems in a highly competitive

environment. As a result, even after major incidents such as SolarWinds (2020) and Colonial Pipeline (2021), significant "regulatory gaps" persist (Atkins and Lawson, 2021; The White House, 2023).

The "hidden face" of the model is the vast national-security surveillance architecture anchored in Section 702 of the Foreign Intelligence Surveillance Act (Foreign Intelligence Surveillance Act of 1978, 1978; FISA §702, as reauthorised in 2018 and again in 2024) and residual authorities from the USA PATRIOT Act of 2001 (USA PATRIOT act of 2001, 2001). These statutes authorize the National Security Agency (NSA) to conduct warrantless collection of both content and metadata of communications whenever at least one communicant is reasonably believed to be a non-US person located abroad—a category that inevitably sweeps in massive volumes of purely domestic US person communications ("incidental collection"). The NSA's unique "dual-hat" leadership of both foreign signals intelligence (SIGINT) and the Cybersecurity Directorate creates a profound conflict of interest: the same organization tasked with defending private networks against foreign adversaries is simultaneously the world's most prolific collector of private communications, including those of the very firms it claims to protect (Weiss and Krieger, 2025).

This arrangement generates acute rule-of-law tensions. The Fourth Amendment's guarantee against unreasonable searches and seizures is significantly weakened in the digital domain, particularly for data stored or transiting overseas. Oversight is delegated to the secretive Foreign Intelligence Surveillance Court (FISC), which operates ex parte, publishes almost no opinions, and historically approved 99–100% of government applications even after the 2013 Snowden disclosures revealed systematic overreach (Donohue, 2016; Edgar, 2024). Civil liberties scholars argue that the combination of bulk collection programs (historically PRISM and Upstream) and minimization procedures that permit querying US person identifiers without judicial warrant constitutes a de facto general warrant regime prohibited by the Founders (Donohue, 2016; Goitein, 2023).

The 2023 National Cybersecurity Strategy explicitly acknowledges the failures of the purely voluntary model and attempts a partial rebalancing by shifting greater responsibility onto technology manufacturers and critical infrastructure operators (The White House, 2023). Yet it deliberately avoids imposing EU-style comprehensive regulation, maintaining the fundamental liberal-market philosophy. Meanwhile, Section 702 was reauthorized in April 2024 with only modest reforms, preserving the core surveillance authorities despite documented abuses (Edgar, 2024).

Thus, the American model remains caught in a structural contradiction: under-regulated in its civilian partnership face and overreaching in its surveillance face. This duality produces persistent legitimacy deficits both domestically and internationally. Domestically, the erosion of public trust in government handling of private data has been consistently documented in public opinion surveys since the 2013 Snowden disclosures, creating a lasting barrier to deeper public-private cooperation (Goitein, 2023). Internationally, the model faces accusations of digital hegemony and extraterritorial overreach. While the system has proven remarkably resilient and adaptive, its internal tensions continue to generate political controversy and constitutional litigation, making the United States a uniquely ambivalent global standard-setter in cybersecurity governance.

3.2 Authoritarian models: cybersecurity as a tool for state control

Authoritarian states approach the nexus of cybersecurity and national security not as a balancing act with fundamental rights, but as an opportunity to reinforce regime stability and extend state power over the digital sphere. These models are characterized by the principle of "digital sovereignty," the subordination of the private sector to state security organs, and the use of cybersecurity infrastructure for mass surveillance and the suppression of dissent. The legal frameworks in China, Russia, and Iran, while distinct in their specifics, share a common logic: the law serves as an instrument of control, rather than a constraint on power.

3.2.1 The Chinese authoritarian cybersecurity model: sovereignty, control, and selective flexibility

China's cybersecurity governance is anchored in a dual legal framework that intertwines universal intelligence obligations with targeted sectoral regulations. The 2017 National Intelligence Law (NIL) mandates that all organizations and citizens assist state intelligence efforts (Article 7), effectively conscripting private entities into the security apparatus (Creemers, 2022). Complementing this are the 2017 Cybersecurity Law (CSL), the 2021 Data Security Law (DSL), and the 2021 Personal Information Protection Law (PIPL) (Cybersecurity Law of the People's Republic of China, 2017; Data Security Law of the People's Republic of China, 2021; Personal Information Protection Law of the People's Republic of China, 2021), which establish a hierarchical data classification system—encompassing "core," "important," and "national core" data—and impose stringent obligations on operators of critical information infrastructure (CIIOs) to localize data and undergo security assessments for cross-border transfers (Guo and Li, 2024; Cheng, 2022). Central to enforcement is the Cyberspace Administration of China (CAC), a multifunctional body that regulates, audits, catalogs prohibited foreign technologies, and exercises content oversight, often with opaque criteria that prioritize national security (Creemers, 2023; Wei, 2022).

Ideologically, the model is underpinned by "cyberspace sovereignty" (wangluo zhuquan), which posits the state's exclusive authority over digital infrastructure, data flows, and content within its borders, rejecting Western notions of a borderless internet in favor of territorial control (Creemers, 2022; Ramich and Piskunov, 2022). This principle is operationalized through technical mechanisms like mandatory data localization—requiring personal and "important" data to remain on domestic servers—and CAC-mandated security reviews for outbound transfers, whose vague definitions of "critical data" enable discretionary state intervention to avert perceived threats (Guo and Li, 2024; Creemers, 2023). Recent amendments, including the 2024 Network Data Security Management Regulations, signal selective relaxation for non-sensitive digital trade to bolster economic integration, yet reinforce core controls (Bird and Bird, 2025).

In implementation, private tech firms are legally bound to furnish data and technical aid to security organs (NIL Article 14; CSL Article 28), rendering conglomerates like Alibaba and Tencent de facto extensions of state surveillance while granting them leeway when commercial goals align with regime stability (Aho and Duffield, 2020; Wang et al., 2024). This symbiosis extends to societal control: the

Great Firewall enforces layered censorship—delegated to firms via self-policing—while mass surveillance systems like Skynet and the Social Credit System enable real-time monitoring and pre-emptive repression under the guise of "social stability" (Aho and Duffield, 2020; Trevaskes, 2024). The CAC's 2023 vulnerability disclosure rules further integrate private reporting into a unified "chess game" of threat sharing, blending economic incentives with political coercion (Cary, 2024).

