No Universal Blueprint: A Structured, Focused Comparison of Eight European National Cyber(-security) Strategies

by Gazmend Huskaj and Stefan Axelsson

Resumé

Denna studie tillämpar en strukturerad, fokuserad jämförelse av åtta europeiska länders nationella cybersäkerhetsstrategier för att beskriva hur och varför stater antar olika modeller för ledning och styrning av cybersäkerhet. Den jämför tekniskt centrerade ramverk, som betonar kompetensförsörjning, reglering och krishantering, med bredare allomfattande strategier. Analysen visar att variationer i hotuppfattning, resursbegränsningar och strategiska kulturer påverkar varje lands fokus på teknik, policy, eller en kombination av båda. Små och medelstora stater balanserar lokala prioriteringar – såsom ekonomisk tillväxt och skydd av kritisk infrastruktur – med yttre åtaganden, inklusive EU-direktiv och NATO-åtaganden. Resultaten visar att det inte finns någon universell modell: nationella kontexter, politiska strukturer och allianstillhörigheter formar strategiernas omfattning. Studien identifierar en konvergens kring internationella ramverk, men också en divergens i hur styrningen utformas. Dessa observationer antyder att cybersäkerhetsinsatserna är beroende av tydliga rättsliga mandat, anpassningsbara partnerskap och förståelse för varje nations unika operativa förutsättningar. Slutsatserna lyfter fram centrala variabler – hotuppfattning, institutionell kapacitet och alliansrelationer – som påverkar hur regeringar utformar och utvecklar sina cyberstrategier.

DIGITAL TRANSFORMATION CONTINUES to reshape societies worldwide, prompting governments to adopt National Cybersecurity Strategies (NCSS) to enhance resilience and security.[1] These strategies typically address a range of objectives: protecting critical infrastructure, securing digital services, promoting economic competitiveness, and building international partnerships.[2] Despite shared global drivers and similar threat landscapes, states frequently diverge in how they conceptualize and implement their NCSS. In particular, smaller and mid-sized nations may balance resource constraints with ambitions to maintain strategic autonomy and fulfill external obligations.[3] Larger or more centralized states often adopt more integrated, top-down approaches.[4] This variation shows that there is no single, "blueprint" for cybersecurity governance—covering everything from workforce training and crisis response to international legal frameworks.[5]

Recent research indicates that even close neighbors can differ considerably in their governance philosophies and strategies for mitigating cyber risk.[6] Certain strategies emphasize a holistic "whole-of-society" perspective, merging citizen engagement, industry partnerships, and public-sector coordination.[7] Others focus on strictly technical or

regulatory measures, guided by legislation or capacity-building programs.[8] The key question, then, concerns the deeper reasons behind these contrasts: Are they attributable to differences in perceived threat levels, structural governance, or economic objectives? Or do they reflect broader foreign-policy stances, including membership in multinational alliances such as NATO and the EU?[9]

The present article joins ongoing scholarly debates by conducting a structured, focused comparative analysis of national cybersecurity strategies across eight European nations. Employing Alexander L. George's structured, focused comparison method, it explores how countries conceptualize cyber threats, shape governance arrangements, and integrate cybersecurity into their broader national security agendas.[10] It focuses on the Nordic region (Sweden, Norway, Finland, Denmark), the Netherlands, Belgium, and the United Kingdom, synthesizing their respective official strategy documents. The aim is to describe the different models of cyber governance and to draw broader lessons about how smaller and mid-sized states develop policy in a field often influenced by larger countries,[11] not to evaluate policy effectiveness.

Sweden's newly released National Cybersecurity Strategy 2025–2029 signals an emphasis on technological-cybersecurity measures, while referring readers to complementary documents for international and policy dimensions. Although this acknowledges the wider range of cyber-related issues, it also suggests a somewhat fragmented approach to developing a cyber strategy.[12] By contrast, the United Kingdom explicitly frames cybersecurity as a whole-of-society issue, led by government but in close partnership with industry, research institutions, and civil organizations.[13]

This divergence raises questions about how small and middle powers conceptualize and structure their cyber strategies, especially when aligning them with directives such as NIS2 or NATO's evolving cyber agenda.[14] Does a technologically centered approach risk overlooking crucial governance or diplomatic aspects, or is it a more practical approach given resource constraints? Conversely, does a holistic approach actually yield better resilience and strategic coherence, or does it introduce complex layers of stakeholder management that undermine efficiency?[15]

This article explores how national cybersecurity strategies compare across governance structures, emphases on technology versus policy, and international alignment—and what implications these differences might reveal about the strategic positioning among small and mid-sized European states.

The countries were selected for their broadly similar socio-economic contexts and varied institutional affiliations. Despite differences in size and governance, they share exposure to European cyber norms, offering a coherent yet diverse base for structured comparison and analysis.[16] Only publicly available documents from 2018–2025 are used.

Mapping the Scientific Domain

National Cybersecurity Strategies (NCSS) have become key policy instruments to mitigate cyber threats and support digital resilience. Scholars have employed diverse analytical approaches to evaluate and compare such strategies across countries. For example, Warren and Leitch,[17] using the ENISA framework, assessed Australia's NCSS through a European perspective, identifying structural and implementation strengths. Karazanishvili[18] and Sharikov[19] reviewed the increasing role of cybersecurity in U.S.

national security, highlighting the shift from deterrence and regulation to proactive, often offensive, postures under recent administrations. Comparative analyses, such as those by Tatar et al.[20] and Luiijf et al.,[21] reveal differences in NCSS across Europe, Asia, and North America, often shaped by national power and political priorities. Studies on Turkey[22] and Ecuador[23] underscore the importance of contextual adaptation and alignment with international standards. In South Korea, Byeon and Suh[24] identified the need to move from reactive to preemptive strategies, while Maglaras et al.[25] document Greece's coordinated institutional progress.

Beyond national and regional insights, the relevance of NCSS in global governance efforts is emphasized by Greiman[26] and Ovchinnikova and Upadhyay,[27] who explore interoperability, legal convergence, and the formation of multilateral frameworks. Across these studies, NCSS are consistently portrayed as dynamic policy instruments balancing national sovereignty, international cooperation, and cyber deterrence.

The evolving cyber threat landscape has prompted scholars to explore the militarization and securitization of cyberspace. Reveron[28] emphasizes that cyber capabilities are increasingly integrated into national defense strategies, noting the establishment of U.S. Cyber Command and the dual physical-virtual nature of modern warfare. Kshetri[29] provides a comparative analysis of North and South Korea, underscoring asymmetrical cyber warfare as a reflection of broader military tensions. Lehto[30] categorizes cyber threats into activism, crime, espionage, terrorism, and warfare, arguing that national strategies often mirror these classifications. Guitton[31] and Kasper[32] critique the European focus on reactive mitigation over deterrence, while highlighting the challenges of achieving international consensus on cyber governance.

Empirical studies have examined strategic infrastructure such as smart grids[33] and proposed frameworks like strategic anti-access/area denial in cyberspace.[34] Kolini and Janczewski[35] employ topic modelling to identify recurring themes in 60 national strategies, revealing an emphasis on critical infrastructure and public-private partnerships. Zheng et al.[36] suggest that China's cyber control mechanisms may enhance its resilience in cyber conflict. Collectively, the literature reflects growing consensus that cyber threats represent security concerns and strategic levers in current interstate competition, requiring integrated national and transnational approaches to both defense and offense in cyberspace.

A significant yet unevenly addressed theme in national cybersecurity strategies is the incorporation of offensive cyberspace capabilities. The United Kingdom stands out as a forerunner, formally establishing the National Cyber Force (NCF) in 2020—a joint initiative integrating intelligence and military expertise to "counter, disrupt, degrade and contest" adversarial threats through cyberspace.[37] The UK strategy explicitly frames offensive cyberspace operations (OCO) as tools of influence and strategic advantage, governed by domestic law and aligned with international legal norms such as the Law of Armed Conflict.

