GOVERNANCE OF SECURITY IN DIGITAL EUROPE: LESSONS FROM CROATIA'S CYBERSECURITY ARCHITECTURE

DOI: https://doi.org/10.37458/nstf.26.2.9
Review paper
Received: October 28, 2025
Accepted: November 26, 2025

Celien De Stercke*

Abstract: Traditional conceptions of crime are challenged in the digital age: cyberspace has blurred the historical divide between civilian and military responsibility, creating a new landscape that demands unprecedented levels of communication and cooperation. To provide a grounded understanding of how the digital realm influences contemporary governance structures; real-world dynamics that define cybersecurity efforts need to be captured. Croatia provides a

* Celien De Stercke is a Criminologist at the Institute for International Research on Criminal Policy (IRCP) (Ghent University, Belgium). She pursues a PhD on the intersection of organized cybercrime and national security, analyzing how national security frameworks are designed to address these ambiguous cyber threats. Drawing on her work in Belgium and Croatia, she ultimately assesses how the hybrid cyber dimension impacts the way we provide security today. *Celien.DeStercke@UGent.be*

compelling European lens to examine the international power dynamics shaping cyberspace. Its resilience-focused strategy reflects an acute awareness of regional geopolitical dynamics, particularly in light of growing Russian cyber activities. The country's efforts underscore how smaller nations navigate the tension between national sovereignty and the need for transnational cooperation in a domain without borders. Hence, this article charts Croatia's cybersecurity architecture using qualitative methods to uncover the main frameworks, key actors, and critical collaborations that that define its approach. By leveraging the Croatian case study, this research contributes empirically to the broader discourse on the governance of security in cyberspace. It addresses the pressing challenges confronting European security frameworks as they adapt to the evolving realities of policing cyberspace, offering valuable insights into the intersection of criminology, technology, and governance.

Keywords: Croatia, cyberspace, digital policing, governance of security, security architecture

Introduction

"In today's interconnected world, cyberspace has emerged as a critical arena where state and non-state actors interact, compete, and confront one another (Stoddart, 2022). The hybrid nature of this domain blurs the lines between civil and military, private and public, as digital systems underpin nearly every aspect of modern life (Missiroli, 2021). Whether it is critical infrastructure, economic stability, or national defense, the cyber domain transcends traditional boundaries and opens new avenues for both cooperation and conflict. This hybrid space is not only a theatre for

> *cybercriminals but also a battlefield for state-sponsored operations, espionage, and even potential for warfare (De Stercke et al., 2024). The increased anonymity and borderless nature of cyber activities allow adversaries to exploit weaknesses, making states vulnerable to an array of threats that range from cybercrime to cyber-enabled espionage (De Stercke et al., 2024; Missiroli, 2021).”*
>
> (De Stercke & Janssens, 2025, p. 2)

Building on this perspective, the evolving digital domain challenges traditional notions of security and governance. As cyber threats evolve, it is particularly interesting to observe the new partnerships and governance structures that have emerged to address these challenges within a rapidly changing digital environment (Bures & Carrapico, 2018; Raymond, 2016). This situation highlights a significant gap in empirical knowledge regarding how states organize and coordinate these efforts, particularly in contexts where cybercrime intersects with national security (see for example de Arimatéia da Cruz & Pedron, 2020; Smeets, 2025). To gain a grounded understanding of how the digital realm influences the governance of security, it is necessary to capture the real-world mechanisms, interactions, and tensions that define national cybersecurity efforts.

Croatia provides a compelling lens through which to explore these dynamics. As a newer member of the European Union (EU),[1] the country’s cybersecurity posture reflects the lasting imprint of the Homeland War

[1] Croatia is a member of European Union since the 1st of July, 2013.

on national consciousness (Polic, 2021) and the geopolitical realities of its position as a EU's external frontier (European Council on Refugees and Exiles, 2024; European Parliament, 2024; Pusić, 2022). Its size, historical experience, and strategic location create a governance environment particularly sensitive to the tension between national sovereignty and the need for transnational cooperation in a borderless digital domain (Baldoni & Di Luna, 2025). These objective factors make Croatia a valuable case for understanding how smaller European states organize and adapt their responses to evolving cyber threats.

As part of a larger doctoral research project, the Croatian case study complements insights derived from Belgium (De Stercke & Janssens, 2025), offering a comparative perspective on how smaller European states govern cyber threats. By capturing the empirical dynamics that define cybersecurity efforts, these case studies provide a grounded understanding of how the digital realm influences traditional governance structures.