Critically, this framework embodies "rule by law," where statutes serve Party objectives rather than constrain power. Broad, ambiguous terms like "national security" and "critical infrastructure" facilitate overreach, sidelining privacy under PIPL exceptions and curtailing judicial review, as courts rarely challenge CAC decisions (Wei, 2022; Creemers, 2023). While fostering innovation—evidenced by reduced cost stickiness post-CSL (Wang et al., 2024)—the model entrenches authoritarianism, diverging sharply from liberal multi-stakeholder paradigms (Ramich and Piskunov, 2022).

3.2.2 The nexus of cybersecurity and national security in Russia: a model of digital sovereignty and state control

Russia's authoritarian cyber-security model rests on a dual legal-institutional framework that grants the state comprehensive operational, technical, and content control over the national internet segment (RuNet) while instrumentalising private-sector infrastructure. Three interlocking legislative pillars form its core: the Sovereign Internet Law (Federal Law No. 90-FZ of 1, 2019), the Data Localization Law (Federal Law No. 242-FZ of 21, 2015), and the Yarovaya package (Federal law no. 374-FZ, 2016). These laws are enforced primarily by two agencies: the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), responsible for content blocking, registration, and fining, and the Federal Security Service (FSB), which conducts operative-technical surveillance and operates the System for Operative Investigative Activities (SORM; Epifanova, 2020; Litvinenko, 2021; Moyakine and Tabachnik, 2021).

The ideological foundation of the model is "digital sovereignty," which justifies the transformation of the Russian internet into a controllable, potentially isolatable space. The 2019 Sovereign Internet Law mandated the installation of Deep Packet Inspection (DPI) equipment in ISP networks under Roskomnadzor supervision, enabling real-time identification and blocking of prohibited content, as well as centralized traffic routing through state nodes. It also required the creation of an independent national Domain Name System and routing infrastructure capable of sustaining RuNet autonomy in the event of external disconnection (Ermoshina et al., 2021; Glasze et al., 2023). Regional disconnection exercises conducted between 2019 and 2021 demonstrated the system's technical feasibility (Ermoshina et al., 2021).

Private-sector subordination is achieved primarily through the Yarovaya package and the long-standing SORM framework. Telecommunication providers and "organizers of information dissemination"—a category that can include foreign internet companies—must store metadata for 3 years and communication content (voice, text, images, video) for 6 months, and hand over encryption keys or decryption capabilities to the FSB upon request without judicial warrant. The Data Localization Law complements this by mandating storage of Russian citizens' personal data on domestic servers, thereby guaranteeing FSB access (Taylor, 2020; Moyakine and Tabachnik, 2021; Sivetc, 2021).

In practice, these instruments have been weaponized for political repression, most dramatically since the 2022 invasion of Ukraine. The "fake news" amendments (Federal law no. 32-FZ, 2022) introduced penalties of up to 15 years' imprisonment for disseminating information contradicting the official narrative, enabling the rapid blocking of independent media outlets (Meduza, Dozhd, Echo Moskvy) and Western platforms (Facebook, Instagram, Twitter/X). The combination of DPI systems and centralized blacklists allowed thousands of websites to be rendered inaccessible within hours, while VPN and proxy circumvention tools have been systematically degraded (Kaye, 2022; Ermoshina et al., 2021).

From a rule-of-law perspective, the Russian model exhibits profound deficiencies. Independent judicial oversight is effectively absent: FSB demands for decryption occur without court approval, statutory definitions such as "extremist activity" or "incitement to mass riots" remain deliberately vague, and proportionality or necessity tests are never applied. Privacy and freedom of expression are consistently subordinated to nebulous state-security imperatives, transforming ostensibly cyber-security measures into instruments of comprehensive political control (Moyakine and Tabachnik, 2021; Sivetc, 2021).

3.2.3 Iran: a theocratic model of digital sovereignty and repression

Iran has developed one of the world's most sophisticated authoritarian cybersecurity architectures, centered on the National Information Network (NIN, locally known as SHOMA). Officially framed as a strategic project to secure "digital sovereignty" and protect Islamic-Iranian cultural identity, the NIN aims to create a fast, inexpensive national intranet while progressively isolating citizens from the global internet (Supreme Council of Cyberspace, 2012; Supreme Council of Cyberspace, 2017). Strategic oversight is exercised by the Supreme Council of Cyberspace (SCC), established in 2012 by order of the Supreme Leader and chaired by the President, which subordinates all cyber-policy decisions to theocratic-political priorities enshrined in Articles 44 and 175 of the Constitution of the Islamic Republic of Iran (Supreme Council of Cyberspace Founding Decree, 2012; Constitution of the Islamic Republic of Iran, 1979). At the operational level, the Islamic Revolutionary Guard Corps (IRGC) cyber units and the Ministry of Intelligence and Security (MOIS) dominate both offensive/defensive capabilities and domestic surveillance, despite persistent institutional rivalry (Serscikov, 2025; Keremoğlu and Weidmann, 2020).

Technically, the NIN rests on massive domestic data-center construction and the mandatory routing of local traffic through state-controlled infrastructure. Internet service providers (ISPs) are legally obliged to filter content, throttle international bandwidth, and hand over user data on demand (Dal and Nisbet, 2022). The controversial "Regulatory System for the Protection of Users in Cyberspace" bill (commonly known as the Protection Bill, debated 2022–2024) sought to institutionalize this control further by mandating data localization, forcing foreign platforms to appoint local representatives, criminalizing unapproved VPNs, and granting authorities direct bandwidth-allocation powers (Protection Bill, 2022; Freedom House, 2024). Domestic platforms such as Soroush and Facenema

consequently enjoy preferential speed and pricing, creating a de-facto walled garden (Yalcintas and Alizadeh, 2020).

The repressive potential of this architecture was dramatically demonstrated during the 2022–2023 Woman, Life, Freedom protests following Mahsa Amini's death. Authorities imposed the longest and most comprehensive internet shutdowns ever recorded, combined near-total international traffic blocks with permanent bans on Instagram and WhatsApp, and deployed deep-packet inspection and mandatory national-ID-linked SIM registration to identify and arrest thousands of protesters (Earl et al., 2022; Feldstein, 2021).