Conversely, many states remain reticent or ambiguous in public strategy documents. In some cases, as detailed in Huskaj,[38] the absence of an official deterrence doctrine, operational authority, and legal mandates hampers strategic coherence in using OCO for national security. He highlights a fragmented governance structure and lack of signalling, limiting the credibility of cyber deterrence. Strategically, OCO offer states flexible, scal-

able, and de-escalatory tools that can impose costs without physical force, making them attractive in grey zone conflicts. Huskaj's[39] Ambidextrous Framework for OCO integrates tactical-level simulations with strategic planning, demonstrating how models can feed into national cyber deterrence policies. The feedback loop between operational insights and strategic decision-making is vital to maintaining effective, adaptive deterrence.

Still, there are risks. Scholars and practitioners alike identify a global governance gap in cyberspace, particularly concerning offensive capabilities. The increasing use of proxies by state and non-state actors complicates attribution and erodes accountability, as highlighted by the Council on Foreign Relation's (CFR) Cyber Operations Tracker (CFR, n.d.)[40] and the Tallinn Manual's interpretation of international law. Moreover, the commodification of offensive tools—such as exploit kits and commercial spyware—lowers the threshold for deployment and increases the risk of escalation.[41] Effective OCO strategies thus demand clear policy frameworks, legal-ethical alignment, and multi-stakeholder coordination to manage risks and maintain strategic stability.

Public–private collaboration is another consistent theme across the literature. Limnéll and Lehto[42] emphasize Finland's comprehensive security model, where public-private coordination is central to national cyber preparedness. Similarly, Montasari[43] points to UK initiatives such as the National Cyber Security Centre (NCSC) and Active Cyber Defence program, which encourage shared threat intelligence and coordinated response mechanisms. In developing contexts, Hossain et al.[44] present a framework for operationalizing national CERTs, such as in Bangladesh, highlighting the importance of readiness and stakeholder coordination. Kim et al.[45] show that in Southeast Asia, public-private cyber cooperation serves both strategic and diplomatic functions, particularly in the rivalry between China, Japan, and South Korea. The Ukrainian case, explored by Semenchenko et al.[46] and Onyshchenko et al.[47] further underscore institutional reforms, technical regulations, and corporate cybersecurity policy to fostering systemic resilience. These insights align with Peter and Sobowale's[48] analysis, which urges Africa to develop multi-stakeholder collaboration.

Overall, public-private collaboration is consistently framed as a core enabler of cybersecurity strategy, especially for enhancing information sharing, capacity building, and coordinated response in both normal and crisis conditions.

In terms of legal and governance frameworks, the literature reflects a shift toward more complex and integrated models. Backman[49] reveals a growing shift within the EU from risk-based to threat-based approaches, triggering member state resistance to deeper integration under EU cybersecurity governance. Similarly, Wright et al.[50] propose a framework that integrates threat modeling and policy analysis to develop national cyber strategy, particularly for critical infrastructure protection. At the national level, Lampe[51] and AlDaajeh and Alrabaee[52] underscore the need for integrating cybersecurity by design into infrastructure and governance, combining digital risk management with national resilience efforts. In Taiwan, Jing[53] shows how cybersecurity has become central to national industrial policy, while in Malaysia, Aborujilah et al.[54] emphasize localized, standards-driven assessments to align education and compliance frameworks with strategy.

Internationally, Izycki and Colli[55] demonstrate converging trends in the protection of critical infrastructure across 86 national strategies, particularly through resilience

building and multi-stakeholder governance. Teoh and Mahmood[56] further assert that NCSSs are key enablers for digital economic growth, rather than mere reactive instruments. Together, these studies highlight that the legal and policy architectures underpinning national cybersecurity strategies are increasingly complex, shaped by geopolitical tensions, sectoral demands, and the imperative of multilateral cooperation in governing digital domains.

International cooperation in cybersecurity has become indispensable amid increasingly transnational cyber threats. Williams and Levi[57] emphasize the shift in the United Kingdom's policy framing of eCrime as a Tier One threat, highlighting the increased need for cooperation between public and private actors. Similarly, Ovchinnikova and Upadhyay[58] explore BRICS cooperation, suggesting that cyber maturity and digital governance are prerequisites for forming a collective cybersecurity strategy. Semenenko et al.[59] underscore Ukraine's efforts to draw on European models for strengthening national cybersecurity, emphasizing the role of institutional coordination. In Egypt, Hashem[60] stresses that knowledge exchange through national CERTs fosters more resilient national frameworks, aligning with Greiman's[61] broader argument for multilateral cyber governance and harmonized legal instruments.

Several scholars emphasize capacity building as the backbone of such cooperation. For instance, Mori and Goto[62] propose strategy reviews via global maturity models to benchmark national progress. Iova and Watashiba[63] offer a comparative study of NCSSs, identifying gaps in references to neutrality and warfare, despite widespread mention of international collaboration. These findings suggest that while cybersecurity strategies increasingly incorporate cooperative elements, significant asymmetries persist in implementation, particularly between advanced economies and emerging states. A globally consistent yet context-sensitive approach to cooperation remains key for sustained capability across jurisdictions.

A recurring theme in NCSSs is the recognition of economic and infrastructure vulnerabilities to cyber threats. Maglaras et al.[64] outline Greece's structured efforts to establish a coordinated cybersecurity policy through institutional reforms and legal decrees. Similarly, Canbek and Sagiroglu[65] emphasize the increased complexity of energy grids and the corresponding necessity for cybersecurity in smart grids. Lampe[66] and Olifirov et al.[67] highlight the shift towards secure-by-design methodologies and the challenges in protecting digital financial systems, respectively. In Taiwan, cybersecurity has been reframed as a national economic priority as according to Jing,[68] while Kasper[69] underscores global concerns over cyberattacks on critical infrastructure, despite limited progress in treaty development.

The protection of critical infrastructure (CIs) is a recurring concern across national strategies, with Izycki and Colli[70] identifying shared structural elements in 86 NCSSs. Kolini and Janczewski[71] support this view, noting institutional alignment among EU and NATO states. Meanwhile, assessments in Malaysia as noted by Aborujilah et al.[72] and Nigeria by Kademi[73] stress the contextual tailoring of frameworks. Estonia's post-2007 reforms as noted by Czosseck et al.[74] and South Africa's delayed implementation by Von Solms & Von Solms[75] demonstrate contrasting national responses. Overall, these works reinforce that protecting economic stability and critical infrastructure demands strategic coherence, adaptive legal frameworks, and public-private coordination within and across borders.

The Analytical Framework

This study employed a mixed methods approach that integrates a computational literature review, topic modeling, and thematic analysis. The overall aim was to systematically identify, organize, and interpret existing scientific literature on national cybersecurity strategy, resulting in seven focused-structured comparison questions. The research process began to collect data by formulating a precise Boolean query for Elsevier's Scopus research database which returned 489 document results. Following refinement, 70 documents were analyzed according to Mortenson and Vidgen's computational literature review method.[76] This approach leverages topic modeling via Latent Dirichlet Allocation (LDA).[77] The LDA algorithm identified 53 recurring themes, which were then interpreted through Braun and Clarke's thematic analysis procedure.[78]

The study then adopted George and Bennett's[79] structured, focused comparison method, transforming each theme into a guiding comparative question. These questions were systematically applied to the NCSSs of eight European countries, yielding an interpretive framework that captures strategic variation without evaluating policy outcomes. This research adheres to Nature's principles on disclosing the use of large language models (LLMs) as research assistants ensuring openness and transparency in the methods and trustworthiness in the results.[80]

Comparative Insights from Eight National Strategies

The seven focused questions derived from the literature review were systematically applied to the selected NCSSs. This section presents the findings across the eight cases. The organization of the results mirrors the thematic structure developed in the preceding analysis phase.

How do different countries conceptualize, design, and adapt their national cybersecurity strategies in response to internal policy goals, shifting threats, and international frameworks?