This article focuses on charting Croatia's cybersecurity architecture, with particular attention to cyber threats that may impact national security. Using qualitative methods, it examines the main frameworks, key actors, and critical collaborations that shape the country's approach. The analysis draws on fieldwork conducted in Zagreb, including interviews across the national cybersecurity ecosystem, and is complemented by a review of open-source literature. In doing so, the study provides a comprehensive, comparative understanding of how Croatia's cybersecurity architecture functions in practice and highlights how its strategies can inform

broader European efforts to govern security in cyberspace.

Methodology

The article adopts a grounded qualitative approach (see Charmaz 2006, 2024) to examine Croatia's governance of cyberspace, with a particular focus on cyber threats that may affect national security. Employing a multifaceted research design, the study draws on a series of expert interviews and supplements them where possible with insights from open literature. Given the interdisciplinary character of cybersecurity and the prominent role of private actors in the field (Button, 2020; Maurer, 2018; Stevens, 2017), the value of a multistakeholder sample is emphasized.

The groundwork for this study was established during three preparatory visits and one extended fieldwork stay, as presented in Table 1. During this period, the non-native researcher became acquainted with Croatia's cybersecurity community through networking events and snowball sampling. Local academic support was also in place: Prof. dr. Gordan Akrap from the Dr. Franjo Tuđman Defence and Security University, a renowned security expert, provided scholarly grounding, local credibility, and access to an extensive professional network that included Dr. Natalija Parlov Una. As a subject-matter specialist, Dr. Natalija Parlov Una notably strengthened the research by opening doors to high-level contacts and facilitating key interviews, complementing the researcher's own independent efforts.

Table 1. Croatian Case Study - Fieldwork Design

Period	Central Opportunity	Fieldwork
19-21st February 2025	CARNET event - ConCERT	prepatory
3-11th April 2025	2025 Defense and Security Conference - Dr. Franjo Tuđman Defense and Security University	prepatory
26-29th May 2025	NKS event - Druga nacionalna konferencija NKS: Kibernetička sigurnost: novi izazovi – nove prilike	prepatory
8 September – 8 December 2025	Zagreb Security Forum 2025	long stay

This resulted in 17 interviews as seen in Table 2, encompassing a diverse range of actors involved in Croatia's cybersecurity landscape. Participants included representatives from central government agencies, academics specializing in cyber issues (including social and technical backgrounds), critical infrastructure operators, law enforcement, the national CSIRT, as well as private cybersecurity professionals such as consultants and major cybersecurity firms. Through a combination of these perspectives, this article provides an exploratory analysis of the national state of the art in governing cyber threats from a Croatian perspective.

Table 2. Interview list

Nr.	Date	Interviewee background	Personal information
1	21 February 2025	Law Enforcement Cybersecurity expert (technical) Academic	Dr. Nikola Protrka (list)
2	4 April 2025	Academic (Professor) Military	Prof. Dr. Gordan Akrap
		Private sector - Consultancy Cybersecurity expert Academic	Dr. Natalija Parlov Una
3	9 April 2025	Academic (Professor) Cybersecurity expert (social)	Prof. Dr. Tihomir Katulić (list)
4	9 April 2025	Academic (Professor) Cybersecurity expert (technical)	Prof. Dr. Roman Domović (list)
5	27 May 2025	Private sector - Telecommunications Cybersecurity expert (social)	Martina Dragičević *A1*
6	27 May 2025	Public sector Cybersecurity expert (social)	Member of the European Cybersecurity Certification Group 2022-24 (list)
7	28 May 2025	Public sector Cybersecurity expert (social)	anon
8	5 September 2025	Private sector - Cybersecurity Cybersecurity expert (technical)	Dragan Topalović *Span*
		Private sector - Cybersecurity Cybersecurity expert (social)	Vedran Benić *Span*
9	9 September 2025	*National CSIRT*[1] Cybersecurity expert	Nataša Glavor (Former head of *NCERT.hr*)
10	12 September 2025	*National CSIRT*[1] Cybersecurity expert	*NCERT.hr*
11	19 September 2025	Private sector - Consultancy Cybersecurity expert	Chief Information Security Officer *Končar - Digital*

12	19 September 2025	Public sector – Critical Infrastructure Cybersecurity expert (technical)	Željko Sičaja *HŽ Infrastruktura*
13	29 September 2025	Academic Cybersecurity expert (technical)	Zlatan Morić *Algebra Bernays University*
14	7 October 2025	Private sector - Telecommunications Cybersecurity expert (technical)	anon
15	10 October 2025	Private sector Cybersecurity expert (technical)	*AKD d.o.o.*
16	11 October 2025	*National CSIRT*[2]	*Croatian National Cyber Security Centre (NCSC)* (list)
17	31 October 2025	Public Sector - Diplomacy	*anon*