Despite its sophistication, the model remains constrained. Legally, it operates with virtually no independent judicial oversight, violating constitutional guarantees of privacy and freedom of expression (Constitution of the Islamic Republic of Iran, 1979, Arts 23–25). Institutionally, rivalry between the IRGC and MOIS fragments coordination (Serscikov, 2025). Socially, widespread VPN use, mesh networks, and creative encryption continue to undermine state control, proving that even advanced digital repression is neither technically nor socially impermeable (Dal and Nisbet, 2022; Feldstein, 2021).

4 Divergent trajectories in the governance of the cybersecurity-national security nexus

The findings presented in the previous chapter reveal a stark divergence in how states govern the nexus of cybersecurity and national security. While all examined countries have developed complex legal frameworks to address digital threats, the underlying logic of how national security imperatives are integrated with cybersecurity measures differs profoundly. Rule-of-law models emphasize transparency, accountability, and multi-stakeholder participation to build public trust and balance security with human rights, whereas authoritarian approaches prioritize centralized control, state sovereignty, and rapid mobilization, often at the expense of civil liberties (Jaber, 2025; Malvenishvili, 2023). Indeed, in authoritarian systems, the absence of public trust is not a system failure but a design feature; governance is predicated on coercion and top-down mobilization rather than voluntary cooperation, rendering empirical measures of trust both unobtainable and conceptually secondary to the model's functioning (Wang and Han, 2025). This chapter moves beyond the descriptive analysis of individual models to a comparative synthesis, interpreting the results to answer how different political regimes structure this critical relationship. To do so, this discussion will compare the rule-of-law and authoritarian models across three dimensions that emerged from the case studies: first, the nature and internal logic of the dual legal-institutional structures that link national security agencies with cybersecurity authorities; second, the practical effectiveness of oversight mechanisms intended to ensure the accountability of these fused powers (Santaniello and Barbieri, 2024); and third, the prevailing models of civil-state cooperation in this hybrid security domain (Park and Kwon, 2024). Through this analysis, we can identify the fundamental fault lines that separate democratic and authoritarian approaches to governing the cybersecurity-national security nexus and explore the distinct trade-offs each model presents in terms of crisis adaptability, innovation, and long-term legitimacy (Boeke, 2018; Wang and Han, 2025).

4.1 The logic of dual structures: convergence in form, divergence in function

A central finding of this comparative analysis is that both rule-of-law and authoritarian states have converged on a functionally similar dual legal-institutional structure to govern the cybersecurity-national security nexus. In each case, a broad, pre-existing national security framework coexists with a newer, more specific body of cybersecurity legislation. This formal convergence is striking: in Hungary, the Act on National Security Services operates alongside the Act on Cybersecurity; in the United States, the Foreign Intelligence Surveillance Act (FISA) provides the national security mandate while the Cybersecurity Information Sharing Act (CISA) governs partnership; in China, the National Intelligence Law (NIL) underpins the Cybersecurity Law (CSL); and in Russia, the operational powers of the FSB complement the technical controls of the "Sovereign Internet Law."

However, this convergence in form masks a profound divergence in function and purpose. In rule-of-law models, these two pillars exist in a state of structural tension. The relationship is ideally one of checks and balances, where cybersecurity partnerships are meant to be transparent and rights-respecting, while the more opaque national security surveillance powers are—in theory—constrained by legal and procedural safeguards (Karim et al., 2019). The American model exemplifies this tension in its most extreme form, creating a paradoxical system where the "public face" of voluntary partnership coexists uneasily with the "hidden face" of mass surveillance under FISA, generating persistent legal and political conflict. The Central European models, influenced by EU law, attempt to formally integrate these pillars, but still grapple with the inherent friction between state security prerogatives and the procedural rights demanded by supranational legal norms (Kelemen et al., 2024b).

In stark contrast, authoritarian models are designed not for tension but for synergy. The dual structures do not check but rather amplify state power. The national security legislation (e.g., China's NIL, Russia's laws on extremism) provides the overarching ideological justification and coercive authority—the "why"—while the cybersecurity laws (e.g., China's CSL, Russia's Yarovaya package) deliver the specific technical and legal instruments for implementation—the "how." This fusion creates a powerful apparatus for social control, where cybersecurity measures become indistinguishable from tools of state surveillance and repression (Conduit, 2023). The principle of "cyber sovereignty," central to these regimes, explicitly legitimizes this fusion, framing the extension of state control into the digital realm as a necessary act of national self-defence (Wang, 2016; Hung, 2025). Thus, while the architectural blueprint appears superficially similar across regimes, its application reveals a fundamental divide: one system is designed to manage and constrain power, the other to maximize and project it.

4.2 The reality of oversight: from flawed guarantees to formalized absence

The most significant divergence between rule-of-law and authoritarian governance models lies in the role and effectiveness of

independent oversight mechanisms. While authoritarian systems are defined by the formalized absence of meaningful accountability, the case studies reveal that even in democratic states, the oversight of powers at the cybersecurity-national security nexus is often procedurally flawed and practically ineffective.

Authoritarian models systematically dismantle or co-opt any form of independent oversight. In China, Russia, and Iran, parliamentary bodies and courts function as instruments of the executive, not as checks upon it. Legal frameworks are intentionally crafted with ambiguous terms like "national security" or "extremist activity," which grants security agencies (the CAC, FSB, and IRGC) virtually unlimited discretion (Wei, 2022; Sivetc, 2021). The legal process is inverted: rather than constraining power, the law is used to legitimize its arbitrary exercise, a clear manifestation of "rule by law" (Schumann, 2025). In these systems, judicial or parliamentary review of surveillance or content-blocking decisions is either non-existent or a mere formality, leaving no effective remedy for citizens against state overreach (Donais, 2017).

In contrast, rule-of-law models formally embed both parliamentary and judicial oversight, yet these guarantees are consistently weakened when confronted with national security imperatives. In Hungary and Slovakia, parliamentary committee oversight is often described as a mere formality, hampered by the dominance of the governing majority and a lack of technical expertise to scrutinize complex cyber operations (West, 2023; Kovanič and Coufalova, 2020). More critically, the case law of the European Court of Human Rights (Szabó and Vissy v. Hungary; Big Brother Watch v. UK) reveals systemic deficiencies in prior judicial authorization for secret surveillance across Europe, a critique that applies directly to the weak judicial safeguards in both the Hungarian and Slovak systems (Zalnieriute, 2022; Hron and Illýová, 2025).

