JOURNAL OF COMPARATIVE POLITICS ◎ vol. 18 ◎ no. 2 ◎ 2025

CYBERSECURITY BETWEEN TECHNOLOGICAL DETERMINISM, POLITICAL GOVERNANCE, AND NATIONAL SECURITY CHALLENGES

Uroš SVETE[1]

The article advances the central thesis that the organization of cybersecurity within a given country is not solely determined by the technical aspects of information and communication technology. Instead, it is profoundly shaped by the relationships among civilian cybersecurity institutions, the intelligence community, military capabilities, and law enforcement agencies, as well as by the country's political (security) culture, its integration into international organizations, and its perception of threats to national security. The study applies the theories of technological determinism and constructivism while employing a comparative methodology. Furthermore, it explores why significant functional and institutional differences exist among countries that are otherwise very similar in political and administrative structures, despite efforts to harmonize approaches through EU cyber legislation, international technical and political standards, and attempts to establish international law in cyberspace.

Key words: cybersecurity; information-communication technology; national security; technological determinism; institutional overlapping.

1 INTRODUCTION – A BRIEF OVERVIEW OF FUNDAMENTAL CYBERSECURITY CHALLENGES

Since its inception in the mid-1970s, modern digital information technology has oscillated between private, individual initiatives, commercial interests, and state involvement, with governments attempting to influence its development through various mechanisms (Abbate 1999). As the number of users, networked devices, and the capacity for data transfer, processing, and storage increased—following Moore's Law (Moore 1965)—the emerging cyberspace built on this technology

[1] **Uroš SVETE**, PhD, Assistant Professor at the Faculty of Social Sciences, University of Ljubljana; director of the Government Information Security Office (GISO/URSIV), national cyber security competent authority of the Republic of Slovenia. Contact: uros.svete@fdv.uni-lj.si.

grew in social power. Its global and international presence also turned it into a new tool in the geostrategic competition between global powers (Nye 2011). While it was crucial to ensure suitable interoperable technical means, such as the TCP/IP protocol (Abbate 1999), the implementation process revealed significant disparities among nations.

The same is the origin of cybersecurity that can be traced back to the 1960s when the development of ARPANET, a precursor to the internet, raised initial concerns about protecting sensitive information. Early efforts focused on physical security and access control to prevent unauthorized use of centralized computing systems (Abbate 1999, 35). In the 1970s, the introduction of the Data Encryption Standard (DES) by the U.S. National Bureau of Standards provided a significant step forward in securing digital communications (Levy 2001, 85).

Cybersecurity became more prominent in the 1980s with the advent of personal computers and networked systems. The 1988 Morris Worm incident—the first major cyberattack—exposed vulnerabilities in internet-connected systems and led to the creation of the first Computer Emergency Response Team (CERT) at Carnegie Mellon University (Spafford 1989, 678). This marked the formal beginning of institutionalized cybersecurity responses.

In the 1990s and early 2000s, as internet usage surged, the threat landscape expanded. Tools like firewalls and intrusion detection systems were introduced to protect networks, while the development of public-key infrastructure provided a framework for secure online communication (Nye 2011, 113). Notably, the 2007 cyberattacks on Estonia—considered one of the first state-sponsored cyber warfare campaigns—highlighted the geopolitical implications of cybersecurity and spurred comprehensive international and national efforts, like strategic, legal, and organizational, to address cyber threats (Czosseck, Ottis and Talihärm 2011).

Today, cybersecurity has evolved into a multifaceted discipline addressing threats ranging from cybercrime to state-sponsored attacks, utilizing tools such as artificial intelligence and blockchain to enhance security measures. Despite advancements, the rapidly changing technological landscape and increasingly sophisticated adversaries continue to pose challenges. While the landscape of cyber threats continues to evolve, their sophistication is not primarily driven by the emergence of new attack types. Instead, it lies in the innovative use of Tactics, Techniques, and Procedures (TTPs) employed by threat actors. These adaptive strategies allow cybercriminals and nation-state actors to bypass defences, exploit vulnerabilities, and achieve their objectives with precision. Cybersecurity experts have noted that many attack types, such as phishing, malware, and ransomware, remain fundamentally unchanged in their core methodology[2]. However, the way these attacks are deployed has become increasingly complex. For example, advanced persistent threat (APT) groups often utilize phishing not merely to steal credentials but to establish long-term footholds and persistent presence in target networks. These groups also leverage multi-staged attack frameworks that integrate reconnaissance, weaponization, delivery phase, exploitation installation phase and the command and control (C2) phase, the attacker establishes a C2 channel to the target system – so called Intrusion Kill Chain (Siukonen 2019; Hutchins, Cloppert and Amin 2020; SentinelOne 2024).

[2] What I published in the same journal twelve years ago (Svete 2012). In this very long era for technology, it has become evident that, from a technical standpoint, attacks have not changed significantly. However, practically everything else has, from complexity and dependence on a functioning cyberspace to, ultimately, geostrategic circumstances.

Moreover, attackers are increasingly exploiting legitimate tools and processes, a tactic known as "living off the land" (LOTL).

This method, which uses native tools such as PowerShell or Windows Management Instrumentation (WMI), enables attackers to blend into normal network traffic and avoid traditional detection methods (Mitre ATT&CK 2023). The MITRE ATT&CK framework highlights the role of TTPs in modern cyberattacks. For instance, attackers are now using techniques like fileless malware, which executes directly in memory and avoids writing files to disk, rendering traditional antivirus solutions ineffective (Mitre ATT&CK 2023). Furthermore, the deployment of modular malware, which can adapt its behaviour depending on the target environment, showcases how TTPs enhance the effectiveness of even well-known attack types). Recent high-profile incidents demonstrate the importance of TTPs in cyber threat sophistication. The SolarWinds attack (CSIS 2021) involved a supply chain compromise that injected malicious code into legitimate software updates, exploiting trust relationships to infiltrate high-value targets. The attackers' meticulous operational security and strategic use of TTPs ensured a prolonged presence in networks before discovery (ibid.). Similarly, the Colonial Pipeline ransomware attack showcased the use of double extortion, combining data encryption with the threat of data leaks to maximize impact and compel victims to pay ransoms. This hybrid TTP significantly increased the pressure on the affected organization to comply (Europol 2022). The sophistication of modern cyber threats does not lie in the invention of new attack vectors but in the innovative application of TTPs. This evolution underscores the need for organizations to focus on understanding and mitigating these techniques rather than solely relying on traditional defence mechanisms. By adopting frameworks like MITRE ATT&CK and enhancing threat intelligence capabilities, cybersecurity practitioners can better anticipate and counteract these advanced strategies. The main elements of cybersecurity, often referred to as the CIA Triad, therefore include confidentiality (ensuring that sensitive information is accessed only by authorized individuals, systems, or processes). Useful measures are encryption, access controls, and authentication mechanisms, integrity (ensuring that data remains accurate, consistent, and trustworthy throughout its lifecycle). This includes protection against unauthorized modifications and ensuring data authenticity and availability (ensuring that information and systems are accessible to authorized users when needed, particularly in the face of threats such as distributed denial-of-service (DDoS) attacks (Whitman and Mattord 2022))[3].