Procedure

Potential interviewees were approached during an event and/or contacted via email or contacted through WhatsApp (references only) and invited to participate in the study. In cases of non-response, a follow-up email or message was sent within a reasonable time frame dependent on the acquaintance. The participants were provided with an information document, an invitation letter, and the informed consent form outlining the study's purpose and procedures. Furthermore, permission to record the interview was sought as well, which was reaffirmed before the start of each interview. Interviews were done through various mediums including in-person meetings or online video

[2] National Cyber Security Incident Response Team (CSIRT). The NCERT.hr is one of the two designated National CSIRTs within the Definition of the NIS legislation, next to the Croatian National Cyber Security Centre (NCSC) (CERT.hr, 2025; NCSC-HR, 2025).

technology. The semi-structured format allowed for flexibility in questioning, enabling the exploration of emergent themes and the validation of preliminary findings. A topic list was developed to guide the discussion, though each interview was customized to fit the expertise and experiences of the participant.

The interviews delved into various aspects, all discussing (1) Croatia's security architecture for countering cyber threats, with a focus on frameworks, key partners, core collaborations, and illustrative examples; (2) modus operandi of serious cybercrimes affecting national security in Croatia; and (3) any indications of cyber mercenary use (proxy deployment by States).[3] By default, interviewees were handled anonymously; however, the informed consent file provided a clear opt-out option for experts who permitted direct attribution of their insights. Interviews took approximately one hour and one and a half hours; 12 were conducted in person, and more than half of the interviewees gave permission to record.

Given the varying levels of confidentiality among participants based on their formal consent - ranging from fully anonymous to fully non-anonymous, or non-anonymous but listed only by name - individual identifiers are treated accordingly. Insights derived from fully anonymous or fully non-anonymous participants are referenced using interview numbers (e.g., Interview 18). However, when a statement or insight is supported by one or more participants, and at least one of them

[3] They can be defined "as intermediate actors with cyber-offensive capabilities that unlawfully peddle hacked intelligence, software or technical expertise to a beneficiary in exchange for financial or ideological gain. Beneficiaries range from nation-states to multinational corporations and wealthy individuals that gain advantage from the activities of these cyber mercenaries" (de Arimateia da Cruz & Pedron, 2020, p. 3).

consented to be referenced only by name in the participant list, the generic format (Interview X) is used to maintain consistency and prevent potential de-identification.

Limitations

Qualitative research inherently has its limitations, as the process depends on the selection of interviewees and the perspective of the researcher conducting and analyzing the data (Charmaz, 2024; Patton, 2014). Moreover, because the researcher is not a native of Croatia, language barriers and cultural differences are inevitable (Berger, 2015). Support from local actors was intended to mitigate these influences, particularly given the unique national context under study. Nevertheless, the outsider perspective was positively received by interviewees, who appreciated the perceived objectivity it could bring. Additionally, the research focuses on a high-level (security) population that is not easily accessible; consequently, some actors may have declined participation despite all efforts to include them. Nonetheless, the sample is broadly representative of the key institutions and actors shaping Croatia's cybersecurity governance,[4] allowing a useful overview of the national system to be constructed below.

Today's Croatian Cybersecurity Ecosystem: Fragmented Hierarchies and Soft-Power Glue

The Croatian cybersecurity ecosystem functions as an operational tandem between the National Cybersecurity

[4] Confirmed by the author's empirical interview data; individual identifiers withheld for confidentiality.

Centre of Croatia (NCSC-HR) and the National Computer Emergency Response Team (NCERT), representing the intelligence and scientific communities, respectively (Cybersecurity Act, 2024; Interview X). These bodies operate in parallel to the law enforcement system, with digital evidence handling and the criminal justice process treated as a separate domain.[5] Complementary institutions include the Office of the National Security Council (UVNS), which plays a strategic role in developing national policy and cybersecurity strategy, the State Information Security Bureau (ZSIS), responsible for cybersecurity certification, and the National Coordination Center for Industry, Technology and Research in the Field of Cybersecurity (NKS-HR) (Interview X).[6] Sectoral authorities also play a supplementary role in overseeing cybersecurity in specific critical sectors (Interview X). The private sector is actively engaged within the ecosystem; however, public-private partnerships are fragmented and not always formally recognized (Interview X). Overall, the system is characterized by informal ties (Interview X),[7] which help maintain functional connections across organizational boundaries. A summarizing overview of the key actors can be found in Figure 1.

[5] Based on the author's empirical observations.

[6] While Croatia also has an Agency for the Protection of Personal Data (AZOP) (AZOP, 2025; Interview X), it was only marginally discussed in interviews and is therefore not examined in detail here.