Several European nations have developed cybersecurity strategies that respond to internal policy goals, evolving threats, and international obligations, often referencing frameworks such as the NIS Directive and NATO commitments. In Belgium, the policy extends through 2025 under the Centre for Cybersecurity Belgium,[81] integrating the NIS Directive into national law to enhance resilience and explicitly recognizing NATO's role in national cyber defence. This comprehensive plan, comprising six objectives, relies on stakeholder involvement and continuous risk assessments. Meanwhile, Denmark emphasizes collective responsibility among authorities, businesses, and citizens,[82] reinforcing digital infrastructure through four strategic aims. Collaboration with the EU, UN, and NATO underpins a rules-based framework in cyberspace, supported by the technology sector, with resources allocated to maintain the country's security.

Finland, for its part, has revised its approach to accommodate shifting operational conditions linked to governmental programs,[83] updating existing policies under NIS2. This ten-year outlook encourages investment and participation from both public and private entities, integrating EU and NATO considerations alongside ongoing monitoring of cyber diplomacy and defence. A focus on future risk scenarios calls for additional resources and periodic reviews. The Netherlands likewise pursues a digitally secure environment to foster economic and social benefits,[84] setting strategic priorities

for a six-year period and employing phased, adaptive measures. Building on earlier strategies, it emphasizes collaboration among public, private, and civil society actors, regarding global cooperation—particularly within EU and NATO—as indispensable.

Other countries underscore different but related facets of cybersecurity preparedness. Norway's fourth cyber strategy, for instance, addresses rapid digitalization through intensified public–private and civil–military partnerships,[85] guiding incident management via coordinated measures across multiple stakeholders, with emphasis on training and mutual notification. The strategy also aligns national priorities with NATO, EU, and other international connections. Sweden similarly integrates NIS2 into an all-risk perspective, targeting issues such as workforce shortages and complex regulation[86] to reinforce systematic efforts established by previous national strategies. Complementing this, Swedish legislation converges with broader international standards, augmented by heightened NATO engagement.

Switzerland's approach builds upon earlier national initiatives,[87] adopting a risk-based framework that acknowledges the impossibility of full prevention but maintains that acceptable risk levels can be upheld through clear definitions of responsibility spanning state, society, and industry. This framework also highlights global cooperation—especially regarding law enforcement—to deter transnational cybercrime. Finally, the United Kingdom envisions itself as a leading democratic cyber power by 2030, anchoring its strategy in five strategic goals that strengthen national resilience and uphold an open cyberspace.[88] Linking cybersecurity with geostrategy, economic considerations, and national security, the UK underscores that border-spanning threats warrant flexible, multi-sector engagement and sustained international outreach.

How do national cybersecurity strategies address the incorporation of offensive cyberspace capabilities, and what strategic implications arise from the observed differences?

In contrast to countries that omit explicit references to offensive cyberspace capabilities, several European nations detail varying degrees of proactive measures in their national strategies. Table 1 provides a comparative overview of whether and how the eight countries under review explicitly incorporate offensive cyberspace operations and related capabilities, alongside the strategic prioritize emphasized by each NCSS.

Belgium's NCSS emphasizes the development of high-tech cyber capabilities to support national defense and critical infrastructure protection. In times of national crisis, the Ministry of Defence may deploy intrusive capabilities to neutralize attacks and identify perpetrators. While the strategy acknowledges the use of offensive cyber arsenals by foreign actors to inflict economic harm and induce instability, Belgium's own posture remains focused on defense and crisis response.[89] Denmark also acknowledges offensive cyberspace capabilities within its NCSS,[90] highlighting the importance of diplomatic responses, potential sanctions, and an offensive cyber defence aimed at detecting and countering threats by both state and non-state actors. These provisions include an "active cyber defence" meant to disrupt or deter adversary operations.

Meanwhile, Finland identifies the threat posed by offensive cyber operations targeting critical infrastructure—including energy, healthcare, and water supply—as a means of influencing political decision-making.[91] While Finland does not articulate an of-

Table 1: Explicit inclusion of offensive cyberspace capabilities in NCSSs.

Country	Explicit Mention of Offensive Operations?	Key Emphasis
Belgium	Yes – Deploys offensive capabilities during crises; supports retaliatory action	Incident response, offensive deterrence, Ministry of Defence role in sustaining high-tech cyber capabilities
Denmark	Yes – Develops "offensive cyber defence" for disruption and deception	Deterrence posture, threat detection and disruption, NATO alignment, cyber diplomacy
Finland	No – Operational capabilities acknowledged but offensive roles not specified	Holistic defence policy integration, joint operations, crisis management, public-private partnerships
Netherlands	Yes – Affirms offensive operations during peace and war	Use of cyber force in peace and war, Ministry of Defence roles, operational readiness, multilateral cooperation
Norway	No – Emphasizes defence, resilience, and coordination	Public-private cooperation, national incident handling, institutional capacity building
Sweden	No –Excludes offensive operations, focuses on regulatory and societal resilience	All-risk approach, EU/NIS2 harmonization, critical infrastructure protection, cyber hygiene
Switzerland	No – Incorporates "active cyber defence" including disruption and attribution	Threat analysis, digital sovereignty, military and intelligence roles, operational support to civil authorities
UK	Yes – Offensive capabilities led by National Cyber Force	Strategic deterrence, global leadership, full-spectrum cyber power, legally governed offensive operations

fensive posture, the strategy signals preparedness for active cyber defence, attribution, and countermeasures in response to state-sponsored threats. These provisions are embedded within a broader emphasis on situational awareness and capability development under its national defence remit. Cyber defence operations are further harmonised with Finland's broader foreign and security policy, underscoring the strategy's comprehensive and integrated approach to national cyber defence.

Other nations articulate similar or complementary positions. The Netherlands frames its Ministry of Defence as an offensive digital force, extending beyond traditional wartime usage to peacetime operations as well.[92] By contrast, Norway's national strategy does not address offensive cyberspace capabilities, instead placing emphasis on stakeholder coordination, civil–military collaboration, and crisis response—specifically omitting references to disruptive or intrusive actions.[93] Sweden likewise refrains from mentioning any offensive role, concentrating instead on regulatory alignment, workforce development, and resilient systems within an all-risk perspective in line with EU directives and NATO commitments.[94]

Switzerland explicitly includes active cyber defence, outlining procedures for threat detection, attribution, and disruption under both military and intelligence domains.[95] The Swiss National Cyberstrategy underscores readiness to identify attackers and forestall future incidents, supporting civil authorities when needed through disruptive actions. Finally, the United Kingdom integrates offensive cyberspace operations most prominently through its National Cyber Force (NCF), which consolidates expertise from GCHQ, the Ministry of Defence, and other agencies.[96] Substantial investments via the National Offensive Cyber Programme and the NCF equip the UK to counter various state and criminal threats under a clear le-

gal framework, reflecting an explicit commitment to using offensive capabilities to shape broader cyber deterrence objectives.

How do states define and address cyber threats (including state-sponsored operations, eCrime, and cyberterrorism) within modern warfare doctrines and national security priorities?

Across Europe, a broad spectrum of cyber threats is recognized, encompassing actors driven by financial profit, geopolitical objectives, and disruptive intent. Belgium identifies criminal organizations engaging in phishing, data theft, and ransomware, occasionally escalating to sabotage activities that imperil institutional stability.[97] Foreign intelligence services reportedly use advanced techniques to obtain classified data or disrupt domestic targets, while cyberterrorism seeks to spread fear by undermining public services and critical infrastructure. The shift from mainly financial motives to geopolitical drivers is highlighted as especially troubling, forming a component of wider hybrid threats.

In Denmark, the strategic overview points to cybercrime, cyberespionage, and potential destructive attacks pursued by both state and criminal operators.[98] Criminal enterprises swiftly exploit technological developments, and foreign intelligence services employ sophisticated hacking to breach Danish systems. Official assessments rate the risk of cybercrime and cyberespionage as very high, while destructive cyberattacks and activism are seen as lower-level concerns.

Several nations underscore the growing complexity of hybrid operations targeting critical services and key infrastructure. Finland notes that state-sponsored espionage and hybrid influences escalate political objectives through cyber means, anticipating an intensification of crime and terrorism online.[99] Defensive measures now extend beyond technical countermeasures, acknowledging an evolving landscape in which organized groups threaten essential services and offensive campaigns may strike energy, water, or healthcare infrastructures. Similarly, the Netherlands identifies state actors and cybercriminals as principal threats, often overlapping in their methodologies.[100] Cybersecurity is integrated into the nation's six fundamental security interests, with law enforcement pursuing a comprehensive disruption strategy to confiscate illicit profits and prosecute offenders. At the same time, Dutch defense policy envisages digital operations beyond last-resort scenarios, indicating a more proactive stance.