For that reason, cybersecurity has become a cornerstone of national security in the 21st century. While ICT advancements provide the technical backbone for cybersecurity frameworks, these alone do not account for the disparities in organizational approaches among states. For example, Estonia’s response to the

[3] A very good example are E-elections. The article by Kuba and Stejskal (2024) explores the potential of electronic voting (e-voting) to increase voter turnout and reduce participation inequalities in the Czech Republic. Using survey data, the study predicts that e-voting could boost turnout by 8.5 percentage points, particularly benefiting younger voters, irregular voters, and those facing logistical barriers to traditional voting. However, the adoption of e-voting varies across demographic groups, with wealthier, more educated individuals being more likely to use it. E-voting highlights how indispensable information and communication technology (ICT) has become in modern societies, streamlining democratic processes and making them more accessible. Yet, it also introduces risks to democratic integrity. In November 2024, Romania's presidential election faced significant cybersecurity challenges, leading to the annulment of the first-round results. The Constitutional Court's decision was based on evidence of cyberattacks and foreign interference, notably linked to Russian entities. These cyber activities included over 85,000 attacks targeting election systems, aiming to disrupt the electoral process and influence outcomes (Ilascu 2024).

2007 cyberattacks showcases how cohesive and centralized civilian-led efforts can bolster national resilience (Ottis 2008), whereas the United States struggles with inter-agency silos despite advanced technological capabilities (Healey 2013). Similarly, Israel's integration of military intelligence, such as Unit 8200, reflects the influence of its securitized political culture (Herman 2021). In Slovenia cybersecurity was first recognized in the context of national security in the Resolution on the National Security Strategy in 2001 and more specifically in the Resolution on the National Security Strategy of the Republic of Slovenia (ReSNV-1) in 2010: "The Republic of Slovenia will develop a national strategy to respond to cyber threats and the misuse of information technologies and adopt necessary measures to ensure effective cyber defence, involving both the public and private sectors to the greatest extent possible. One of the priority tasks in ensuring cybersecurity will also be the establishment of a national coordination body for cybersecurity." Unfortunately, it took six years to adopt the Cybersecurity Strategy (2016) and another four years to establish the responsible authority (formally, the Information Security Administration of the Republic of Slovenia assumed all tasks on January 1, 2020).

This article posits that effective cybersecurity relies equally on the structural and cultural dynamics of a country's institutions, as well as its geopolitical positioning. By integrating perspectives from technological determinism and constructivism, this research highlights the socio-technical co-evolution of cybersecurity systems and provides a comparative analysis of various national models.

2 ICT AND ITS SECURITY (R)EVOLUTION

ICT has undergone transformative changes, from the mainframe computing era of the 1960s to the decentralized (local) networks and cloud computing paradigms of today. These developments have altered the landscape of vulnerabilities and capabilities. Technological determinism suggests that the trajectory of ICT dictates societal and organizational structures (Smith and Marx 1994). However, this view must be tempered with constructivist insights, which emphasize the human agency and cultural factors shaping technology adoption (Bijker, Hughes and Pinch 1987). For instance, the early adoption of cybersecurity measures in the United States contrasted with the delayed but centralized approaches in many European nations, reflecting differing cultural attitudes toward privacy and state intervention. Allan Dafoe examines the theory of technological determinism as well, which posits that technology drives societal and cultural change in a unidirectional and inevitable manner. Dafoe critiques oversimplified interpretations of this theory, offering a typology to distinguish between strong and weak forms of determinism. He emphasizes the interplay between technological innovations and socio-political factors, arguing that the effects of technology are mediated by contextual variables. This nuanced framework moves beyond binary debates, focusing on the conditions under which technological impacts occur (Dafoe 2015, 1047).

As noted by Dunn Cavelty and Wenger (2020), the rapid digitalization of economies and societies has significantly expanded the scope and strategic relevance of cybersecurity, embedding technological development deeply within broader political and security frameworks. They emphasize that cyber incidents increasingly shape both national and international security dynamics, illustrating the intricate interplay between evolving technological capabilities and governance challenges. The integration of cybersecurity into national security strategies reflects its growing importance in modern conflicts.

Cyberattacks, such as the 2020 SolarWinds breach and the 2021 Colonial Pipeline ransomware attack, have demonstrated the vulnerability of critical infrastructure and the potential for widespread economic and social disruption. Governments are increasingly investing in offensive and defensive cyber capabilities as well. Military doctrines now incorporate cyber operations as a core component of national defence. However, this militarization of cyberspace poses challenges for international stability. The lack of clear norms and agreements on cyber warfare risks escalating conflicts and undermining trust among nations.

Dafoe (2015) extends this discussion by proposing a typology of technological determinism, emphasizing the interplay between military-economic competition and sociotechnical evolution. He argues that while technologies often evolve within social contexts, competitive pressures can create deterministic trajectories, especially in domains such as cybersecurity, where national security imperatives dominate decision-making.

3 INSTITUTIONAL INTERSECTIONS IN CYBERSECURITY

The interplay between civilian cybersecurity institutions, intelligence communities, military capabilities, and law enforcement agencies shapes a nation's cybersecurity posture. These interactions are deeply embedded in political governance structures and historical experiences of the state. The complexity in delineating the roles and responsibilities among civilian cybersecurity institutions, intelligence communities, military capabilities, and law enforcement agencies arises from overlapping mandates, evolving cyber threats, and the necessity for inter-agency collaboration.

The division of responsibilities among civilian cybersecurity institutions, intelligence communities, military capabilities, and law enforcement agencies is critical for effective national cybersecurity governance, to delineate their roles and avoid overlaps. Firstly, clearly defined laws and regulations (legislative framework) should outline the scope of authority and responsibilities for each entity. Civilian agencies should focus on protecting critical infrastructure, issuing guidelines, and managing public-private partnerships. Intelligence agencies should be tasked with cyber threat intelligence and counterintelligence activities. Military units should handle offensive and defensive operations in cyberspace during armed conflicts. Law enforcement should investigate, prosecute, and prevent cybercrimes[4].