The United States presents a unique paradox. It possesses a highly institutionalized oversight body in the Foreign Intelligence Surveillance Court (FISC), yet its effectiveness is deeply contested. Operating in secret, with an ex parte process where only the government's case is heard, the FISC has historically approved over 99% of surveillance applications (Donohue, 2016). This has led critics to argue that the court functions more as a legitimizing rubber stamp than as a robust check on the executive, particularly concerning the NSA's bulk collection programs under FISA Section 702 (Goitein, 2023).

Thus, while a clear line separates the formalized absence of oversight in authoritarian states from the flawed guarantees in democracies, the latter are far from a complete solution. The "national security" justification tends to create a zone of exception where executive power expands, and judicial and legislative scrutiny recedes, even within otherwise robust constitutional systems (Perriello, 2024). The critical difference, however, remains: in democracies, these deficiencies are subject to public debate, legal challenge, and potential reform, whereas in authoritarian systems, they are a deliberate feature of the design.

4.3 The civil–state relationship: from partnership to subordination

The models examined in the previous chapter delineate three distinct types of civil–state relations, ranging from voluntary, incentive-based partnership (United States), through regulated partnership with mandatory elements (EU Member States: Hungary and Slovakia), to legally enforced, complete subordination (authoritarian models). The more the state's control over cyberspace becomes totalised, the more the private sector is transformed into an extended executive arm of the state; conversely, in democratic models, it is precisely the lack of trust and voluntariness that constitutes the greatest practical limitation.

In states implementing authoritarian/totalitarian models, compulsory subordination is observed, as exemplified by China (National Intelligence Law of the People's Republic of China, 2017, Article 7), Russia (Yarovaya Package 2016, Sovereign Internet Law 2019) and Iran (National Information Network and Protection Bill 2022–2024). In these countries, legal provisions explicitly oblige the private sector to provide immediate and unrestricted data, surrender decryption keys, and actively participate in censorship and surveillance. Companies do not function as partners but as operative executors of state control. The principle of "no right of refusal" (China), the mandatory deployment of DPI-based filtering systems (Russia), and the state-supported domestic platforms favored by pricing policy (Iran) structurally embed the private sector into the surveillance–repressive apparatus serving regime stability.

The democratic model based on voluntary, incentive-driven partnership is most characteristically represented by the United States. The voluntary public-private partnership model emphasized by the Cybersecurity Information Sharing Act (CISA, 2015) and the 2023 National Cybersecurity Strategy is, in principle, built on mutual benefits and trust. In practice, however, the lack of trust (lingering effects of the Snowden revelations and data privacy scandals), the unidirectional nature of liability protection, and market logic (cost of security investment versus profit) leave a significant portion of critical infrastructure under-protected. For this reason, the 2023 Strategy explicitly formulates the objectives of "rebalancing the responsibility to defend cyberspace" and "realigning incentives," thereby acknowledging that voluntariness alone is insufficient.

The European Union follows a distinct regulatory model. The regulated partnership interwoven with mandatory elements is characteristic of the EU as a whole and thus of the two countries examined. This is illustrated by the compulsory incident reporting, audits and risk management required by the NIS/NIS2 Directives, meaning that partnership is not entirely voluntary. At the same time, neither Hungary nor Slovakia possesses the coercive toolkit found in authoritarian models (no mandatory backdoors, no obligation to surrender keys, no DPI requirement for ISPs). Here, the principal problem is not the degree of legal compulsion but the absence of deeper, strategic cooperation: the private sector continues to operate primarily in a compliance-driven mindset; due to a "blame culture" and mutual distrust, genuine, proactive information-sharing does not emerge (see the 2023 NBÚ report for Slovakia: approximately 50% of obliged entities failed to meet even the audit requirements). The National Cybersecurity Forum (Hungary) and the Steering Committee of the National Cybersecurity Strategy (Slovakia) perform a consultative rather than decision-making role. While both countries exhibit this pattern of state-centric, consultative partnership, a notable difference lies in their institutional architecture: Slovakia maintains a more centralized model with the National Security

Authority (NBÚ SR) as the single national competent authority, whereas Hungary's 'hybrid model' distributes key functions across civilian, military, and regulatory bodies, potentially creating greater coordination challenges.

4.4 Comparative synthesis and policy recommendations for rule-of-law models

In the three democratic models examined, the relationship between cybersecurity and national security exhibits persistent tension. This tension—compounded by the limited scope of independent oversight and the only partial strategic depth of civil–state relations—produces moderate operational effectiveness and a legitimacy deficit (Table 1).

Drawing on the findings of the preceding chapters, the future development of democratic cyber governance should be guided by a triple balancing principle—transparency, innovation, and the protection of fundamental rights. This principle is formulated here as a set of recommendations adaptable to all rule-of-law states:

1 While preserving the existing dual regulatory structure (cybersecurity law alongside national security law), guarantees of transparency, verifiability, and proportionality must be codified and institutionalized in full conformity with the "end-to-end safeguards" developed in ECtHR case law, particularly with respect to network-level monitoring and system-level interventions.
2 The current consultative forums for civil–state cooperation (e.g., the Hungarian National Cybersecurity Forum, the Slovak Steering Committee, and the sector-specific ISACs in the United States) should be transformed into a Cyber Governance Council endowed with genuine decision-preparation and, where appropriate, co-decision powers, in which critical infrastructure operators, academia, and civil society are represented on a paritary basis.
3 To stimulate innovation and proactive engagement, positive incentives should be introduced (tax relief, reduced cyber-insurance premiums, state-backed guarantee funds) that reward exceeding the minimum requirements laid down in cybersecurity regulation and encourage strategic-level information-sharing.
4 In order to sustain democratic legitimacy, a regular, anonymized yet substantive public reporting obligation must be imposed concerning major incidents and measures of national security relevance.