[7] Croatia has a relatively small cybersecurity community whose members interact frequently, fostering an 'everybody knows everybody' culture (Interview X). Moreover, it is not rare for private-sector employees to have former backgrounds in public (security) institutions (Interviews 9, 11, 12 for example), contributing to interorganizational connections through informal ties. In practice, actors often contact one another directly before resorting to formal (incident) procedures (Interview X).

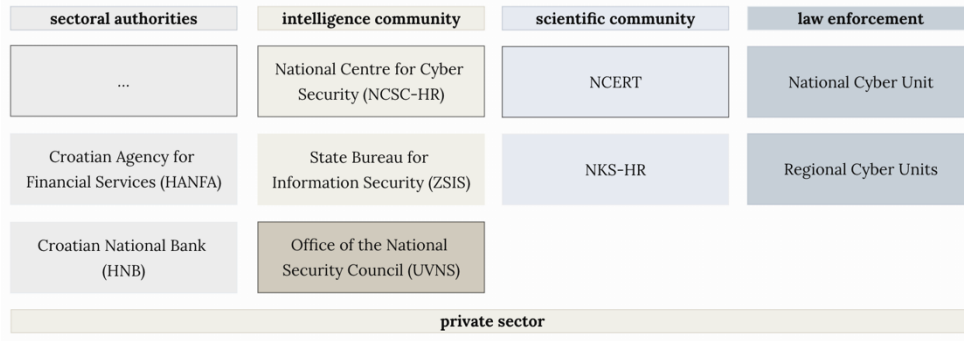

Figure 1: Today's Croatian Cybersecurity Ecosystem - Fragmented Hierarchies and Soft-Power Glue

The ecosystem will be presented across four key domains: intelligence, science, law enforcement, and the private sector, highlighting the roles and interactions of both public and private actors.

Intelligence

A central role is played by the intelligence community, as the National Cybersecurity Centre (NCSC-HR) is hosted by the Security and Intelligence Agency (SOA), parallel to the State Information Security Bureau (ZSIS). With the national transposition of the European Network and Information Systems (NIS) 2 Directive (2022) in 2024 (Cybersecurity Act, 2024), NCSC-HR was designated as a main competent CSIRT, responsible for ten of the fifteen regulated sectors (Interview X). It also operates the sk@ut system, a defensive SOC platform accessible to a range of national entities (Interview X; NCSC-HR, 2025).

ZSIS, by contrast, has transitioned into a specialized role, acting as Croatia's designated certification

authority (NCCA) under the EU Cybersecurity Certification framework (Interview X; *"Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act),"* 2019). This marks a narrowing of its earlier, more central position in the national cybersecurity ecosystem (see infra).

Science

The Croatian Academic and Research Network (CARNET) originated as a provider of internet access for universities, schools, and research institutions, but has since evolved into a key hub for national cyber expertise (Interview 9). It hosts the National CERT (NCERT), which has evolved from technically supporting the academic and research sector, into carrying out CSIRT functions for the public under the NIS I (2016) framework (then named CERT.hr). Its current mandate as a formalized national CSIRT under NIS II is confined to five regulated domains of public interest: banking, financial market infrastructure, digital infrastructure limited to national domain names, research and education (Interview 9; CERT.hr, 2025; Cybersecurity Act, 2024).

In parallel, CARNET also houses the National Cybersecurity Competence Centre (NCC-HR, NKS-HR), established under the EU Cybersecurity Competence Centre and Network Regulation (2021). Unlike NCERT, NKS-HR is not an operational CSIRT but focuses on cyber resilience, research, capacity

building, training, and awareness at the national level (Interview 9).

Law Enforcement

The Ministry of Interior (MUP) anchors Croatia's law enforcement response to cyber threats. At the National level, a cybercrime unit functions as acts as the Single Point of Contact (SPOC) for international cooperation, including with Europol's European Cybercrime Centre (EC3) and INTERPOL (Interview X; MUP, 2025a, 2025b). In parallel, regional cybercrime departments operate across Croatia's 20 police administrations, providing on-the-ground investigative capacity (Interview X). Cybercrime investigations in Croatia are primarily situated within the Criminal Police Units, where strategic police officers lead the investigative process (Interview X; MUP 2025b). These officers manage the case, develop investigative lines, and integrate cybercrime into broader criminal investigations (Interview X). Technical specialists play a supportive role, providing digital forensics and technological assistance on demand, ensuring that strategic decisions are backed by technical expertise (Interview X).

While the hierarchical police structure strengthens operational reach, horizontal links between law enforcement and the wider cybersecurity ecosystem tend to be pragmatic and case-driven rather than systematically institutionalized.[8]

[8] Based on the author's empirical observations.