Norway classifies potential adversaries as states, groups, or private entities capable of sabotage, espionage, or criminal attacks, some of which may qualify as armed aggression under the UN Charter.[101] Police efforts have increased to address cybercrime, although rapid technological progress introduces added challenges for investigations.[102] Distinctions between peace and conflict are blurred by hybrid threats, creating security and economic vulnerabilities for Norway.

Other countries emphasize both espionage and criminal threats with varying degrees of sophistication. In Sweden, state-backed actors increasingly target critical infrastructure for data exfiltration or disruption, sometimes as standalone incidents and sometimes as part of broader hybrid activities.[103] Ransomware and data theft perpetrated by criminal groups have also proliferated, and the growing use of tools such as generative AI and new communication services enhances the cross-border reach and sophistication of such operations. Politically motivated cyberactivists may also align with state interests, further complicating the threat environment. Switzerland, meanwhile, under-

scores the role of state or semi-state groups engaging in cyberespionage and cybersabotage to disrupt or destroy ICT functionality.[104] Instances of cybersubversion seek to weaken the political systems of adversaries, occasionally through disinformation campaigns. As cyberoperations gain traction in armed conflicts—due to their capacity for high-impact actions with ambiguous attribution—the prevalence of cybercrime for extortion also remains a persistent concern.

Finally, the United Kingdom continues to face an expanding array of threat actors, including state agencies and criminal collectives, that employ cyberattacks for espionage, profit, sabotage, and disinformation.[105] National law enforcement, anchored by the National Crime Agency, coordinates anti-cybercrime measures. Ransomware is singled out as a leading challenge, on par with state espionage in severity. Offensive cyberspace operations fall under the purview of the National Cyber Force, further supported by alliances aimed at neutralizing significant global threats, including those originating from Russia's organized crime networks.

In what ways do national cybersecurity strategies foster public-private partnerships, and how do these collaborations influence cyber resilience and information-sharing?

Collaboration between public, private, and academic institutions emerges as a central theme across multiple European countries' cybersecurity strategies. In Belgium, platforms for continuous information sharing are jointly managed by public and private actors alongside academia, facilitated by the Cyber Security Coalition and the Centre for Cybersecurity Belgium.[106] Denmark likewise emphasizes shared responsibility among government, industry, and citizens, bolstering cyber readiness through practical measures and advisory councils, including the Danish Cyber Security Council and a specialized unit for small and medium-sized enterprises.[107] In Finland, a partnership-based model fosters trust by encouraging information exchange across public and private sectors, supported by centralized cybersecurity services and a predominantly business-driven cyber ecosystem.[108]

Similarly, the Netherlands maintains a public–private framework that broadens threat awareness, calling for larger or more advanced participants to assist less mature entities. This approach is reinforced by the digital cybersecurity knowledge center, Dcypher, and information-sharing frameworks such as the LDS.[109]

A comparable reliance on shared responsibilities and strong communication structures is evident elsewhere. Norway focuses on public–private partnerships for improved situational awareness and incident handling, acknowledging that much of the nation's digital infrastructure is privately owned.[110] Sweden promotes close and sustained cooperation and communication channels between governmental and private organizations, including real-time data exchange platforms, recognizing that effective incident prevention and response require collective engagement.[111] In Switzerland, federal and cantonal collaboration is underpinned by various mixed public–private formats, a steering committee bridging expertise across sectors, and an Information Sharing and Analysis Centre (ISAC).[112]

Finally, the United Kingdom highlights multi-sector integration, mobilizing government, industry, and academia through regional networks, Cyber Resilience Centres, and the National Cyber Security Centre's threat intelligence communities, all shaped by ongoing consultations with devolved administrations and private entities.[113]

How do legal and policy frameworks for cybersecurity governance vary across jurisdictions, and to what extent do they align (or conflict) with international norms and regulations?

A shared emphasis on international legal frameworks and multi-level regulations characterizes many nations' cybersecurity strategies. In Belgium, federal authorities take the lead, with the transposition of the 2016 NIS Directive into Belgian law in April 2019 forming a core legal scaffold for safeguarding public networks and information systems.[114] Subsequent acts, including the Cybersecurity Act of 2019, expanded ENISA's role at the EU level. The Belgian NIS Act and accompanying decrees clarify the obligations of sectoral authorities in designating essential service operators and enforcing security standards, while alignment with EU certification protocols reinforces ICT product security assessments. Similarly, Denmark adopts the NIS Directive as the backbone of its regulatory approach, mandating risk-based technical and organizational measures.[115] In parallel, Denmark engages with international organizations such as the UN and the tech industry to strengthen rule-based norms for cyberspace, also delineating boundaries between war and peace in this domain.

Other countries likewise anchor their national laws in EU or allied directives, sometimes integrating principles from broader organizations like NATO. Finland aligns its cybersecurity legislation with EU regulations, underscoring that international law, including the possibility of state liability, applies to ICT activities.[116] It also advocates coordinated objectives between NATO and the EU. In the Netherlands, a hierarchical legislative principle favors applying EU-level regulations first and resorting to national statutes as necessary.[117] Here, proportional security requirements address market gaps, while national policy holds that prohibitions on force and non-intervention extend to cyberspace—therefore, a cyberattack could constitute an armed attack. Norway, although not an EU member, draws its regulatory basis from national security and data-processing acts, while coordinating cross-border digital dependencies through partnerships with the UN, NATO, EU, OECD, and OSCE.[118] An open, internationally agreed-upon set of standards is encouraged, and stakeholder involvement is considered paramount.

A similar pattern emerges in Sweden, which adapts its policy to comply with the NIS2 Directive through ongoing legislative revisions.[119] Meanwhile, both the Cyber Resilience Act and the Cybersecurity Act apply directly within EU member states, highlighting the significance of EU–NATO cooperation as NATO focuses increasingly on technical matters. Switzerland, despite its distinct federal structure, likewise links cybersecurity measures to international standards, noting that any new policies require legal clarity on data sharing and scope of authority.[120] International law underpins Swiss digital policy, and bilateral agreements define state responsibilities. In the United Kingdom, domestic legislation, including the Intelligence Services Act 1994 and the Investigatory Powers Act 2016, informs the operations of the National Cyber Force.[121]

Concurrently, the UK enforces the NIS Regulations, which obligate operators of essential services and digital providers to maintain robust technical and organizational safeguards. Supporting NATO's cyber capacities, the UK acknowledges that member nations' sovereign cyber operations may integrate with collective defense missions, indicating a further commitment to global partnerships and established international norms.

How do bilateral, multilateral, and institutional partnerships shape national cybersecurity policies, and what are the key enablers or barriers to deeper global collaboration?

Collaboration and engagement with international institutions emerge as central threads in many European cybersecurity strategies, reflecting the transnational character of digital threats. In Belgium, the strategy underscores alignment with EU and NATO agendas to preserve an "open, free and secure cyber environment," complemented by bilateral ties designed to bolster mutual trust.[122] The Centre for Cybersecurity Belgium works in tandem with the Ministry of Defence and Foreign Affairs to ensure coherent external representation, while the Cyber Security Coalition fosters knowledge-sharing among private, public, and academic sectors. Denmark likewise views EU, UN, and NATO cooperation as pivotal to maintaining an open and secure internet, emphasizing that diplomacy and engagement with global technology firms can address root causes of cyberattacks.[123]

Finland relies on the EU Cyber Diplomacy Toolbox and close coordination with NATO, the UN, and various international forums.[124] Finnish policy focuses on attributing attacks and applying countermeasures when necessary, reinforcing synergy among administrative tiers and spotlighting resource, workforce, and compliance challenges.