Secondly, coordination mechanisms in the form of inter-agency coordination bodies can help bridge gaps and prevent overlaps. A National (Cyber)security Council can oversee and harmonize activities across sectors. Regular inter-agency meetings and joint task forces can foster collaboration. As an example, we emphasize the German Cyberabwehrzentrum (Cyber Defence Centre) which is a cybersecurity coordination and response entity in Germany, established to strengthen the country's cyber defence capabilities. It serves as a central hub for cooperation among government agencies, military, intelligence services, and law enforcement in addressing cyber threats. The Cyberabwehrzentrum brings together various federal agencies to ensure coordinated responses to cyber

[4] In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for civilian infrastructure protection, while the National Security Agency (NSA) oversees cyber intelligence, and the Department of Defence (DoD) conducts military operations in cyberspace (CISA 2023).

incidents. This includes collaboration among the Federal Office for Information Security (BSI), responsible for civilian cybersecurity and critical infrastructure protection, the Federal Criminal Police Office (BKA), focused on cybercrime investigations, the Federal Intelligence Service (BND), which provides intelligence on foreign cyber threats and the Federal Office for the Protection of the Constitution (BfV), which monitors domestic cyber threats and espionage. The centre manages real-time responses to significant cyberattacks, ensuring information sharing and cooperation between the agencies involved. Collaboration with the Military: The Cyber and Information Space Command (Kommando Cyber- und Informationsraum, CIR) of the German Armed Forces (Bundeswehr) plays a critical role in defending against cyberattacks targeting military systems, often in collaboration with the Cyberabwehrzentrum (Federal Office for Information Security (BSI, 2024). The solution employed by the Republic of Slovenia is very comparable. According to Slovenia's Information Security Act (ZInfV), cyber defence is primarily implemented by state authorities, with distinct roles being assigned to various institutions. These include government bodies, security services, and specialized agencies tasked with protecting national information infrastructure and responding to cyber threats. The Government Information Security Office (URSIV) serves as the central authority responsible for coordinating cybersecurity policies and implementing the provisions of the national information security bill ZInfV. It oversees national strategies for information security and cooperates with other state institutions. The Ministry of Defence (MORS) is responsible for the military aspects of cyber defence, including protecting defence-related systems. SI-CERT (Slovenian Computer Emergency Response Team) acts as the national response centre for cybersecurity incidents. It provides technical assistance and guidance during cyberattacks and manages incident reporting from critical infrastructure operators and digital service providers. The Ministry of the Interior (MNZ), which includes the police, focuses on cybercrime investigations through law enforcement. Finally, the Intelligence and Security Agency (SOVA) addresses cyber espionage and other threats to national security. The ZInfV establishes a framework for inter-agency collaboration, particularly during significant cyber incidents, ensuring that state authorities act in a unified and efficient manner (Republic of Slovenia Information Security Act (Zakon o informacijski varnosti 2018).

Thirdly, distinct operational domains prevent conflict and confusion. Civilian agencies handle cybersecurity awareness, education, and infrastructure monitoring. Historically, the first CERTs (Computer Emergency Response Teams) were integral parts of the information infrastructure used by end-users, who relied on them to handle incidents. Over time, these teams transformed into more generic support services, offering broad methodological assistance during cyber incidents. However, in recent years, some countries are revisiting their roots, as increasingly more cybersecurity agencies and CERTs are deploying sensors within the infrastructure for which they are responsible. This approach enables them to detect even the most advanced cyberattacks more efficiently and quickly, particularly those designed to evade traditional cyber defence tools. Examples of such practices include the Security and Intelligence Agency (SOA) of Croatia, which has significantly enhanced its cyber defence capabilities through the establishment of the Cyber Security Centre and the implementation of the SK@UT system. In 2019, the SOA inaugurated the Cyber Security Centre to safeguard Croatia's national cyberspace from state-sponsored cyberattacks and advanced persistent threats (APTs). This centre serves as a hub for monitoring, detecting, and responding to cyber threats targeting critical infrastructure and government institutions. Its main application is the SK@UT System, a distributed network of sensors deployed across more than 60 key government and critical

infrastructure entities. It functions by continuously monitoring network traffic to detect anomalies and potential cyber threats in real-time. Notably, SK@UT is recognized among the top three of such programs within the European Union, reflecting its advanced capabilities in cyber threat detection and prevention. On February 15, 2024, Croatia enacted the Cyber Security Act, in compliance with the European Union's NIS2 Directive. This legislation designates SOA as the central state body for cybersecurity, expanding its mandate to include comprehensive oversight and coordination of national cyber defence efforts. Consequently, the existing Cyber Security Centre is being transformed into the National Cyber Security Centre (NCSC-HR) to better address evolving cyber threats. The SOA actively collaborates with international partners to bolster its cyber defence capabilities. For instance, in 2022, the U.S. Cyber Command deployed "hunt forward" teams to Croatia, working alongside the SOA's Cyber Security Centre to enhance the security of Croatian cyber infrastructure amid heightened concerns over cyberattacks linked to regional conflicts (SOA 2024; Janofsky 2022; ZSIS 2024).

The next example is a system called Einstein, operated by the Cybersecurity and Infrastructure Security Agency (CISA). It is an intrusion detection and prevention system deployed across federal civilian networks. Einstein monitors network traffic for malicious activity and provides real-time threat detection. While primarily focused on federal networks, the CISA also collaborates with state, local, tribal, and territorial governments, as well as private sector partners, to enhance cybersecurity monitoring and information sharing (Cybersecurity and Infrastructure Security Agency (CISA) 2024).

The third case is the Danish SektorCERT as a private one. SektorCERT is Denmark's cybersecurity centre dedicated to critical infrastructure sectors. It plays a pivotal role in defending these sectors against cyber threats by detecting and managing cyberattacks targeting critical infrastructure. SektorCERT also facilitates the accumulation and dissemination of essential knowledge to prevent future attacks. Established by Green Power Denmark, Dansk Fjernvarme, and Energinet, SektorCERT has been operational since 2019. As of January 1, 2023, the DANVA (Danish Water and Wastewater Association) joined as an equal partner, expanding SektorCERT's reach to include the water sector. Among its services, SektorCERT offers network monitoring, OT (Operational Technology) security training, and incident handling during cyberattacks. It monitors companies within its sectors through an extensive sensor network, enabling the early detection and mitigation of cyber threats (Cybersecurity Intelligence 2024)

Intelligence agencies focus on covert cyber operations and international threat intelligence. Covert cyber operations are clandestine activities conducted in cyberspace to achieve strategic objectives without revealing the identity or intent of the actor behind them. These operations typically aim to gather intelligence, disrupt adversarial systems, or manipulate information while maintaining plausible deniability. Covert operations often use tools like proxy servers, anonymizing networks, and compromised systems to obscure the origin of the attack (Rid 2013, 25). These operations may target critical infrastructure, extract sensitive data, or disrupt adversarial capabilities. Examples include the deployment of malware, Distributed Denial of Service (DDoS) attacks, or disinformation campaigns (Singer and Friedman 2014, 78). Covert cyber operations occupy a grey area in international law. They often blur the line between espionage and acts of war, complicating attribution and response (Lin 2016, 102). Covert cyber operations are a cornerstone of modern geopolitical strategy, offering states a way to achieve objectives without direct confrontation.

However, their covert nature makes them difficult to attribute and respond to, raising challenges for international security and legal frameworks.

Military units conduct offensive cyber operations (OCO's) under strict governmental oversight. OCOs are state-sponsored activities conducted by military or defence organizations to project power in cyberspace. Their goal is to achieve tactical, operational, or strategic advantages using disrupt, deny, degrade, or destroy adversarial capabilities and often together with conventional military campaigns. The targets are enemy military infrastructure, critical infrastructure, or strategic assets (e.g., air defence systems, command centres) (Zetter 2014, 125).