Private sector involvement

The private sector in Croatia participates in the national cybersecurity ecosystem in a highly eclectic manner. Some private actors are actively engaged in exercises and partnerships, while others are less involved, reflecting the government's reserved approach rather than a lack of willingness from the private sector.[9] Collaborations are often driven by practical necessity, such as when private entities manage government IT systems or perform other operationally relevant functions (Interview 8, 14). Certain private actors also take part in supranational exercises, such as NATO tabletop simulations, highlighting informal, pragmatic, and varied ties between public and private actors (Interview X). Public-private interactions are rarely formally acknowledged and often occur through ad hoc or loosely structured channels (Interview X; See also footnote 8 on informal ties). Despite this variability, private actors remain an important component of national cybersecurity resilience, contributing expertise, operational capacity, and sector-specific knowledge to support policy implementation and incident response.

The interviews have indicated that the domains and entities have limited insight into each other's internal workings, highlighting a siloed institutional architecture.[10] Yet, informal ties exist,[11] and while daily

[9] The ultimate position of the government can be exemplified by the working group on the national transposition of NIS 2 coordinated by the Ministry of Justice and Public Administration (MPU). A selected set of industry stakeholders have been consulted on the drafting of the implementation, whereas others were sought to give comments on the legislative draft. However, the government retained ultimate authority over the legislative framework, as certain decisions were politically determined. (Interview 5, 7, 13, 15)

[10] Based on the author's empirical observations.

[11] See footnote 6 on informal ties.

interactions are generally unofficial rather than formally recognized (Interview X), they are nevertheless professional, creating a form of "soft-power glue" that helps maintain functional links across the system. Given that Croatia is a relatively small country, the cybersecurity sector is likewise compact, and many actors are personally acquainted reinforcing these informal networks (Interview X; See also footnote 6 on informal ties).

In sum, the Croatian cybersecurity ecosystem is characterized by fragmented hierarchies, in which multiple top-down actors pursue distinct institutional goals, while informal networks of influence and soft-power linkages function as the glue that holds the system together under the ultimate authority of the government.

From NIS I to NIS II: Historical Shifts in Cybersecurity Competencies in Croatia

Croatia's approach to cyber governance has evolved through a series of incremental yet consequential shifts in its legal and institutional architecture over the years (Interview X; Katulić & Lisicar, 2024). The Information Systems Security Act of 2007 established an initial framework for information security, influenced by early data protection legislation, and laid a robust legal foundation that enabled the national implementation of the first NIS Directive (2016) in 2018 (Interview X; Katulić & Lisicar, 2024). Nevertheless, academic sources note that these early structures were often underutilized in practice (Katulić & Lisicar, 2024). A more decisive transformation occurred in 2024 with the transposition of NIS II (2022), which reallocated

institutional competences across national cybersecurity actors (Interview X). The result is a decentralized cybersecurity system, embedded within the country's intelligence community, reflecting an organic and ongoing evolution of Croatia's cyber governance model.

2007 - Information Systems Security Act

With the adoption of the Information Systems Security Act in 2007, Croatia established the foundations of its national cybersecurity framework. Building on earlier data protection legislation, the Act formalized pre-existing structures and clarified institutional responsibilities for the protection of public authorities (Interview X; Katulić & Lisicar, 2024). Within the Croatian Academic and Research Network (CARNET), CERT.hr was designated as the national contact point for the academic and research community, tasked with incident response, monitoring, and awareness-raising activities (Interview X; Katulić & Lisicar, 2024). In parallel, the State Information Security Bureau (ZSIS), hosted govCERT, which was responsible for the protection of governmental and classified information systems, including those forming part of critical national infrastructure (Interview X; Katulić & Lisicar, 2024). Oversight and strategic coordination functions were vested in the Office of the National Security Council (UVNS), which subsequently assumed the leading role in the formulation of national cyber policy and, in 2015, oversaw the development of Croatia's first National Cybersecurity Strategy (Interview X; The National Cyber Security Strategy of the Republic of Croatia, 2015). Through this division of roles, the Act institutionalized a functional allocation of responsibilities: CERT.hr focusing on the research and

education sector, ZHIS/govCERT safeguarding government and critical infrastructure, and UVNS providing overarching coordination and policy guidance.

2018 – Cyber Security Act (NIS I)

The adoption of the Cybersecurity Act in 2018 marked Croatia's transposition of the EU's NIS I Directive (2016) and the beginning of a more consolidated national approach to cyber governance. The Act formally designated the State Bureau for Information Security (ZSIS) as the national main CSIRT, giving it a clear legal mandate under EU law for incident handling and coordination across critical sectors.[12] This step clarified earlier overlaps between CERT.hr and govCERT by anchoring ZSIS as the state's primary authority for cybersecurity incident response, while maintaining CARNET's CERT.hr as a sectoral CSIRT with a broad mandate covering multiple domains (Interview X).