Implementation of these recommendations would enable rule-of-law models to integrate cybersecurity into the national security framework not as an instrument of exclusive state control, but as a transparent, innovation-driven, and fundamental-rights-compliant governance system. This would ensure continued alignment with Euro-Atlantic constitutional standards while simultaneously enhancing societal resilience.

5 Conclusion

The elevation of cybersecurity to a core domain of state security has inevitably extended national-security practices into the digital realm, creating one of the twenty-first century's most profound constitutional dividing lines. The comparison of six states clearly demonstrates that there is no continuum, only a rupture, between rule-of-law and authoritarian governance logics. Where democratic states attempt to bridge the trust deficit by extending the national-security exception into cyberspace, they undermine their own legitimacy. Where authoritarian states instrumentalize cybersecurity for regime stability, they purchase short-term effectiveness at the price of long-term societal and technological fragility.

TABLE 1 Comparative analysis of cybersecurity governance models, oversight mechanisms, and public trust dynamics in the six case countries (United States, Hungary, Slovakia, China, Russia, Iran).

Country	Relationship between cybersecurity and national security (tension vs. synergy)	Strength of independent oversight in national security-related cyber measures	Nature of civil–state relations in the cybersecurity–national security nexus
Hungary	Tension (hybrid model with concentration of powers)	Exists but limited (parliamentary oversight formal; lack of prior judicial control)	Regulated partnership (mandatory but consultative)
Slovakia	Tension (centralised NIS2 framework alongside national security dimension)	Exists but developing (limited parliamentary access; structural judicial independence issues)	Regulated partnership (compliance-driven, lacking strategic depth)
United States	Strong tension (public voluntary PPP vs. covert bulk collection – Section 702)	Limited and fragmented (FISC secret; partial congressional oversight; civil litigation cumbersome)	Voluntary partnership (persistent trust deficit)
China	Full synergy (cybersecurity = regime security)	Absent (party-state control)	Full subordination (NIL Article 7)
Russia	Full synergy (sovereign internet = political control)	Absent (direct FSB access)	Full subordination (Yarovaya package)
Iran	Full synergy (NIN = theocratic digital sovereignty)	Absent (IRGC/MOIS dominance)	Full subordination (Protection Bill)

Democratic societies therefore have no other realistic path: they must take their own constitutional principles and traditions deadly seriously in the digital domain as well. This requires treating cybersecurity as a collectively produced public good whose precondition in a rule-of-law state is an accountable and fundamental-rights-compliant institutional system. The erosion of this system means that democracies will gradually but surely lose the very legitimacy advantage that has hitherto distinguished them from authoritarian models.

In cyberspace there is no neutral governance. Whoever compromises their own principles here will, in the long run, dismantle their own resilience.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

RK: Conceptualization, Investigation, Methodology, Project administration, Supervision, Writing – original draft, Writing – review & editing. BB: Conceptualization, Investigation, Methodology, Writing – review & editing. MM: Conceptualization, Investigation, Methodology, Writing – review & editing. JS: Conceptualization, Investigation, Methodology, Writing – review & editing. JC: Conceptualization, Investigation, Methodology, Writing – review & editing. HS: Conceptualization, Investigation, Methodology, Writing – review & editing.

Funding

The author(s) declared that financial support was received for this work and/or its publication. The Article Processing Charge (APC) for this publication was funded by Széchenyi István University.

Conflict of interest

The author(s) declared that this work was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declared that Generative AI was not used in the creation of this manuscript.

Any alternative text (alt text) provided alongside figures in this article has been generated by Frontiers with the support of artificial intelligence and reasonable efforts have been made to ensure accuracy, including review by the authors wherever possible. If you identify any issues, please contact us.

Publisher's note

References

Act CXXV of 1995 on the National Security Services. (1995). Hungary.

Act LXIX of 2024 on Hungary's cybersecurity. Hungary.

Act no. 366/2024 Coll. Amending act no. 69/2018 Coll. (2024). Slovak Republic.

Act no. 69/2018 Coll. On cybersecurity. (2018). Slovak Republic.

Aho, B., and Duffield, R. (2020). Beyond surveillance capitalism: privacy, regulation and big data in Europe and China. *Econ. Soc.* 49, 187–212. doi: 10.1080/03085147.2019.1690275

Arroyabe, M. F. A., Arranz, C. F. A., de Fernanz Arroyabe, I., and de Fernanz Arroyabe, J. C. (2024). Navigating cybersecurity: environment's impact on standards adoption and board involvement. *J. Comput. Inf. Syst.* doi: 10.1080/08874417.2024.2394440

Atkins, S., and Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *J. Cybersecur.* 7:tyab024. doi: 10.1093/cybsec/tyab024

Barrinha, A., and Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *Int. Aff.* 96, 749–766. doi: 10.1093/ia/iiz274

Bird and Bird (2025) China data protection and cybersecurity: Annual review of 2024 and outlook for 2025 (II). Available online at: https://www.twobirds.com/en/insights/2025/china/china-data-protection-and-cybersecurity-annual-review-of-2024-and-outlook-for-2025-%28ii%29 (Accessed: 18 November 2025).

Boeke, S. (2018). National cyber crisis management: different European approaches. *Governance* 31, 87–102. doi: 10.1111/gove.12309

Calcara, A., Csernatoni, R., Lavallée, C., and Siddi, M. (2022). State-industry relations and cybersecurity governance in Europe. *Rev. Int. Polit. Econ.* 29, 1237–1262. doi: 10.1080/09692290.2021.1913438

Cary, D. (2024). Governing cybersecurity. China: Interpret.

Cavelty, M. D., and Egloff, F. J. (2019). The politics of cybersecurity: balancing different roles of the state. *St. Antony's Int. Rev.* 15, 9–32.

Centrum för rättvisa v. Sweden, grand chamber, app. No. 35252/08 (European court of human rights, 25 June 2021).

Cheng, P. (2022). Decoding the rise of central Bank digital currency in China: designs, problems, and prospects. *J. Bank. Regul.* 24, 156–170. doi: 10.1057/s41261-022-00193-5

Chovancová, K. (2016). Institutional opportunities of the parliamentary opposition in Slovakia: useless tools or powerful weapons? *Politolog. Cas. / Czech J. Polit. Sci.* 23, 211–234. doi: 10.5817/PC2016-3-211

CISA (2015). Binding Operational Directive 15-01: Critical Vulnerability Mitigation Requirement for Federal Civilian Executive Branch Departments and Agencies. Available online at: https://www.cisa.gov/news-events/directives/binding-operational-directive-15-01 (Accessed November 13, 2025).