Law enforcement addresses cybercrime within a domestic legal framework. Law enforcement agencies are continually adapting to the evolving landscape of cybercrime by implementing specialized training, fostering international collaboration, and developing advanced investigative frameworks. The establishment of dedicated cybercrime units and the provision of targeted training are essential for effective cybercrime investigation. A qualitative analysis emphasizes the need for law enforcement to enhance capacity, capability, and collaboration to address the complexities of cyber offenses (Holt et al. 2023). Additionally, the integration of body-worn cameras, drones, and artificial intelligence has been proposed to advance policing strategies in the digital age (Davies and Krame 2023). The transnational nature of cybercrime necessitates robust international cooperation. The Convention on Cybercrime (Budapest Convention) remains a cornerstone in facilitating cross-border collaboration (Broadhurst 2006). Recent studies underscore the importance of harmonizing legal frameworks and joint operations to effectively combat cyber threats (Holt and Lee 2019). Law enforcement agencies are developing comprehensive frameworks that integrate technological tools with traditional investigative methods. The Cybersecurity Resilience and Law Enforcement Collaboration (CyRLEC) Framework, for instance, emphasizes collaboration with law enforcement agencies to mitigate cyber threats (Schiliro 2023). Furthermore, the integration of digital forensics into investigative processes has been crucial in addressing cybercrime (Casey 2011). Despite advancements, challenges persist, including rapid technological evolution, jurisdictional issues, and resource constraints. Law enforcement agencies continue to adapt by embracing new technologies, fostering public-private partnerships, and engaging in continuous training to stay ahead of cybercriminals (Wall 2007). The need for a harm-centric perspective in policing cyberspace has been highlighted, necessitating a shift from traditional methods to effectively address cybercrime (Lee 2019). In contrast to other cyber actors, law enforcement agencies are increasingly adopting offensive cyber operations to dismantle the digital infrastructure of cybercriminals, complemented by on-the-ground arrests and asset seizures[5].

[5] Dismantling of the 'Ghost' Cybercrime Platform. In September 2024, an international law enforcement operation led by Europol successfully dismantled the 'Ghost' cybercrime platform, which was extensively used for drug trafficking and money laundering. The operation resulted in 51 arrests across various countries, with additional apprehensions anticipated. The platform's advanced security features had made it a preferred tool among criminal organizations. This action also prevented several threats to life, led to the dismantling of a drug lab in Australia, and resulted in the seizure of weapons, drugs, and over 1 million euros in cash (Olive and Van Campenhout 2024). Operation PowerOFF is an ongoing joint initiative by the FBI, Europol, and other international law enforcement agencies targeting 'booter' or 'stresser' services that offer Distributed Denial of Service (DDoS) attacks for hire. Since its inception in 2018, the operation has led to the seizure of numerous domains associated with these services and the arrest of individuals operating them. In December 2022, the FBI announced the seizure of 48 domains linked to DDoS-for-hire platforms, significantly disrupting these illegal services

TABLE 1: DIVERSIFICATION OF CYBER SECURITY PERPETRATORS

Aspect	Military OCOs	Cyber Espionage	Cybercrime
Primary Goal	Strategic disruption or destruction	Intelligence gathering	Financial gain
Actors	State military organizations	State intelligence agencies, proxy actors	Non-state criminal groups, rogue state "supported" criminal groups
Legal Status	Governed by international law	Often a grey area	Criminalized globally
Targets	Military and strategic assets	Government and private data	Financial institutions, companies, individuals
Implications	Significant due to potential collateral cyber and/or physical damage	Often covert and difficult to attribute	Exploitative and harmful to victims

Source: based on Healy (2024) and own analysis.

From the examples provided, it becomes evident how challenging it is to distinguish between the many "state" cyber actors, as the tools, techniques, and methods they use are often strikingly similar. As a result, the differentiation can only be "artificial and biased" meaning non-technical. The table 1 illustrates that the actual differences lie primarily in the attackers, their legal status, and their targets, with partial distinctions in their (ethical) implications.

The delineation of responsibilities among cybersecurity stakeholders requires a mix of clear legislative frameworks, robust coordination mechanisms, and adaptive operational practices. These analyzed measures ensure that agencies can focus on their core missions while collaborating effectively to address the dynamic nature of cyber threats[6].

4 POLITICAL GOVERNANCE AND SECURITY CULTURE AS CYBERSECURITY DRIVERS

Political governance structures shape the prioritization and framing of cybersecurity. States with centralized governance structures, such as Russia, favour top-down approaches integrating all aspects of state power, which enables swift decision-making but may limit stakeholder input and adaptability. In contrast, decentralized democracies, like Germany, prioritize sectoral responsibilities and stakeholder engagement, fostering collaboration but sometimes leading to slower response times. The cultural perception of risk—influenced by historical experiences, such as Estonia's 2007 cyberattacks and the

(https://en.wikipedia.org/wiki/Operation_PowerOFF. In December 2024, U.S. authorities charged a Russian-Israeli dual national, Rostislav Panev, for his alleged involvement with the LockBit ransomware group. Panev, arrested in Israel in August, is awaiting extradition to the United States. As a developer for LockBit from its inception in 2019 until February 2024, Panev contributed to the group's growth, which has been identified as one of the most active and destructive ransomware operations globally. Since 2020, LockBit has been associated with attacks on more than 2,500 victims across 120 countries, targeting various sectors (Reuters 2024).

[6] As a good practice, the Counter Ransomware Initiative (CRI) could be emphasized. It is a global coalition established in 2021 by the United States to combat the escalating threat of ransomware. Its mission is to enhance collective resilience, disrupt the ransomware ecosystem, and develop comprehensive policy approaches to address ransomware threats. Key objectives of the CRI are building collective resilience, enhancing the ability of member nations to prevent and withstand ransomware attacks through shared best practices and resources, disruption of ransomware ecosystem—coordinating efforts to dismantle the infrastructure and networks utilized by ransomware operators and policy development—formulating and promoting policies that deter ransomware activities, including discouraging ransom payments and countering illicit financial activities associated with ransomware. The CRI underscores the importance of international collaboration in addressing the multifaceted challenges posed by ransomware, aiming to create a secure and resilient cyberspace for all member nations (see https://www.counter-ransomware.org/aboutus)

United States' emphasis on protecting critical infrastructure from state-sponsored threats—further determines the aggressiveness and scope of national strategies (Ottis 2008). These examples highlight how governance structures interact with security cultures to shape diverse cybersecurity approaches.