Specifically, CERT.hr was responsible for handling cybersecurity incidents involving entities located in Croatia or using the .hr domain or Croatian IP address space, including academia, research, certain public institutions outside ZSIS's jurisdiction, private sector entities, and individual users (Interview X). During this period, six main authorities were responsible for various aspects of national cybersecurity: ZHIS, CERT.hr, the Office of the National Security Council (UVNS), the Ministry of the Interior (MUP), the Ministry of Justice, Public Administration and Digital Transformation

[12] Note that UVNS was appointed Croatian single point of contact under the Act, while ZSIS was designated as the main competent CSIRT, accompanied by CERT.hr under CARNET as a sectoral CSIRT (Katulić & Lisicar, 2024).

(MPUDT), and the Croatian Regulatory Authority for Network Industries (HAKOM) (Interview 7).

Nevertheless, the European revision of the NIS II (2022) Directive created renewed momentum in Croatia to reconsider the distribution of national cyber competences. The process of NIS II transposition has sparked debates on how to recalibrate the national cybersecurity governance model, particularly in light of the directive's broader scope, expanded sectoral coverage, and increased operational and strategic responsibilities for national authorities (Interview X).

Through a national working group coordinated by the Ministry of Justice and Public Administration (MPU), a selected set of industry stakeholders were invited to advise on the national transposition of NIS II (Interview 5, 7, 13, 15). Their role, however, remained consultative, as the government retained primacy in shaping the legislative framework. In parallel, the draft Cybersecurity Act was submitted to Croatia's mandatory online consultation platform (e-Savjetovanje),[13] which allowed a broader range of actors from the private sector, civil society, and academia to provide input (Government of the Republic of Croatia, 2025; Interview 7, 8). While these mechanisms opened formal channels for participation, interviewees suggested that industry input was secondary to state security priorities, with final decision-making concentrated within governmental institutions (Interview 5, 7, 13, 15).

[13] See https://esavjetovanja.gov.hr/ECon/Dashboard.

2024 – Cyber Security Act (NIS II)

With the transposition of NIS II into the national Cybersecurity Act in 2024, a more decisive transformation occurred. This reform entailed a reallocation of institutional competences: the national CSIRT function was transferred from ZSIS to the newly established National Cyber Security Centre (NCSC-HR) within SOA, while complementary CSIRT responsibilities were assigned to NCERT (formerly CERT.hr) (Interview X). Under this framework, NCERT's mandate was narrowed to a defined set of sectors, including research, education, banking, financial market infrastructure, and digital infrastructure, while NCSC-HR became the central authority for incident handling across the broader national landscape (Interview 9). The outcome is a tandem model, where NCERT continues to provide sectoral CSIRT services and NCSC coordinates national-level incident response, creating a decentralized cybersecurity system embedded within the country's intelligence community. This reflects an organic and ongoing evolution of Croatia's governance model, streamlining roles from the previous structure to the following main entities: NCSC, NCERT, UVNS, and sectoral authorities.[14]

The technical expertise of ZSIS now primarily supports cybersecurity certification, audits, and risk assessments under the framework of EU Cybersecurity Certification legislation (2019), ensuring continuity of institutional knowledge and compliance with European standards. In parallel, NKS-HR was established under CARNET as a

[14] The sectoral authorities include for example the Croatian Regulatory Authority for Network Industries (HAKOM), the Croatian National Bank (HNB), the Croatian Financial Services Supervisory Agency (HANFA), and the Croatian Civil Aviation Agency (HACZ) (NCSC-HR, 2025).

national Cyber Competence Centre, in line with EU policy (EU Cybersecurity Competence Centre and Network Regulation, 2021; NKS/NCC-HR, 2025). NKS-HR focuses on cyber resilience, capacity building, training, and awareness (NKS/NCC-HR, 2025), providing national-level support across all sectors, complementing the national cybersecurity architecture.

According to some observers within the system, the reform was intended to make better use of available resources (Interview X), though opinions vary on whether the resulting structure is actually more efficient in practice (Interview X). Overall, the shift is very recent, and most stakeholders remain cautiously optimistic, waiting to see how the new framework performs over time (Interview X).

Concluding Discussion

To summarize, the Croatian cybersecurity ecosystem is characterized by fragmented hierarchies, in which multiple top-down actors pursue distinct institutional goals. At the same time, informal networks of influence and "soft-power linkages" serve as the glue that keeps the system functioning under the ultimate authority of the state.