Other nations underscore similar principles while tailoring their approaches to distinct national contexts. The Netherlands aspires to form coalitions that advance responsible state behavior, integrating fundamental freedoms into EU and Council of Europe discussions.[125] National authorities offer incentives or impose regulations where necessary, in accordance with each sector's maturity and overarching interests. Norway, in turn, partners with the UN, NATO, EU, OECD, and OSCE to promote established standards of state conduct and hinder cybercrime, alongside bilateral and regional dialogues that recognize global interdependencies.[126] In Sweden, authorities intensify bilateral and multilateral network participation, coordinating at home through interagency structures and abroad through forums linked to EU and NATO security.[127] Moreover, Sweden's expanding involvement in standardization and research enhances its credibility as a reliable ally.

Switzerland focuses on operational partnerships and bilateral pacts that clarify legal obligations online, aligning national cybersecurity efforts with international frameworks and supporting global organizations through robust collaboration.[128] Finally, the United Kingdom strengthens ties with key institutions such as the UN, NATO, and G7, employing "cyber hygiene" campaigns and sanctions to deter malicious actors.[129] Broader capacity-building efforts across diverse regions further protect UK interests, promote shared values, and advance both economic and security goals.

How do states integrate cybersecurity into their critical infrastructure protection and overall economic resilience, and what factors guide their investment decisions?

Several national strategies prioritize identifying essential services and integrating investment plans to enhance resilience against emerging technological risks. In Belgium, "Organizations of Vital Interest" (OVI) span both public and private spheres—encompassing critical infrastructures, essential services, digital services, and nuclear sites—supported by government and private funding to promote economic opportunities and readiness.[130] The Federal Public Service (FPS) Economy coordinates cybersecurity

endeavors across multiple domains, highlighting that trust in digital services is vital for productivity and growth. Denmark, likewise, addresses government, critical infrastructure operators, and private businesses jointly, aiming to maintain vital societal functions even under cyberattacks that could disable core ICT systems.[131]

Ministries overseeing critical functions must formulate sectoral strategies and set up decentralized cyber units, culminating in an overall allocation of DKK 270 million for 34 initiatives. A stronger cyber ecosystem is envisioned to drive both security and market development, mindful of persistent threats from cybercrime and state-sponsored espionage.

A similar emphasis on infrastructure and strategic investments appears in Finland, where essential services, data storage, and security-of-supply frameworks form the core of national cybersecurity policy.[132] Public spending of approximately €300 million is augmented by businesses investing around ten times more, aligning with NATO and EU support to cultivate a dynamic cyber ecosystem. This approach reinforces comprehensive security, defense, and broader digital engagement. In the Netherlands, organizations with critical or governmental responsibilities adhere to a risk-based model, centering on operational technology crucial for service continuity.[133] Cyber resilience is framed as an economic advantage that enhances competitiveness. Implementation unfolds through phased strategic aims, funded by €111 million in structural investments and an additional €300 million devoted to intelligence, economic security, and critical infrastructure.

Norway's policy underlines trustworthy digital infrastructure for critical societal services, taking into account interdependencies such as power grids and telecommunications.[134] Public and private owners of key systems must fulfill security requirements, and digitalization is identified as integral to fostering public trust and economic growth. In Sweden, the focus on critical infrastructure, often managed by private entities, is viewed as essential for societal security and stability, prompting site-specific defense measures and joint public–private innovation.[135] Heightened collaboration among leadership in essential services aims to strengthen risk-based approaches, including resilience against hybrid threats.

Switzerland underscores its neutral stance and strong educational and innovation capacity to bolster the security of indispensable goods and services.[136] Comprehensive risk analyses drive resilience improvements and encourage adherence to international standards, reinforcing consumer trust and spurring business success. Finally, the United Kingdom concentrates on fortifying its critical national infrastructure (CNI), partnering with operators to exceed baseline NIS Regulations.[137] A risk management framework, further reinforced by the National Security and Investment Act, seeks to enhance regulator capabilities, supply chain security, and operator skills. Alongside these measures, £2.6 billion over three years is allocated for cyber and legacy IT, supplemented by investments in defense, innovation, and skills development to promote a secure, growth-oriented digital environment.

Interpreting the Comparative Insights

This study set out to answer the research question:

How do different national cybersecurity strategies compare in their governance models, emphases on technology versus

policy, and alignment with international frameworks, and what implications might these divergences hold for understanding strategic coherence among small and mid-sized states? The following discussion outlines the answer.

The comparative analysis reveals a marked divergence in governance models. Countries such as the United Kingdom and the Netherlands exemplify comprehensive whole-of-society approaches, integrating cybersecurity into national security, economic, and foreign policy. These models reflect centralized coordination mechanisms and prioritize multi-sector engagement. In contrast, countries like Sweden and Switzerland adopt a more segmented or risk-management-based approach, emphasizing resilience through regulation and institutional alignment, but avoiding the full integration of offensive or proactive cyber doctrines. Historical administrative traditions, such as strong civil-military coordination or decentralization, appear to shape whether cybersecurity is approached as a societal obligation or a technical-administrative challenge.

> *Countries like Sweden and Switzerland adopt a more segmented or risk-management-based approach, emphasizing resilience through regulation and institutional alignment, but avoiding the full integration of offensive or proactive cyber doctrines.*

Another axis of differentiation lies in the balance between technology-driven and policy-centric strategies. States such as the United Kingdom, Finland, and the Netherlands leverage their industrial capacities to underpin robust technical infrastructures, often linking cyber resilience with innovation, research, and workforce development. Equally, several mid-sized and smaller states emphasize regulatory coherence, incident response, and legal adaptation over the direct deployment of advanced technologies. In these cases, strategic aims are pursued through public-private cooperation, legal compliance with supranational directives, and a risk-based framework that aligns national systems with broader regulatory ecosystems. This distinction underscores how industrial base and technological maturity shape strategic emphases.

> *The United Kingdom, the Netherlands, Finland, Belgium, and Denmark—acknowledge the existence or potential use of offensive cyberspace operations within national strategy documents.*

All of the reviewed NCSSs reveal varying degrees of alignment with supranational frameworks, including EU directives (particularly NIS and NIS2), NATO's evolving cyber agenda, and United Nations norms. Countries deeply embedded in transatlantic or European institutional frameworks demonstrate more rapid legal harmonization and capacity-building alignment. This is evident in the incorporation of European certification schemes, cross-border information sharing mechanisms, and coordinated incident response systems. However, there could be likely shift as a result of the new Trump administration and related policies. Additionally, not all alignments are equal. While NATO membership tends to accelerate integration of cyber defense language, five states explicitly include offensive cyberspace

capabilities in their strategies—highlighting a divergence in how far national strategies go in operationalizing alliance commitments.

The subset of countries that include offensive cyberspace capabilities in their NCSSs—namely the United Kingdom, the Netherlands, Finland, Belgium, and Denmark—acknowledge the existence or potential use of offensive cyberspace operations within national strategy documents. These strategies often frame offensive capabilities as a deterrence mechanism or as part of active cyber defense (e.g. Switzerland). Where included, offensive capabilities are positioned as essential for disrupting adversaries, attributing attacks, or projecting cyber power in support of national interests. The absence of such references in strategies from Sweden and Norway, despite their high levels of digitalization and international engagement, signals not just possible policy restraint but potentially unresolved political, legal, or normative debates on the legitimacy and utility of state-led cyberspace operations.

Across the board, cyber threats are defined in multi-dimensional terms encompassing cybercrime, espionage, sabotage, hybrid interference, and terrorism. While all states recognize the rising significance of state-sponsored operations and the blurring lines between criminal and geopolitical cyber activities, the specific threat prioritization varies. Countries situated closer to geopolitical flashpoints, or those with advanced digital economies, tend to exhibit heightened concern over strategic espionage and infrastructure sabotage. Others emphasize ransomware and economic extortion as core threats. These variances suggest that while threat actors are universally acknowledged, the framing of these actors is mediated by perceived vulnerabilities, historical experience, and alliance obligations.