Conduit, D. (2023). Digital authoritarianism and the devolution of authoritarian rule: examining Syria's patriotic hackers. *Inf. Commun. Technol. Law* 32, 979–997. doi: 10.1080/13510347.2023.2187781

Constitution of the Islamic Republic of Iran. (1979). Available online at: https://www.constituteproject.org/constitution/Iran_1989 (Accessed November 13, 2025).

Creemers, R. (2022). China's emerging data protection framework. *SSRN Electron. J.* doi: 10.2139/ssrn.3964684

Creemers, R. (2023). Cybersecurity law and regulation in China: securing the smart state. *China Law Soc. Rev.* 6, 111–150. doi: 10.1163/27669217-12340020

Cybersecurity information sharing act of 2015 (CISA 2015), pub. L. No. 114–113, div. N, 129 stat. 2935.

Cybersecurity Law of the People's Republic of China (2017). Standing Committee of the National People's congress of the people's republic of China.

Dal, A., and Nisbet, E. C. (2022). Walking through firewalls: circumventing censorship of social media and online content in a networked authoritarian context. *Soc. Media Soc.* 8. doi: 10.1177/20563051221137738

Data Security Law of the People's Republic of China (2021). Standing Committee of the National People's congress of the people's republic of China.

Directive (EU) 2016/1148. (2016). 2022/2555 of the European Parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the union (NIS2 directive). *Off. J. Eur. Union L333*, 80–152.

Donohue, L. K. (2016). The future of foreign intelligence: Privacy and surveillance in the digital age. Oxford: Oxford University Press.

Earl, J., Maher, T. V., and Pan, J. (2022). The digital repression of social movements, protest, and activism: a synthetic review. *Sci. Adv.* 8:eabl8198. doi: 10.1126/sciadv.abl8198

Edgar, T. (2024) Reauthorizing section 702: Congress missed its best chance for real reform. Lawfare, 22 April. Available online at: https://www.lawfaremedia.org/article/reauthorizing-section-702-congress-missed-its-best-chance-real-reform (Accessed: 18 November 2025).

Egloff, F. J., and Smeets, M. (2023). Publicly attributing cyber attacks: a framework. *J. Strateg. Stud.* 46, 502–533. doi: 10.1080/01402390.2021.1895117

Ekimdzhiev and others v. Bulgaria, app. Nos. 70078/12 and 5 others (European court of human rights, 11 January 2022).

Epifanova, A. (2020). Deciphering Russia's "sovereign internet law": Tightening control and accelerating the splinternet. DGAP analysis no. 2. Berlin: German Council on Foreign Relations.

Ermoshina, K., Loveluck, B., and Musiani, F. (2021). A market of black boxes: the political economy of internet surveillance and censorship in Russia. *J. Inf. Technol. Polit.* 19, 18–33. doi: 10.1080/19331681.2021.1905972

European Court of Human Rights (2016) Case of Szabó and Vissy v. Hungary (application no. 37138/14)

European Court of Human Rights 2021 Case of big brother watch and others v. the United Kingdom (applications nos. 58170/13, 62322/14 and 24960/15)

European Union Agency for Cybersecurity (ENISA) (2023). Governance framework for National Cybersecurity Strategies. Heraklion: ENISA.

Federal Law No. 242-FZ of 21. (2015). On amendments to certain legislative acts of the Russian Federation regarding clarification of personal data processing procedures in information and telecommunication networks (Data Localization Law).

Federal law no. 32-FZ (2022). On amendments to the criminal code of the Russian Federation.

Federal law no. 374-FZ (2016). On amendments to the Federal law on counteracting terrorism and certain legislative acts of the Russian Federation (Yarovaya law).

Federal Law No. 90-FZ of 1 (2019). On amendments to the Federal law 'on communications' and the Federal law 'on information. *Information Technologies and Protection of Information' (Sovereign Internet Law).*

Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford: Oxford University Press.

Foreign Intelligence Surveillance Act of 1978. (1978). pub. L. No. 95–511, 92 stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885c), especially section 702.

FRA (European Union Agency for Fundamental Rights) (2022). Fundamental rights and digital security in the EU

Freedom House (2024). Nations in transit 2024: A region reordered by autocracy and democracy. Washington, D.C.: Freedom House.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., et al. (2023). Contested spatialities of digital sovereignty. *Geopolitics* 28, 919–958. doi: 10.1080/14650045.2022.2050070

Goitein, E. (2023). The fourth amendment in the digital age. New York: Brennan Center for Justice.

Government of the Slovak Republic (2021) National Cybersecurity Strategy of the Slovak Republic 2021–2025

Government Office SR (2024) Prechodné ustanovenia k zákonu 366/2024 Z. z

Government resolution 1089/2025 (III. 31.) on Hungary's cybersecurity strategy. Hungary.

Grand Chamber. (2021). Big brother watch and others v. the United Kingdom, grand chamber, app. Nos. 58170/13, 62322/14 and 24960/15 (European court of human rights, 25 may 2021).

Guo, S., and Li, X. (2024). Cross-border data flow in China: shifting from restriction to relaxation? *Comput. Law Secur. Rev.* 56:106079. doi: 10.1016/j.clsr.2024.106079

Hron, I., and Illýová, Z. M. (2025). ECtHR: KULÁK v. SLOVAKIA (application no. 57748/21, 3 April 2025): exposing structural flaws in the Slovak code of criminal procedure on legal professional privilege. *Bratisl. Law Rev.* 9, 255–268. doi: 10.46282/blr.2025.9.1.1020

Huang, K., Madnick, S., Zhang, F., and Siegel, M. (2021). Varieties of public–private co-governance on cybersecurity within the digital trade: implications from Huawei's 5G. *J. Chin. Gov.* 7, 81–110. doi: 10.1080/23812346.2021.1923230

Hung, H. T. (2025). Exploring China's cyber sovereignty concept and artificial intelligence governance model: a machine learning approach. *J. Comput. Soc. Sci.* 8:24. doi: 10.1007/s42001-024-00346-8

Jaber, A. (2025). Cybersecurity governance and political structures: comparing centralized and decentralized approaches to cyber defense. *Comp. Strateg.* 44, 752–771. doi: 10.1080/01495933.2025.2507310

Jardine, E., Porter, N., and Shandler, R. (2024). Cyberattacks and public opinion: the effect of uncertainty in guiding preferences. *J. Peace Res.* 61:178. doi: 10.1177/00223433231218178

Jones, B. (2025). Trust in crisis: rebuilding public confidence in national security institutions. Washington, DC: Center for Strategic and International Studies.