Membership in international organizations like NATO, the EU, or ASEAN significantly influences national cybersecurity policies, too. NATO's cooperative defence strategies, including the Tallinn Manual on the Law of Cyber Warfare, provide a framework for member states by offering detailed guidelines on responding to cyber operations within international law, as demonstrated by its influence on coordinated member responses to ransomware threats. Damjan Štrucl's article, "Cyber Security and Cyber Defence Comparison of Various NATO Member States," explores the diverse approaches to cybersecurity and cyber defence among NATO countries. It highlights critical variations in strategy, organization, and resource allocation, reflecting each nation's unique geopolitical circumstances and security priorities. Štrucl emphasizes that NATO countries vary significantly in their cybersecurity organizational frameworks. Some nations integrate their cyber capabilities within military structures, while others operate through civilian-led agencies, reflecting diverse national priorities. For instance, the U.S. emphasizes offensive cyber operations within its military strategy, while European nations such as Germany focus on defensive measures to protect critical infrastructure (Štrucl 2023, 52). The article underscores the disparities in cybersecurity policies, influenced by historical experiences and perceived threats. Countries like Estonia, having faced significant cyberattacks in 2007, have robust national cybersecurity strategies with an emphasis on public-private partnerships. Conversely, nations with fewer historical cyber threats, such as some Southern European countries, have less-developed cyber defence frameworks (ibid., 53). Štrucl discusses how NATO's Cyber Defence Pledge serves as a unifying framework, urging member states to enhance their cyber defence capabilities. However, the level of integration and commitment varies. Northern European countries, particularly those bordering Russia, actively participate in NATO's Cooperative Cyber Defence Centre of Excellence, while others contribute to a lesser extent (ibid., 55). Štrucl concludes that while NATO provides a collective framework for cyber defence, the varying capabilities and priorities of member states pose challenges to achieving a cohesive strategy. He recommends enhancing information sharing, standardizing cybersecurity practices, and increasing investments in capacity building across NATO members (ibid., 59).

Similarly, ASEAN's emphasis on capacity-building has led to initiatives like the ASEAN-Japan Cybersecurity Capacity Building Centre[7], which fosters regional expertise and unified approaches to tackling cyber threats. These actions illustrate how such organizations directly shape the cybersecurity strategies of member states, enhancing stability and shared technological growth. Threat perception varies across nations based on geopolitical realities. For instance, the United States' National Cybersecurity Strategy prioritizes countering state-sponsored threats from China and Russia, while smaller states like Singapore focus on cyber resilience against economic espionage and criminal syndicates (National Cybersecurity Strategy 2023).

[7] ASEAN-Japan Cybersecurity Capacity Building Centre, see https://ajccbc.ncsa.or.th.

4.1 Cybersecurity Coordination Bodies – Comparative Analysis

By comparing the cybersecurity frameworks of countries such as the United States, Estonia, Israel, and others, this article illustrates the diversity in organizational models, especially in the field of civil cyber security. The analysis highlights the interplay of specific metrics, such as the integration of public and private sectors, the degree of military involvement in cyber operations, and the prioritization of threat types (e.g., espionage vs. sabotage). For instance, the United States' emphasis on inter-agency coordination contrasts with Estonia's cohesive and centralized civilian-led approach, while Israel's innovation-driven model emphasizes rapid technological development. These examples underline the varied approaches to achieving cybersecurity resilience and national security goals.

While differences in cybersecurity frameworks between countries can be understood considering their unique governmental structures and priorities, the situation becomes far more complex when viewed within the context of the European Union (EU). The NIS Directive (Directive on Security of Network and Information Systems) is a key legislative instrument adopted by the EU to enhance cybersecurity across member states. It requires each member state to designate a single point of contact (SPOC) responsible for coordinating EU-wide communication on cybersecurity incidents, at least one competent national authority for cybersecurity, and a national Computer Security Incident Response Team (CSIRT) tasked with managing and mitigating cyber incidents. This directive aims to create a minimum standard for cybersecurity capabilities and coordination across the EU. However, the way member states have implemented these requirements reveals significant institutional and functional heterogeneity.

As illustrated in the table 2, EU member states have applied the NIS Directive's requirements in widely varying ways. Institutional Variations: Some countries have centralized their cybersecurity responsibilities under a single coordinating body, while others have distributed responsibilities across multiple agencies. Functional Variations: Confirm cybersecurity agencies in the EU perform a diverse range of functions following coordination tasks (acting as liaison bodies between national stakeholders and EU entities (e.g., SPOCs)), policy development (drafting and enforcing national cybersecurity strategies and legislation), fusion cells (integrating intelligence, defence, and civilian capabilities to respond to cyber threats) or cyber defence capacities (playing an active role in national defence against cyber threats). In some countries, cybersecurity agencies are part of national security and counterterrorism efforts, placing cyber threats within the broader context of homeland security. In others, the development of civilian cybersecurity capabilities has been rooted in intelligence services, reflecting the perceived criticality of cyber threats to national security.

This divergence is driven in part by the perception of cyber threats as existential risks to national security across almost all member states. Since the EU's legislative tools—whether directives or regulations—cannot directly dictate national security measures and organizational/institutional models, each country has significant autonomy in defining its cybersecurity strategy. The NIS Directive, while fostering minimum standards, highlights the difficulty of harmonizing approaches in an area where national sovereignty remains paramount. As such, the institutional and functional differences among member states reflect a broader tension between EU-level coordination and national-level autonomy in addressing cyber threats.

TABLE 1: CYBERSECURITY COORDINATION BODIES – COMPARATIVE ANALYSIS

Country	Placement	Focus Area	Responsible Institution
Belgium	Prime Minister's Office	Centralized Coordination	Cyber Security Center Belgium (CCB)
Czech Republic	Prime Minister's Office	Strategic Oversight	National Cyber and Information Security Agency (NÚKIB)
France	Prime Minister's Office	High-Level Oversight	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Israel	Prime Minister's Office	Strategic Integration	Israeli National Cyber Directorate (INCD)
Italy	Prime Minister's Office	Strategic Integration	National Cybersecurity Agency (ACN)
Japan	Prime Minister's Office	Strategic Integration	National Center of Incident Readiness and Strategy for Cybersecurity (NISC)
Slovenia	Prime Minister's Office	Centralized Coordination/ High-Level Oversight	Government Information Security Office (URSIV)
United Kingdom	Prime Minister's Office	Indirect Coordination	National Cyber Security Centre (NCSC)/ GCHQ
Denmark	Ministry of Defence	Defence Strategy	Centre for Cyber Security (CFCS)
Lithuania	Ministry of Defence	Defence Strategy	National Cyber Security Centre
Portugal	Ministry of Defence	Defence Strategy	National Cybersecurity Centre (CNCS)
Latvia	Ministry of Defence	National Defence and Cybersecurity	Latvian National Cyber Security Policy Coordination
Estonia	Ministry of Economic Affairs and Communications	Critical Infrastructure Protection	Information System Authority (RIA)
Germany	Ministry of the Interior	Internal Security	Federal Office for Information Security (BSI)
Spain	Ministry of the Interior	Internal Security	National Cybersecurity Institute (INCIBE)
Poland	Ministry of the Interior & Digital Affairs	Counterintelligence & Digital Policy	Ministry of Digital Affairs & Internal Security Agency (ABW)
Ireland	Other Ministry (Environment & Communications)	Policy-Driven Approach	National Cyber Security Centre (NCSC)
Cyprus	Other Ministry (Innovation & Digital Policy)	Digital Innovation	Cyprus Cybersecurity Agency
Netherlands	Other Ministry (Justice & Security)	Legal Framework	National Cyber Security Centre (NCSC)
Sweden	Other Ministry (Justice)	Emergency Preparedness	Swedish Civil Contingencies Agency (MSB)
Croatia	President and Prime Minister (Hybrid Model)	Hybrid: National Security & Digital Policy	Security and Intelligence Agency (SOA)

Sources: https://enisa.europa.eu; https://csirtsnetwork.eu; https://ecs-org.eu/publications/; webpages of responsible institutions.