Another key finding is the critical role of public-private partnerships, especially in countries where critical infrastructure is largely privately held. States such as Norway, Switzerland, the Netherlands, and the United Kingdom have institutionalized stakeholder collaboration, involving industry and academia in cyber strategy design and implementation. Information-sharing platforms, cyber innovation hubs, and dedicated advisory councils demonstrate that effective cyber resilience is not achievable without multilevel stakeholder commitment. This embedded cooperation, often described as stakeholder density, strengthens situational awareness, supports coordinated incident response, and fosters trust in digital ecosystems. Yet, this density also brings coordination challenges, particularly in federated or decentralized governance systems where overlapping mandates may hinder unified action.

Economic security considerations further emphasize the mutual relationship between economic resilience and digital security. Many countries, particularly the Netherlands, Finland, and Belgium, argue that digital trust and cybersecurity are prerequisites for national competitiveness. Investment in cybersecurity is thus framed not only as a protective measure but as a catalyst for economic innovation, productivity, and digital sovereignty. At the same time, high digitalization levels expand the threat surface, necessitating further investment and policy refinement. This feedback loop—where security enables economic growth, which in turn requires more cybersecurity—lies at the core of many NCSSs.

A further explanatory mechanism lies in institutional interdependence. Countries deeply embedded in multilateral arrangements often exhibit accelerated alignment with international norms, iterative policy adaptation, and a tendency to serve as norm entrepre-

neurs within global cyber governance fora. For example, the legal alignment with EU law and active contributions to NATO cyber dialogues are associated with higher standardization of cyber practices and legislation. However, institutional membership also exerts pressures for conformity that may not align with national preferences or capacities, particularly for mid-sized states managing competing internal demands. Consequently, institutional leverage both enables and constrains strategic agency.

The interplay between domestic governance models, technological capacity, international alignments, and threat perception reveals that there is no single blueprint for cybersecurity strategy. Instead, each national strategy reflects a negotiated outcome shaped by political priorities, resource availability, and external obligations. For small and mid-sized states, this results in a strategic balancing act: they must secure sufficient technical capacity, fulfill alliance commitments, and adapt to rapidly evolving threats—all while navigating internal political and economic constraints.

Technologically advanced states can afford to lead with innovation and deterrence, whereas others seem to prioritize governance, regulation, and partnership-building. Where strategies integrate offensive capabilities and multistakeholder engagement, strategic coherence appears stronger, particularly in the face of hybrid threats. In contrast, narrowly scoped strategies—focusing mainly on compliance or reactive measures—risk underperforming in complex threat environments.

Overall, the findings support theoretical perspectives that emphasize the role of multi-level governance, institutional diffusion, and securitization in national cyber policymaking. They also resonate with literature on cyber power, wherein states utilize a blend of military, diplomatic, technological, and normative instruments to shape their strategic posture. Moreover, the divergent approaches to offensive cyberspace capabilities reaffirm the analytical utility of distinguishing between sovereign cyber power and cooperative cyber governance models. The study thereby contributes to both comparative cyber strategy analysis and international relations theory by identifying patterns of adaptation, diffusion, and resistance in national approaches.

The analysis reveals that national strategies generally fall along a spectrum between technologically centered approaches and broader whole-of-society frameworks.

Key Takeaways and Future Directions

This study set out to answer the research question:

How do different national cybersecurity strategies compare in their governance models, emphases on technology versus policy, and alignment with international frameworks, and what implications might these divergences hold for understanding strategic coherence among small and mid-sized states?

The analysis reveals that national strategies generally fall along a spectrum between technologically centered approaches and broader whole-of-society frameworks. The former prioritize technical capacity-building—such as workforce development, cyber infrastructure, and risk-based frameworks—while the latter integrate cybersecurity within wider political, economic, and diplomatic ecosystems.

These orientations are not mutually exclusive, but reflect likely underlying variations in governance models, strategic cultures, and domestic institutional capacities.

International alignment, especially through mechanisms such as the EU's NIS2 directive and NATO's cyber agenda, fosters partial convergence in areas like incident response, regulatory structure, and cross-border cooperation. However, divergence persists in how states conceptualize threats, incorporate offensive capabilities, and institutionalize public-private cooperation. This divergence is particularly pronounced among small and mid-sized states, which must strike a balance between external compliance, domestic political feasibility, and operational resilience.

Strategic coherence, therefore, is not about achieving uniformity but managing trade-offs: between innovation and regulation, deterrence and diplomacy, national agency and institutional interdependence. Cybersecurity governance has evolved from a technical niche into a strategic domain embedded in broader questions of sovereignty, security, and statecraft. Therefore, it can be deduced that cybersecurity governance has advanced beyond purely technical concerns and now constitutes a strategic domain, intersecting with sovereignty, diplomacy, national security, and economic objectives.

Building on the example of the United Kingdom, an integrated approach—explicitly framed as a "National Cyber Strategy"—can more effectively address these interconnected policy areas.

Looking ahead, future studies can extend beyond the Euro-Atlantic sphere—especially into the Global South—to examine how differing institutional and geopolitical contexts shape cyber strategy. Longitudinal analysis could reveal how leadership shifts, technological advances, or security shocks reshape national approaches. Future work might also explore how offensive cyber capabilities are operationalized in practice and constrained by law, or how institutions implement global norms like NIS2 and NATO guidelines. Emerging technologies such as AI and quantum computing may challenge existing doctrines and require new legal frameworks. Such inquiries would enrich both policymaking and theory in an increasingly complex cyber governance environment.

Dr Gazmend Huskaj is the Head of Global Cyber and Security Policy at the Geneva Centre for Security Policy (GCSP), where he leads the Centre's work on developing global cyber policy.

Stefan Axelsson is Professor of Digital Forensics and Cybersecurity at the Department of Computer and Systems Sciences at Stockholm University.

Notes

1. Warren, Matthew and Leitch, Shona: "Australian cyber security policy through a European lens", *European Conference on Information Warfare and Security, ECCWS*, 2018, pp. 489-495; Luiijf, Eric; Besseling, Kim and De Graaf, Patrick: "Nineteen national cyber security strategies", *International Journal of Critical Infrastructures*, vol. 9, 2013, pp. 3-31, *https://doi.org/10.1504/IJCIS.2013.051608*.
2. Tatar, Ünal; Çalik, Orhan; Çelik, Minhac and Karabacak, Bilge: "A comparative analysis of the national cyber security strategies of leading nations", *9th International Conference on Cyber Warfare and Security, ICCWS*, 2014, pp. 209-216; Karazanishvili, Tamar: "Understanding US cyber security policies during the Donald J. Trump and Biden-Harris administrations" in *Cyber Security Policies and Strategies of the World's Leading States*, 2023, pp. 211-223, *https://doi.org/10.4018/978-1-6684-8846-1.ch013*.
3. Greiman, Virginia: "Cyber security and global governance", *European Conference on Information Warfare and Security, ECCWS*, 2015, pp. 71-78.
4. Byeon, Seo-hui and Suh, Woo-jong: "A study on the government's countermeasures against cyber attacks" in *Proceedings – 2020 IEEE International Conference on Big Data and Smart Computing, BigComp 2020*, 2020, pp. 495-499, *https://doi.org/10.1109/BigComp48618.2020.00-17*.
5. Sharikov, Pasha A.: "Evolution of American cyber security policies", *World Economy and International Relations*, vol. 63, no. 10 2019, pp. 51-58, *https://doi.org/10.20542/0131-2227-2019-63-10-51-58*.
6. Maglaras, Leandros; Drivas, George; Chouliaras, Nestoras; Boiten, Eerke; Lambrinoudakis, Costas and Ioannidis, Sotiris: "Cybersecurity in the Era of Digital Transformation: The case of Greece", *2020 International Conference on Internet of Things and Intelligent Applications, ITIA 2020*, 2020, *https://doi.org/10.1109/ITIA50152.2020.9312297*.
7. Luiijf, Besseling and De Graaf, "Nineteen national cyber security strategies".
8. Aborujilah, Abdulaziz; Al-Othmani, Abdulaleem Z.; Hussien, Nur Syahela; Mokhtar, Shamsul Anuar; Long, Zalizah Awang and Nizam, Mohd: "Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study", *2022 9th International Conference on Electrical and Electronics Engineering, ICEEE 2022*, 2022, pp. 440-450, *https://doi.org/10.1109/ICEEE55327.2022.9772546*.
9. Kasper, Agnes: "The fragmented securitization of cyber threats" in *Regulating eTechnologies in the European Union: Normative Realities and Trends*, 2014, pp. 157-188, *https://doi.org/10.1007/978-3-319-08117-5_9*.
10. George, Alexander L. and Bennett, Andrew: *Case Studies and Theory Development in the Social Sciences*, MIT Press, 2005.
11. Sharikov, "Evolution of American cyber security policies"; Ron, Mario; Ninahualpa, Geovanni; Molina, David and Díaz, Javier: "How to develop a national cybersecurity strategy for developing countries. Ecuador case", *Advances in Intelligent Systems and Computing*, 2020, pp. 553-563, *https://doi.org/10.1007/978-3-030-40690-5_53*.
12. Greiman, "Cyber security and global governance".
13. Montasari, Reza: "Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom" in *Advances in Information Security*, 2023, pp. 7-25, *https://doi.org/10.1007/978-3-031-21920-7_2*.
14. Karazanishvili, "Understanding US cyber security policies during the Donald J. Trump and Biden-Harris administrations"; Lehto, Martti: "The ways, means and ends in cyber security strategies", *European Conference on Information Warfare and Security, ECCWS*, 2013, pp. 182-190.
15. Tatar, Çalik, Çelik and Karabacak, "A comparative analysis of the national cyber security strategies of leading nations"; Kshetri, Nir: "Cyberwarfare in the Korean peninsula: Asymmetries and strategic responses", *East Asia*, vol. 31, no. 3 2014, pp. 183-201, *https://doi.org/10.1007/s12140-014-9215-1*.
16. Luiijf, Besseling and De Graaf, "Nineteen national cyber security strategies".