Karim, R., Bonhi, T. C., and Afroze, R. (2019). Governance of cyberspace: personal liberty vs. national security. *Int. J. Sci. Technol. Res.* 8, 2636–2641.

Kaye, D. (2022). Online propaganda, censorship and human rights in Russia's war against reality. *Am. J. Int. Law Unbound* 116, 140–144. doi: 10.1017/aju.2022.22

Kelemen, R., Bucko, B., and Mazuch, M. (2024a). Modernizing Hungary's cybersecurity framework: addressing evolving threats and enhancing national resilience. *Rechtskultur.*

Kelemen, R., Farkas, Á., Bučko, B., and Jordan, Z. (2024b). Public trust in national security institutions as a key to sustainable security. *Connections Q. J.* 23, 49–62. doi: 10.11610/Connections.23.4.03

Keremoğlu, E., and Weidmann, N. B. (2020). How dictators control the internet: a review essay. *Comp. Polit. Stud.* 53, 1690–1703. doi: 10.1177/0010414020912278

Kianpour, M., Davis, P. A. E., and Windekilde, I. M. (2025). Digital sovereignty in practice: analyzing the EU'S NIS2 directive. *Int. J. Inf. Secur.* 24:167. doi: 10.1007/s10207-025-01090-4

Knutelská, V. (2011). Working practices winning out over formal rules: parliamentary scrutiny of EU matters in the Czech Republic, Poland and Slovakia. *Perspect. Eur. Polit. Soc.* 12, 379–397. doi: 10.1080/15705854.2011.619527

Kovanič, M., and Coufalova, A. (2020). The legitimacy of intelligence surveillance: the fight against terrorism in the Czech Republic and Slovakia. *Intell. Natl. Secur.* 35, 115–130. doi: 10.1080/02684527.2019.1634389

Liebetrau, T. (2022). Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization. *Policy Des. Pract.* 6, 131–145. doi: 10.1080/25741292.2022.2127551

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media Commun.* 9, 5–15. doi: 10.17645/mac.v9i4.4292

Lukáč, J., Kudlová, Z., Kopčáková, J., and Gallo, P. (2025). Impact of socio-economic factors on digital literacy and security. *TEM J.* 14, 123–134. doi: 10.18421/TEM141-15

Malvenishvili, M. (2023). "Analyzing cybersecurity strategies in democratic and authoritarian regimes: a comparative study of the United States and China" in Cyber security policies and strategies of the world's leading states. ed. A. A. Khan (Hershey, PA: IGI Global), 234–255.

Manjikian, M. (2023). Cybersecurity ethics: A normative approach. London: Routledge.

McIntosh, T., Liu, T., Susnjak, T., Alavizadeh, H., Ng, A., and Watters, P. (2023). Harnessing GPT-4 for generation of cybersecurity GRC policies: a focus on ransomware attack mitigation. *Comput. Secur.* 134:103424. doi: 10.1016/j.cose.2023.103424

Ministry of Defence SR (2024). Cyber Defence Framework

MIRRI SR (Ministry of Investment, Regional Development and Informatization) (2024). Dôvodová správa k NIS2 transpozícii

Mishra, A., Alzoubi, Y. I., Anwar, M. J., and Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: an evidence from seven nations. *Comput. Secur.* 120:102820. doi: 10.1016/j.cose.2022.102820

Moyakine, E., and Tabachnik, A. (2021). Struggling to strike the right balance between interests at stake: the 'Yarovaya', 'fake news' and 'disrespect' laws as examples of ill-conceived legislation in the age of modern technology. *Comput. Law Secur. Rev.* 40:105512. doi: 10.1016/j.clsr.2020.105512

National Council of the Slovak Republic (2023) Mandate and activities of the defence and security committee

National Intelligence Law of the People's Republic of China (2017) Standing Committee of the National People's congress of the people's republic of China

NATO (2021). Climate change and security action plan. Brussels: NATO.

NATO (2022). Strategic concept. Brussels: NATO.

NBÚ SR (National Security Authority) (2023) Správa o stave kybernetickej bezpečnosti SR

NBÚ SR (National Security Authority) (2024). Prehľad zmien v zákone o kybernetickej bezpečnosti

NIST (2020). Cybersecurity framework version 1.1. Gaithersburg, MD: National Institute of Standards and Technology.

NIST (2024). Cybersecurity framework 2.0. Gaithersburg, MD: National Institute of Standards and Technology.

Park, S., and Kwon, H. (2024) "Governance of cyber threat information sharing for public-private partnerships: comparative analysis of National Cases." In *2024 IEEE/ACIS*

24th international conference on computer and information science (ICIS 2024) – Proceedings, pp. 41–48.

Perriello, L. E. (2024). Digital surveillance under European scrutiny. A dangerous alliance unveiled. *Ital. Law J.* 10, 237–259. doi: 10.23815/2421-2156.ITALJ

Personal Information Protection Law of the People's Republic of China (2021). Standing Committee of the National People's congress of the people's republic of China.

Pijpers, P.B.M.J., Boddens Hosang, J.F.R., and Ducheine, P.A.L. (2021) Collective cyber defence – The EU and NATO perspective on cyber attacks. Amsterdam law school research paper no. 2021–37, Amsterdam Center for International law no. 2021–13. Available online at: https://ssrn.com/abstract=3962163 (Accessed: 18 November 2025).

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., et al. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cogn. Tech. Work* 24, 371–390. doi: 10.1007/s10111-021-00683-y

Protection Bill. (2022). Regulatory System for Cyberspace Services Bill (Protection Bill). Tehran: Islamic Consultative Assembly. Available online at: https://rc.majlis.ir/fa/legal_draft/show/1600586 (Accessed November 13, 2025).