The current arrangement reflects a novel institutional evolution, rooted in earlier practices but shaped decisively by the transposition of NIS II. Croatia now operates a tandem cybersecurity model, with the NCSC-HR and the NCERT representing the intelligence and scientific communities respectively. This tandem is complemented by decentralised functions such as certification and the national competence centre, resulting in a distribution of cyber-related competences

that stands in contrast to Belgium's more centralised approach (De Stercke & Janssens, 2025).

Both NIS I and NIS II allow EU Member States to adopt flexible institutional arrangements for CSIRTs and competent authorities, while requiring each Member State to designate a single national point of contact (SPOC) for EU-level coordination (NIS I, 2016, art. 8-9; NIS II, 2018). While such decentralization can enhance resilience by reducing dependence on a single entity, the growing uneven proliferation of CSIRTs across Europe raises concerns about efficiency and coordination (See for example ENISA, 2025b). Although NIS II sought to clarify responsibilities within the complex European cybersecurity ecosystem (NIS I, 2016; NIS II, 2018), it remains debatable whether the resulting fragmentation is a flaw or a latent strength.

Unlike Ukraine's decentralized and highly adaptive cyber structures, which have proven resilient in practice (Dmitri, 2023), the European Framework tends to be more rigid, potentially limiting its capacity to respond swiftly to transnational cyber incidents. Food for thought, particularly considering the Union's current deregulatory stance (Corporate Europe Observatory, 2025).

Next to the multitude, a variety of actors is always involved in any national cybersecurity ecosystem (Trimintzios et al., 2017). In Croatia, the 'cyberdefence centre of gravity' is primarily situated within the intelligence community, reflecting an intelligence-driven model that is not uncommon (Morgus et al., 2015). Yet, the recent Italian reform removing national CSIRT functions from the intelligence domain into a

civilian-led model (Agenzia per la Cybersicurezza Nazionale (ACN), 2022; Interview 10), illustrates ongoing debates about where these responsibilities are best placed (see Trimintzios et al., 2017).

Despite the recent dynamics in Croatian cyber governance (see supra), Croatia's traditional security siloes remain largely intact. Compared to Belgium, horizontal integration on an organizational level is rather weak: institutions focus on their own mandates, display limited insight into partners' internal processes, and rely heavily on legal frameworks.[15] Hybridised or deeply collaborative arrangements, such as those seen in Belgium (De Stercke & Janssens, 2025), are not observed. Whether this reflects a less stress-tested cybersecurity environment in Croatia compared to Belgium,[16] or stems from Croatia's experience of their Homeland War favoring a more militarized and siloed organizational structure,[17] remains an open question.

The private sector is integrated in eclectic and often less formally structured ways. Engagement tends to emerge through existing networks or government reliance on private actors to manage IT systems, rather than through structured public-private partnerships (see supra). This contrasts with Belgium, where partnerships are more formalised, and private actors play visible roles in delivering critical services (De Stercke & Janssens, 2025).

[15] Based on the author's empirical observations.

[16] As '[c]ybercriminals and state-sponsored threat actors alike have been targeting English-speaking economies with resource-rich businesses …' (van der Walt, 2024), Croatia's smaller economy (European Union, 2025) and language-specific barriers may indeed reduce its vulnerability.

[17] See for example Polic (2021) on Croatia's contemporary war legacy.

Still, Croatia benefits from a small and interconnected cybersecurity community, where personal relations act as the soft-power glue not necessarily formally acknowledged (see supra). As in Belgium (De Stercke & Janssens, 2025), much depends on people contacting people. This may be the strength of small states perhaps, or is it the paradox of the information society; that one of the strongest ways to provide resilience, is to physically connect? Within light of this observation, practices that foster cross-fertilization across Europe should be encouraged. For example, frameworks for seconded national experts (see for example ENISA, 2025a), liaison officers (see for example Europol, 2025b), or cyber reservists following the military model, to name a few.

Broader societal dynamics were also evident: a strong attachment to the 'Homeland' was frequently observed, with higher education often pursued abroad but followed, sooner or later, by a return to Croatia.[18] This pattern appears to be reflected in recent migration statistics, which indicate that 'return migration' has become a notable trend (CroatiaWeek, 2025). From a capacity-building perspective, one might derive the hypothesis that such mobility may create temporary gaps in domestic expertise yet ultimately enriches the national system through the reintegration of internationally trained professionals.