17. Warren and Leitch, "Australian cyber security policy through a European lens".
18. Karazanishvili, "Understanding US cyber security policies during the Donald J. Trump and Biden-Harris administrations".
19. Sharikov, "Evolution of American cyber security policies".
20. Tatar, Çalik, Çelik and Karabacak, "A comparative analysis of the national cyber security strategies of leading nations".
21. Luiijf, Besseling and De Graaf, "Nineteen national cyber security strategies".
22. Çifci, Hasan: "Analysis of Türkiye's cybersecurity strategies: Historical developments, scope, content and objectives", *Sakarya University Journal of Science*, vol. 28, no. 1 2024, pp. 204-219, *https://doi.org/10.16984/saufenbilder.1249760*.
23. Ron, Ninahualpa, Molina and Díaz, "How to develop a national cybersecurity strategy for developing countries. Ecuador case".
24. Byeon and Suh, "A study on the government's countermeasures against cyber attacks".
25. Maglaras, Drivas, Chouliaras, Boiten, Lambrinoudakis and Ioannidis, "Cybersecurity in the Era of Digital Transformation: The case of Greece".
26. Greiman, "Cyber security and global governance".
27. Ovchinnikova, Oksana and Upadhyay, Niteesh Kumar: "The level of cybersecurity of the BRICS member countries in international ratings: Prospects for cooperation", *BRICS Law Journal*, vol. 10, no. 1 2023, pp. 7-34, *https://doi.org/10.21684/2412-2343-2023-10-1-7-34*.
28. Reveron, Derek S.: *Cyberspace and national security: Threats, opportunities, and power in a virtual world*, Georgetown University Press, 2012, pp. 3-19.
29. Kshetri, "Cyberwarfare in the Korean peninsula: Asymmetries and strategic responses".
30. Lehto, "The ways, means and ends in cyber security strategies".
31. Guitton, Clement: "Cyber insecurity as a national threat: Overreaction from Germany, France and the UK?", *European Security*, vol. 22, no. 1 2013, pp. 21-35, *https://doi.org/10.1080/09662839.2012.749864*.
32. Kasper, "The fragmented securitization of cyber threats".
33. Canbek, Gürol and Sagiroglu, Seref: "Strategic cyber-security perspective in smart grids", *6th International Symposium on Digital Forensic and Security, ISDFS 2018*, 2018, pp. 1-6, *https://doi.org/10.1109/ISDFS.2018.8355346*.
34. Russell, Alison Lawlor: "Strategic anti-access/area denial in cyberspace", *7th International Conference on Cyber Conflict, CYCON*, 2015, pp. 153-168, *https://doi.org/10.1109/CYCON.2015.7158475*.
35. Kolini, Farzan and Janczewski, Lech: "Clustering and topic modelling: A new approach for analysis of national cybersecurity strategies", *PACIS 2017: Societal Transformation Through IS/IT*, 2017.
36. Zheng, An-ka; Song, Ping; Han, Bing-xia and Zheng, Min-jiao: "Reflection of the nation cybersecurity's evolution", *Applied Mechanics and Materials*, 2013, pp. 2553-2558, *https://doi.org/10.4028/www.scientific.net/AMM.347-350.2553*.
37. UK Cabinet Office: *National Cyber Strategy 2022*, 2022, *https://www.gov.uk/government/publications/national-cyber-strategy-2022*.
38. Huskaj, Gazmend: *Offensive Cyberspace Operations: Implications for Sweden*, doctoral dissertation, Stockholm University, 2024, *https://su.diva-portal.org/smash/record.jsf?pid=diva2%3A1871270*.
39. Ibid.
40. Council on Foreign Relations (CFR): *Cyber Operations Tracker*, *https://www.cfr.org/cyber-operations/*.
41. Schmitt, Michael N. (ed.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017, *https://doi.org/10.1017/9781316822524*.
42. Limnéll, Jarno and Lehto, Martti: "The importance of strategic leadership in cyber security: Case of Finland", *Proceedings of the European Conference on Information Warfare and Security (ECCWS)*, 2019, pp. 288-296.
43. Montasari, "Cyber Threats and the Security Risks They Pose to National Security: An Assessment of Cybersecurity Policy in the United Kingdom".
44. Hossain, Zakir; Zaman, Golam Kibria and Taher, Kazi Abu: "Cyber Emergency Response Team for Bangladesh", *2021 International Conference on ICT for Sustainable Development*,