4.2 Consolidation and International Collaboration in National Cybersecurity Approaches

National cybersecurity frameworks are increasingly converging around common trends, driven by the need for greater efficiency, capacity building, and international alignment. A key development is the consolidation of capabilities, as acute shortages of skilled personnel in public cybersecurity sectors have led to the integration of technical, operational, and policy functions within single agencies. This approach simplifies coordination at national and international levels. Civilian cybersecurity agencies are merging policymaking, operational, and technical responsibilities, while military cyber units and law enforcement are expanding their cyber capabilities. In intelligence, Techint (Technical Intelligence) and Hackint (Hacking Intelligence) have become indispensable tools, reflecting the evolving nature of cyber threats (Singer and Friedman 2014, 95).

Joint operations are increasingly common, showcasing collaboration across civilian, military, intelligence, and law enforcement domains. Notable examples include Operation PowerOFF, targeting DDoS-for-hire services in a joint effort by Europol and the FBI to disrupt illegal cyber services (Europol 2024). Another example is the disruption of the Conti ransomware group, a coordinated effort involving international law enforcement and private cybersecurity firms

(Europol 2022). NATO's Cyber Coalition Exercise serves as a prime example of integrating military and civilian capabilities during simulated cyberattacks to enhance collective defence (NATO 2024).

In May 2024, Polish authorities reported a significant cyber espionage campaign attributed to the Russian-linked group APT28, also known as Fancy Bear. This operation targeted Polish government institutions, aiming to compromise networks and exfiltrate sensitive information. The collaborative response involved CERT Polska (CSIRT NASK) and CSIRT MON, exemplifying the importance of joint efforts in addressing sophisticated cyber threats (CERT Polska 2024).

On the international front, agreements and frameworks are adapting to reflect these changes. NATO's Cyber Defence Pledge requires member states to designate Points of Contact (POCs) that integrate technical, military, and political aspects, ensuring cohesive responses during crises (NATO 2016). Memoranda of Understanding (MoUs) between NATO and member states formalize collaboration between national and NATO cyber entities. Additionally, updates to the Budapest Convention on Cybercrime enhance international cooperation and the ability to conduct joint operations. This consolidation of capabilities and adaptation of international frameworks underscores a global trend toward integrated and interoperable cybersecurity strategies. These efforts aim to address the growing complexity of cyber threats through unified domestic measures and strengthened international collaboration. In our opinion, the future organization of cybersecurity will be determined by the following key factors:

- **Technology Infrastructure**: The evolution of technology infrastructure significantly influences the organization of cybersecurity within nation-states. The integration of advanced technologies such as cloud computing, Internet of Things (IoT) devices, and artificial intelligence (AI) has expanded the digital landscape, introducing both opportunities and challenges for cybersecurity frameworks. The convergence of information technology (IT) and operational technology (OT) has led to increased interconnectivity, enhancing efficiency but also broadening the attack surface vulnerable to cyber threats. This integration necessitates a re-evaluation of cybersecurity strategies to encompass both IT and OT environments, ensuring comprehensive protection across all technological facets (Deloitte Insights 2022). Emerging technologies, while offering innovative solutions, also introduce new vulnerabilities. The rapid adoption of AI and machine learning, for instance, presents challenges in securing these systems against adversarial attacks. Similarly, the anticipated rise of quantum computing poses potential risks to current cryptographic standards, prompting the need for quantum-resistant encryption methods. To address these complexities, organizations are increasingly adopting a "resilience by design" approach, which emphasizes building systems capable of withstanding and recovering from cyber incidents. This paradigm shift moves beyond traditional security measures, advocating for inherent resilience within technological infrastructures (World Economic Forum 2024). Furthermore, the expansion of digital infrastructure requires a re-evaluation of cybersecurity investments. Organizations are recognizing the necessity of integrating cybersecurity measures into the foundational design of technological systems, rather than treating them as ancillary considerations. This integration ensures that security is an integral component of technological advancement, aligning with the evolving threat landscape (Katara 2022). In conclusion, the progression of technology infrastructure profoundly impacts the organization of cybersecurity within nation-states. The increasing

complexity and interconnectivity of digital systems demand a holistic and proactive approach to cybersecurity, integrating resilience and security into the very fabric of technological development. By embracing these strategies, nation-states can better safeguard their digital assets and maintain robust cybersecurity postures in an ever-evolving technological landscape.

- **Institutional Dynamics**. Institutional dynamics significantly influence the organization and effectiveness of national cybersecurity frameworks. In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) has faced challenges due to inter-agency silos and political pressures, which have impacted its ability to coordinate comprehensive cybersecurity strategies. Recent developments suggest that changes in administration could further affect CISA's role and effectiveness in safeguarding national infrastructure (Geller 2024). In contrast, Estonia exemplifies a cohesive, civilian-led approach to cybersecurity. Following significant cyberattacks in 2007, Estonia established the Estonian Information System Authority (RIA), which coordinates cybersecurity efforts across government agencies and the private sector. This centralized model has enhanced Estonia's resilience against cyber threats and serves as a model for effective national cybersecurity organization (Choucri et al 2017). The disparity between fragmented and cohesive institutional approaches underscores the importance of integrated strategies in cybersecurity. Nations with centralized coordination mechanisms, clear policy frameworks, and collaborative environments are better equipped to respond to and mitigate cyber threats. As cyber threats continue to evolve, the effectiveness of national cybersecurity efforts will increasingly depend on the ability to foster cohesive institutional dynamics and inter-agency collaboration.
- **Cultural and Strategic Drivers**. Cultural and strategic drivers significantly influence the organization of cybersecurity within nation-states. National culture shapes perceptions of cyber threats and informs the development of cybersecurity policies. For instance, societal attitudes toward privacy and authority can determine the emphasis placed on individual versus collective security measures. Kshetri and Alcantara (2015) note that cultural factors influence how cybercrimes are defined and addressed, leading to variations in cybersecurity practices across countries. Strategic drivers, including national security priorities and economic considerations, also play a crucial role. Nations perceiving cyber threats as significant risks may establish centralized cybersecurity agencies to coordinate defence efforts. Conversely, countries prioritizing economic growth might focus on protecting intellectual property and critical infrastructure. The alignment of cybersecurity strategies with national objectives ensures that resources are allocated effectively to address the most pertinent threats.