Ramich, M. S., and Piskunov, D. A. (2022). The securitization of cyberspace: from rulemaking to establishing legal regimes. *Vestn. RUDN. Mezhdunar. Otnosheniya* 22, 238–255. doi: 10.22363/2313-0660-2022-22-2-238-255

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., and Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors* 23:7273. doi: 10.3390/s23167273

Santaniello, M., and Barbieri, M. (2024). Monocratic cybersecurity in the EU member states: insights from Italy, France, Germany and Spain. *Eur. Politics Soc.* 26, 1–25. doi: 10.1080/23745118.2024.2349893

Schumann, M. P. (2025). Legalizing control: the rise of restrictive internet regulation in sub-Saharan Africa. *Democratization*, 1–26. doi: 10.1080/13510347.2025.2503370

Serscikov, G. (2025). NOCs and illegals in the current surveillance landscape: can mimicry help overcome evolving challenges? *Intell. Natl. Secur.* 40, 507–532. doi: 10.1080/02684527.2025.2485806

Shah, M. U., Iqbal, F., Rehman, U., and Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: implications for cyber governance. *IEEE Access* 11, 87970–87987. doi: 10.1109/ACCESS.2023.3296580

Sivetc, L. (2021). Controlling free expression "by infrastructure" in the Russian internet: the consequences of RuNet sovereignization. *First Monday* 26:698. doi: 10.5210/fm.v26i5.11698

NIS2 Smernica (2024) Čo je SK-CERT, CSIRT či ENISA a prečo sú dôležité pre našu kyberbezpečnosť?

Soesanto, S., and Smeets, M. (2021). "Cyber deterrence: the past, present, and future" in NL ARMS Netherlands annual review of military studies 2020: Deterrence in the 21st century—Insights from theory and practice. eds. F. Osinga and T. Sweijs (The Hague: T.M.C. Asser Press), 409–429.

Sokol, P., and Rózenfeldová, L. B. (2025). Content blocking mechanism in cybersecurity: Slovakia case study. *EURASIP J. Inf. Secur.* 2025:4. doi: 10.1186/s13635-025-00190-x

Supreme Council of Cyberspace (2012). Founding Decree of the Supreme Council of Cyberspace. Tehran: Office of the Supreme Leader. Available online at: https://www.leader.ir/fa/content/9213/ (Accessed November 13, 2025).

Supreme Council of Cyberspace (2017). Tabyin-e al-Zāmāt-e Shabake-ye Mellī-ye Eṭṭelā'āt (Clarification of the Requirements of the National Information Network). Tehran: Supreme Council of Cyberspace. Available online at: https://www.ekhtebar.ir/س-نان-ع-اب-ی-زاچم-یاضف-یلاع-ی-اروش-هبوصم/ (Accessed November 13, 2025).

Szabó, V., and Vissy, V. (2016). App. No. 37138/14 (European court of human rights, 12 January 2016). Hungary.

Taylor, R. D. (2020). Data localization: the internet in the balance. *Telecommun. Policy* 44:102003. doi: 10.1016/j.telpol.2020.102003

The White House (2023). National Cybersecurity Strategy. Washington, DC.

Trevaskes, S. (2024). Integrating stability maintenance into comprehensive governance: the burgeoning "safe China" behemoth. *Modern China* 50, 3–34. doi: 10.1177/00977004231205889

Ullah, M. W., Alam, M. T., Sultana, T., Rahman, M. M., Faraji, M. R., and Ahmed, M. F. (2024). A systematic review on information security policies in the USA banking system and global banking: risks, rewards, and future trends. *Edelweiss Applied Sci. Technol.* 8, 8437–8453. doi: 10.55214/25768484.v8i6.3816

United Nations (2021). Our common agenda – policy brief 2: strengthening the international response to complex global shocks. New York: United Nations.

USA PATRIOT act of 2001. (2001). pub. L. No. 107–56, 115 stat. 272 (uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism act of 2001).

Vaško, A. (2022). The legal regulation of special means by the intelligence Agency of the Slovak Republic within the case law of the European court of human rights. *Access to Justice in Eastern Europe* 5, 123–140. doi: 10.33327/AJEE-2022.5.3.123

Veigurs, M., Lasmanis, T., and Romanovs, A. (2024). "IT governance in critical sectors: towards the NIS2 implementation." In *2024 IEEE 65th international scientific conference on information technology and management science of Riga Technical University (ITMS)*, pp. 1–6.

Wang, C. (2016). Four principles on internet governance reflecting a global norm based on international law. *J. Nanjing University of Posts and Telecommunications (Social Science Edition)* 16, 1–6. doi: 10.14132/j.cnki.1673-5439.2016.01.002

Wang, Y., and Han, R. (2025). Authoritarian elasticity: how autocracies may effectively mobilize for crisis management. *Governance* 38, 1–20. doi: 10.1111/gove.70074

Wang, F., Wang, H., and Li, J. (2024). The effect of cybersecurity legislation on firm cost behavior: evidence from China. *Pac. Basin Financ. J.* 86:102460. doi: 10.1016/j.pacfin.2024.102460

Wei, X. (2022). A critical evaluation of China's legal responses to cyberterrorism. *Comput. Law Secur. Rev.* 47:105768. doi: 10.1016/j.clsr.2022.105768

Weiss, M., and Krieger, N. (2025). The political economy of cybersecurity: governments, firms and opportunity structures for business power. *Contemp. Secur. Policy* 46, 403–428. doi: 10.1080/13523260.2025.2474867

West, H. (2023). Parliamentary committees and ex-post oversight: institutional options and design. *Parliam. Aff.* 76, 345–362. doi: 10.1093/pa/gsac012

Whyte, C. (2020). Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare. *J. Cybersecur.* 6:tyaa013. doi: 10.1093/cybsec/tyaa013

Yalcintas, A., and Alizadeh, N. (2020). Digital protectionism and national planning in the age of the internet: the case of Iran. *J. Inst. Econ.* 16, 519–536. doi: 10.1017/S1744137420000077

Zalnieriute, M. (2022). Big brother watch and others v. the United Kingdom. *Am. J. Int. Law* 116, 585–592. doi: 10.1017/ajil.2022.35