2021, pp. 477-480, *https://doi.org/10.1109/ICICT4SD50815.2021.9396922*.
45. Kim, Yu-Kyung; Go, Myong-Hyun; Kim, Sonyong; Lee, Jaeyeon and Lee, Kyungho: "Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis", *Journal of Internet Technology*, vol. 24, no. 2 2023, pp. 495-505, *https://doi.org/10.53106/160792642023032402031*.
46. Semenchenko, Andrii; Pleskach, Valentyna; Zaiarnyib, O. and Pleskach, Mariia: "Cyber security and cyber protection: The current state of public administration in Ukraine", *CEUR Workshop Proceedings*, vol. 2866, 2020, pp. 276-284.
47. Onyshchenko, Svitlana; Yanko, Alina; Hlushko, Alina and Maslii, Oleksandra: "Economic cyber security of business in Ukraine: Strategic directions and implementation mechanism", *Economic and Cyber Security*, 2023, pp. 30-58, *https://doi.org/10.15587/978-617-7319-98-5.CH2*.
48. Peter, Ada and Sobowale, Idowu: "The future of economic and political conflicts in Africa: Is the continent ready?", *25th IBIMA Conference Proceedings*, 2015, pp. 73-86.
49. Backman, Sarah: "Risk vs. threat-based cybersecurity: The case of the EU", *European Security*, vol. 32, no. 1 2023, pp. 85-103, *https://doi.org/10.1080/09662839.2022.2069464*.
50. Wright, Marc; Chizari, Hassan and Viana, Thiago: "Analytical Framework for National Cyber-security and Corresponding Critical Infrastructure: A Pragmatistic Approach", *2020 International Conference on Computational Science and Intelligence*, 2020, pp. 127-130, *https://doi.org/10.1109/CSCI51800.2020.00029*.
51. Lampe, Benjamin: "On the Application of Cyber-Informed Engineering (CIE)", *6th International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, TPS-ISA 2024*, pp. 537-542, *https://doi.org/10.1109/TPS-ISA62245.2024.00073*.
52. AlDaajeh, Saleh and Alrabaee, Saed: "Strategic cybersecurity", *Computers and Security*, vol. 141, 2024, art. 103845, *https://doi.org/10.1016/j.cose.2024.103845*.
53. Jing, Bo-jiun: "Cybersecurity is national security: Can Taiwan have the digital cake and eat it too?", *Chinese (Taiwan) Yearbook of International Law and Affairs*, vol. 38, 2020, pp. 120-137, *https://doi.org/10.1163/9789004501638_006*.
54. Aborujilah et al., "Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study".
55. Izycki, Eduardo and Colli, Rodrigo: "Protection of critical infrastructure in national cyber security strategies", *European Conference on Information Warfare and Security, ECCWS*, 2019, pp. 219-228.
56. Teoh, Chooi Shi and Mahmood, Ahmad Kamil: "National cyber security strategies for digital economy", *ICRIIS 2017*, 2017, *https://doi.org/10.1109/ICRIIS.2017.8002519*.
57. Williams, Matthew and Levi, Michael: "Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors", *Security Journal*, vol. 28, no. 3 2015, pp. 252-271, *https://doi.org/10.1057/sj.2012.47*.
58. Ovchinnikova and Upadhyay, "The level of cybersecurity of the BRICS member countries in international ratings: Prospects for cooperation".
59. Semenenko, Oleh; Dobrovolskyi, Uzef; Sliusarenko, Maryna; Levchenko, Ihor and Mytchenko, Serhii: "Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience", *Social and Legal Studios*, vol. 6, no. 4 2023, pp. 192-199, *https://doi.org/10.32518/sals4.2023.192*.
60. Hashem, Sherif: "Establishing a national CERT/CISRT in Egypt", *WMSCI 2019 – 23rd World Multi-Conference on Systemics, Cybernetics and Informatics*, vol. 2, 2019, pp. 38-43.
61. Greiman, "Cyber security and global governance".
62. Mori, Shigeo and Goto, Atsuhiro: "Reviewing national cybersecurity strategies", *Journal of Disaster Research*, vol. 13, no. 5 2018, pp. 957-966, *https://doi.org/10.20965/jdr.2018.p0957*.
63. Iova, Radu Antonio Serrano and Watashiba, Tomoe: "NCSS: A global census of national positions on conflict, neutrality and cooperation", *European Conference on Information Warfare and Security, ECCWS*, 2023, pp. 420-428.
64. Maglaras et al., "Cybersecurity in the Era of Digital Transformation: The case of Greece".
65. Canbek and Sagiroglu, "Strategic cyber-security perspective in smart grids".

66. Lampe, "On the Application of Cyber-Informed Engineering (CIE)".
67. Olifirov, Alexander; Makoveichuk, Krystina A. and Petrenko, Sergei: "Cybersecurity measures of the digital payment ecosystem", *CEUR Workshop Proceedings*, vol. 3035, 2021, pp. 133-142.
68. Jing, "Cybersecurity is national security: Can Taiwan have the digital cake and eat it too?".
69. Kasper, "The fragmented securitization of cyber threats".
70. Izycki and Colli, "Protection of critical infrastructure in national cyber security strategies".
71. Kolini and Janczewski, "Clustering and topic modelling: A new approach for analysis of national cybersecurity strategies".
72. Aborujilah et al., "Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study".
73. Kademi, Anas Muazu: "Strengthening strategic approach to counter cyberspace threats in Nigeria", *13th International Conference on Cyber Warfare and Security, ICCWS 2018*, 2018, pp. 328-337.
74. Czosseck, Christian; Ottis, Rain and Talihärm, Anna-Maria: "Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security", *10th European Conference on Information Warfare and Security, ECIW 2011*, 2011, pp. 57-64.
75. Von Solms, Rossouw and Von Solms, Basie: "National cyber security in South Africa: A letter to the minister of cyber security", *10th International Conference on Cyber Warfare and Security, ICCWS 2015*, 2015, pp. 369-374.
76. Mortenson, Michael J. and Vidgen, Richard: "A computational literature review of the technology acceptance model", *International Journal of Information Management*, vol. 36, no. 6 2016, pp. 1248-1259, *https://doi.org/10.1016/j.ijinfomgt.2016.07.007*.
77. Blei, David M.; Ng, Aandrew Y. and Jordan, Michael I.: "Latent Dirichlet Allocation", *Journal of Machine Learning Research*, vol. 3 (Jan.), 2003, pp. 993-1022.
78. Braun, Virginia and Clarke, Victoria: "Using thematic analysis in psychology", *Qualitative Research in Psychology*, vol. 3, no. 2 2006, pp. 77-101, *https://doi.org/10.1191/1478088706qp063oa*.
79. George and Bennett, *Case Studies and Theory Development in the Social Sciences*.
80. Nature Editorial: "Tools such as ChatGPT threaten transparent science; here are our ground rules for their use", *Nature*, 2023, *https://www.nature.com/articles/d41586-023-00191-1*.
81. Centre for Cyber Security Belgium: *Cybersecurity strategy for Belgium 2.0 (2021–2025)*, 2021, *https://ccb.belgium.be/en/cybersecurity-strategy-belgium-20*.
82. Centre for Cyber Security: *Cyber and information security strategy 2022–2024*, Danish Ministry of Defence, 2022, *https://www.cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf*.
83. Finnish Prime Minister's Office: *Finland's Cyber Security Strategy 2024–2035*, 2024, *https://julkaisut.valtioneuvosto.fi/handle/10024/165893*.
84. Dutch Government: *The Netherlands Cybersecurity Strategy 2022–2028*, National Coordinator for Security and Counterterrorism (NCTV), 2022, *https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028*.
85. Norwegian Government: *National Cyber Security Strategy for Norway*, Ministry of Justice and Public Security, 2019, *https://www.regjeringen.no/en/dokumenter/national-cyber-security-strategy-for-norway/id2627177/*.
86. Swedish Cabinet Office: *National Cybersecurity Strategy 2025–2029*, 2025, *https://regeringen.se/rattsliga-dokument/skrivelse/2025/03/skr.-202425121*.
87. Swiss National Cybersecurity Centre: *National Cyberstrategy (NCS)*, 2023, *https://www.ncsc.admin.ch/ncsc/en/home/strategie/cyberstrategie-ncs.html*.
88. UK Cabinet Office: *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*, 2022, *https://www.gov.uk/government/publications/national-cyber-strategy-2022*.
89. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
90. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
91. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
92. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*.
93. Norwegian Government, *National Cyber Security Strategy for Norway*.

94. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
95. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
96. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.
97. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
98. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
99. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
100. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*.
101. Norwegian Government, *National Cyber Security Strategy for Norway*.
102. Ibid.
103. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
104. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
105. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.
106. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
107. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
108. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
109. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*.
110. Norwegian Government, *National Cyber Security Strategy for Norway*.
111. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
112. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
113. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.
114. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
115. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
116. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
117. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*
118. Norwegian Government, *National Cyber Security Strategy for Norway*.
119. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
120. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
121. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.
122. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
123. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
124. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
125. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*.
126. Norwegian Government, *National Cyber Security Strategy for Norway*.
127. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
128. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
129. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.
130. Centre for Cyber Security Belgium, *Cybersecurity strategy for Belgium 2.0 (2021–2025)*.
131. Centre for Cyber Security, *Cyber and information security strategy 2022–2024*.
132. Finnish Prime Minister's Office, *Finland's Cyber Security Strategy 2024–2035*.
133. Dutch Government, *The Netherlands Cybersecurity Strategy 2022–2028*.
134. Norwegian Government, *National Cyber Security Strategy for Norway*.
135. Swedish Cabinet Office, *National Cybersecurity Strategy 2025–2029*.
136. Swiss National Cybersecurity Centre, *National Cyberstrategy (NCS)*.
137. UK Cabinet Office, *National Cyber Strategy 2022 – Pioneering a cyber future with the whole of the UK*.