Organizational culture within institutions further impacts cybersecurity effectiveness. An environment that promotes security awareness and compliance can enhance an organization's resilience to cyber threats. Conversely, a lack of emphasis on cybersecurity within the organizational culture can lead to vulnerabilities. The MIT Sloan School of Management defines organizational cybersecurity culture as "the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organization from cyber-attacks" (MIT Sloan School of Management 2018). In conclusion, cultural and strategic drivers are integral to shaping the organization of cybersecurity. Understanding and integrating these factors into policy development and organizational practices are essential for creating robust cybersecurity frameworks that are responsive to both national and organizational contexts.

5 CONCLUSION

Cybersecurity is not merely a technological challenge, but a multidimensional issue deeply embedded in political, social, and economic contexts. It intersects with governance, national security, and societal resilience, making it a complex and evolving field. Bridging the gaps between technological determinism, governance, and security demands nuanced understanding and collaborative efforts. As the digital landscape continues to evolve, so too must our approaches to ensuring a safe and equitable cyberspace for all.

The organization of cybersecurity within nation-states exemplifies this complexity. While technology provides the tools, outcomes are critically shaped by socio-political contexts, institutional interplay, and cultural underpinnings. National approaches vary widely, reflecting functional and institutional heterogeneity. Many countries adopt a "silos-based" structure, developing distinct yet interconnected pillars of cybersecurity: cybercrime enforcement, intelligence operations, military cyber commands, and civilian cybersecurity agencies. Each of these pillars addresses specific aspects of cybersecurity, from protecting critical infrastructure and responding to incidents (e.g., GovCERTs and Security Operations Centers, SOCs) to safeguarding national defence and conducting cyber intelligence.

This diversity highlights the tension between the need for functional interoperability and harmonization on one hand, and the persistence of organizational and institutional heterogeneity on the other. While frameworks such as the EU's NIS Directive and NATO's Cyber Defence Pledge promote collaboration and standardization, effective implementation requires significant effort in aligning policies and integrating capabilities across national and international levels. Moreover, emerging technologies like artificial intelligence (AI) and quantum computing present new challenges and opportunities. These technologies have the potential to revolutionize cybersecurity practices but also amplify risks, necessitating proactive strategies and adaptive governance. Future research should explore the socio-technical implications of these advancements, focusing on how they can be integrated into existing cybersecurity frameworks without exacerbating disparities or vulnerabilities.

Ensuring cybersecurity requires more than technical solutions; it demands cohesive strategies that balance innovation, governance, and social considerations. Functional interoperability must be pursued alongside respect for institutional diversity, recognizing that cybersecurity is as much about culture and policy as it is about technology. By fostering collaboration and resilience at all levels, from local agencies to global frameworks, we can work toward a secure digital future that benefits all members of society.

REFERENCES

Abbate, Janet. 1999. *Inventing the Internet*. Cambridge, MA: MIT Press.

Bijker, W. E., T.P. Hughes and T.J. Pinch. 1987. *The Social Construction of Technological Systems*. Cambridge, MA: MIT Press.

Broadhurst, Roderic. 2006. "Developments in the Global Law Enforcement of Cyber-Crime." *Policing: An International Journal of Police Strategies & Management* 29 (3): 408–433.

Budapest Convention on Cybercrime. 2001. Available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Casey, Eoghan. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed*. Waltham, MA: Academic Press.

CERT Polska. "APT28 Campaign Targeting Polish Government Institutions." 8 May 2024. Available at https://cert.pl/en/posts/2024/05/apt28-campaign.

Choucri, Nazli, Stuart Madnick and Jeremy Koepke. 2017. *Institutions for Cybersecurity: Challenges and Opportunities*. Cambridge, MA: Massachusetts Institute of Technology. Available at https://dspace.mit.edu/bitstream/handle/1721.1/144062/Choucri%2C%20Madnick%2C%20Koepke%20%282017%29%20Institutions%20for%20cyber%20security.pdf.

Croatian Security and Intelligence Agency (SOA). 2024. Available at https://www.soa.hr/.

CSIS. 2021. "The SolarWinds Cyberattack." Center for Strategic and International Studies. Available at https://www.cisecurity.org/solarwinds.

Cybersecurity and Infrastructure Security Agency (CISA). 2024. "Einstein Intrusion Detection and Prevention System." Available at https://www.cisa.gov/einstein.

Cybersecurity Intelligence. "SektorCERT." Available at https://www.cybersecurityintelligence.com/sektorcert-10219.html.

Czosseck, Christian, Rein Ottis and Anna-Maria Talihärm. 2011. "Estonia after the 2007 Cyber Attacks: Legal, strategic and organisational changes in cyber security." *International Journal of Cyber Warfare and Terrorism* 1 (1): 24–34.

Dafoe, Allan. 2015. "On Technological Determinism: A Typology, Scope Conditions, and a Mechanism." *Science, Technology, & Human Values* 40 (6): 1047–1076.

Davies, Amanda and Ghaleb Krame. 2023. "Integrating Body-Worn Cameras, Drones, and AI: A Conceptual Framework for Advancing Policing Strategies." *Policing: A Journal of Policy and Practice* 17: 1–13.

Deloitte Insights. 2022. "Incentives are key to breaking the cycle of cyberattacks on critical infrastructure." Available at https://www2.deloitte.com/us/en/insights/industry/public-sector/cyberattack-critical-infrastructure-cybersecurity.html.

Dunn Cavelty, Myriam and Andreas Wenger. 2020. "Cybersecurity Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41 (1): 5–32.

European Parliament and Council. 2016. Directive (EU) 2016/1148 on Security of Network and Information Systems (NIS Directive). *Official Journal of the European Union*, 19 July 2016. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

Europol. 2022. "Ransomware: Key Insights and Mitigation Strategies." *European Union Agency for Law Enforcement Cooperation.* Available at https://www.europol.europa.eu.

Europol. 2023. "International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war." Available at https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war.

Europol. 2024. Operation PowerOFF: Tackling DDoS-for-Hire Services. Available at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-shuts-down-27-ddos-booters-ahead-of-annual-christmas-attacks.

Federal Office for Information Security (BSI). 2024. "Das Nationale Cyber-Abwehrzentrum." Available at https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/Nationales-IT-Lagezentrum/Nationales-Cyber-Abwehrzentrum/nationales-cyber-abwehrzentrum.html.

Geller, Eric. 2024. "The Top Cybersecurity Agency in the US Is Bracing for Donald Trump." *Wired*, 16 December 2024. Available at https://www.wired.com/story/cisa-cuts-trump-2.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. Washington, DC: Cyber Conflict Studies Association.

Healy, Jason. 2024. "Cyber Effects in Warfare: Categorizing the Where, What, and Why." *Texas National Security Review* (7): 37–50.

Herman, Michael. 2021. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Holt, Thomas J. and Jin R. Lee. 2019. "Policing Cybercrime through Law Enforcement and Industry Mechanisms." In *The Oxford Handbook of Cyberpsychology*, ed. Alison Attrill-Smith et al., 645–662. Oxford: Oxford University Press.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2015. *Policing Cybercrime and Cyberterror*. Durham, NC: Carolina Academic Press.

Hutchins, Eric M., Michael J. Cloppert and Rohan M. Amin. 2020. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." *Security and Technology*, available at https://securityandtechnology.org/wp-content/uploads/2020/07/lm-white-paper-intel-driven-defense.pdf.

Ilascu, Ionut. 2024. "Romania's election systems targeted in over 85,000 cyberattacks." *Bleeping Computer*, available at https://www.bleepingcomputer.com/news/security/romanias-election-systems-targeted-in-over-85-000-cyberattacks/.

Janofsky, Adam. 2022. "U.S. Cyber Command Deployed 'Hunt Forward' Defenders to Croatia to Help Secure Systems." *The Record*, 18 August 2022. Available at https://therecord.media/cyber-command-deployed-hunt-forward-defenders-to-croatia-to-help-secure-systems.

Katara, Si. 2022. "How Technology Can Mitigate Cybersecurity Risks To Infrastructure." *Forbes*, available at https://www.forbes.com/councils/forbestechcouncil/2022/09/23/how-technology-can-mitigate-cybersecurity-risks-to-infrastructure/.

Kshetri, Nir and Lailani Laynesa Alcantara. 2015. "Cyber-threats and cybersecurity challenges: A cross-cultural perspective." Available at https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cyberthreats_2015.pdf.

Kuba, Ondřej and Jan Stejskal. 2024. "E-Voting as a Tool to Reduce Unequal Voter Turnout in the Czech Republic." *Journal of Comparative Politics* 17 (1): 19–31.

Levy, Steven. 2001. *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age*. New York: Viking Penguin.

Lin, Herbert. 2016. "Cyber Conflict and International Law." *Georgetown Journal of International Affairs* 17 (1): 98–106.

MIT Sloan School of Management. 2018. "Building a Model of Organizational Cybersecurity Culture." Available at https://mitsloan.mit.edu/shared/ods/documents?PublicationDocumentID=7507.

Mitre ATT&CK. 2023. "Adversarial Tactics, Techniques, and Common Knowledge." Available at https://attack.mitre.org/.

Moore, Gordon E. 1965. "Cramming More Components onto Integrated Circuits." *Electronics* 38 (8): 114–117.

National Cybersecurity Strategy. 2023. Available at https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

NATO. 2016. Cyber Defense Pledge. Available at https://www.nato.int/cps/en/natohq/topics_133127.htm.

NATO. 2024. Cyber Coalition Exercise: Enhancing Collective Defense. Available at https://www.act.nato.int/article/cyber-coalition-collective-defence.

Nye, Joseph S. 2011. *The Future of Power*. New York: Public Affairs.

Olive, Noemie and Charlotte Van Campenhout. 2024. "'Ghost' cybercrime platform dismantled in global operation 51 arrested." Available at https://www.reuters.com/technology/cybersecurity/ghost-cybercrime-platform-dismantled-global-operation-51-arrested-2024-09-18/.

Ottis, Rain. 2008. "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." *Proceedings of the 7th European Conference on Information Warfare and Security*, 163–168.

Reuters. 2024. "US charges Russian-Israeli dual national tied to Lockbit ransomware group." 20 December 2024. Available at https://www.reuters.com/technology/cybersecurity/us-charges-russian-israeli-dual-national-tied-lockbit-ransomware-group-2024-12-20/.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Schiliro, Francesco. 2023. "Building a Resilient Cybersecurity Posture: A Framework for Leveraging Prevent, Detect and Respond Functions and Law Enforcement Collaboration." *arXiv preprint*, available at https://arxiv.org/abs/2303.10874.
SentinelOne. 2024. "What Are TTPs? Tactics, Techniques & Procedures – Inside the Mind of a Cyber Attacker." Available at https://www.sentinelone.com/blog/inside-the-mind-of-a-cyber-attacker-tactics-techniques-and-procedures-ttps-every-security-practitioner-should-know/.
Singer, P. W. and Allan Friedman. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.
Siukonen, Veikko. 2019. "Human factors of cyber operations: Decision making behind advanced persistence threat operations." *Reading: Academic Conferences International Limited*. Available at https://www.proquest.com/conference-papers-proceedings/human-factors-cyber-operations-decision-making/docview/2261007345/se-2.
Smith, Merritt R. and Leo Marx. 1994. *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge, MA: MIT Press.
Spafford, Eugene H. 1989. "The Internet Worm Incident." *Communications of the ACM* 32 (6): 678–687.
Štrucl, Damjan. 2023. "Cyber Security and Cyber Defence Comparison of Various NATO Member States." *Baltic Rim Economies* 2 (2023): 52–59.
Svete, Uroš. 2012. "European E-Readiness? Cyber Dimension of National Security Policies." *Journal of Comparative Politics* 5 (1): 38–59.
Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.
Wall, David S. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.
Whitman, Michael E. and Herbert J. Mattord. 2022. *Principles of Information Security. 7th ed*. Boston: Cengage Learning.
World Economic Forum. "5 cybersecurity risks posed by emerging technology – and how we can defend against them." Available at https://www.weforum.org/stories/2024/10/cyber-resilience-emerging-technology-ai-cybersecurity.
Zakon o informacijski varnosti (ZInfV) [Information Security Act]. 2018. *Official Gazette of the Republic of Slovenia,* no. 30/18, 25 April 2018. Available at https://pisrs.si/pregledPredpisa?id=ZAKO7707.
Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown.
ZSIS. 2024. National Cyber Security Framework in Croatia. Available at https://www.zsis.hr/default.aspx?id=553.

KIBERNETSKA VARNOST MED TEHNOLOŠKIM DETERMINIZMOM, POLITIČNIM VLADOVANJEM IN IZZIVI NACIONALNE VARNOSTI

Članek izhaja iz temeljne teze, da organiziranost kibernetske varnosti v posamezni državi ni določena zgolj s tehničnimi vidiki informacijsko-komunikacijske tehnologije, temveč jo oblikujejo kompleksni odnosi med civilnimi institucijami za kibernetsko varnost, obveščevalnimi službami, vojaškimi zmogljivostmi in organi pregona. Poleg tega imajo pomembno vlogo tudi politična in varnostna kultura države, njena vpetost v mednarodne organizacije ter način zaznavanja groženj nacionalni varnosti. Analiza v članku temelji na teoretskih okvirih tehnološkega determinizma in konstruktivizma ter uporablja primerjalno metodologijo. Avtor preučuje razloge za obstoječe funkcionalne in institucionalne razlike med

državami, ki so si sicer politično-upravno sorodne in si prizadevajo za uskladitev svojih pristopov prek mehanizmov, kot so evropska zakonodaja o kibernetski varnosti, mednarodni tehnični in politični standardi ter pobude za vzpostavitev mednarodnega pravnega okvira za delovanje v kibernetskem prostoru.

Ključne besede: kibernetska varnost, informacijsko-komunikacijska tehnologija, nacionalna varnost, tehnološki determinizem, institucionalni imperializem.