Lastly, it is noted that Croatia occupies a strategically significant position in South-Eastern Europe, serving as

[18] These findings are supported by the author's empirical observations of high-level professionals who pursued studies or a (European) career abroad and later returned to Croatia, either early in their careers or after gaining senior experience. Meanwhile, student exchange programmes remain widely utilized among younger generations as well.

a bridge towards the Western Balkan within the European Union (Lawless, 2025). This unique status enhances its role in fostering regional cooperation and advancing EU integration efforts for neighboring countries. However, this prominence also renders Croatia a potential target for geopolitical and cyber threats. Croatia and the Balkan region, have witnessed a surge in cyberattacks, with incidents such as phishing campaigns and ransomware attacks becoming more prevalent (Salipur, 2024). The rise of AI-driven cyber threats further exacerbates these challenges, enabling more sophisticated and widespread attacks (Europol, 2025a). Despite these pressures, Croatia's EU membership positions it as a pivotal actor in regional (cyber)security initiatives (Lawless, 2025; Pitu, 2025), and henceforth, its influence in shaping the Western Balkans' strategic landscape continues to expand.

Essentially, the Croatian cybersecurity ecosystem is characterized by fragmented hierarchies, in which multiple top-down actors pursue distinct institutional goals. At the same time, informal networks of influence and "soft-power linkages" serve as the glue that keeps the system functioning under the ultimate authority of the state. By capturing the Croatian frameworks, key actors, and critical collaborations, the case study illustrates how cybersecurity is reshaping but also extending traditional dynamics. It highlights the need for further comparative analysis to understand how different national systems adapt to European imperatives, and what this means for the future of security governance in the digital era.

Acknowledgements

This work was supported by the Ghent University Special Research Fund (BOF) through a PhD fellowship (BOF22/DOC/295). Fieldwork in Croatia was additionally funded by the Research Foundation Flanders (FWO – grant number V439925N), and supplementary support was received from the Faculty Mobility Fund and the FFWO of the Faculty of Law and Criminology, Ghent University.

Literature:

1. Agenzia per la Cybersicurezza Nazionale (ACN). (2022). National Cybersecurity Strategy.
2. Baldoni, R., & Di Luna, G. (2025). Sovereignty in the Digital Era: The Quest for Continuous Access to Dependable Technological Capabilities. IEEE Security & Privacy, 23, 91-96.
3. Berger, R. (2015). Now I see it, now I don't: researcher's position and reflexivity in qualitative research. Qualitative Research, 15(2), 219-234. https://doi.org/10.1177/1468794112468475
4. Bures, O., & Carrapico, H. (2018). Private Security Beyond Private Military and Security Companies: Exploring Diversity Within Private–Public Collaborations and Its Consequences for Security Governance. In O. Bures & H. Carrapico (Eds.), Security Privatization: How Non-security-related Private Businesses Shape Security Governance (pp. 1-19). Springer International Publishing. https://doi.org/10.1007/978-3-319-63010-6_1
5. Button, M. (2020). The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions. Journal of Contemporary Criminal Justice,

36(1), 39-55. https://doi.org/10.1177/1043986219890194

6. CERT.hr. (2025). About National CERT. https://www.cert.hr/en/home-page/
7. Charmaz, K. (2006). Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis. SAGE Publications. https://books.google.be/books?id=w2sDdv-S7PgC
8. Charmaz, K. (2024). Constructing Grounded Theory. Sage. https://books.google.be/books?id=6yyx0AEACAAJ
9. Corporate Europe Observatory. (2025). A crash course on the EU's deregulation wave. https://www.corporateeurope.org/en/2025/07/crash-course-eus-deregulation-wave
10. Croatian Personal Data Protection Agency (AZOP). (2025). About the Agency. https://azop.hr/about-the-agency/#:~:text=The%20Croatian%20Personal%20Data%20Protection,Regulation%20(Official%20Gazette%2C%20No
11. CroatiaWeek. (2025). 30,000 Croatians return home in last 3 years, many launching businesses. https://www.croatiaweek.com/30000-croatians-return-home-in-last-3-years-many-launching-businesses/?utm_source=chatgpt.com
12. Cybersecurity Act [Zakon o kibernetičkoj], br. 42 Narodne novine (2024).
13. De Arimatéia da Cruz, J., & Pedron, S. (2020). Cyber Mercenaries. A New Threat to National Security. International social science review, 96(2), 1-33. https://www.jstor.org/stable/27071316

14. De Stercke, C., & Janssens, J. (2025). Plural Policing in Cyberspace: Unveiling Belgium's Cybersecurity Architecture. European Journal of Policing Studies.

15. De Stercke, C., Petrovska, O., & Janssens, J. (2024). Cybercrime & Cyberwarfare: Entering the Grey Zone. Freedom From Fear Magazine (F3), pp. 31-41. https://unicri.org/sites/default/files/2025-05/F3-2024-Cybercrime-cyberwarfare-grey-zone-Celien-De-Stercke-Olga-Petrovska-Jelle-Janssens.pdf

16. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), European Parliament & Council (2016).

17. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), European Parliament & Council (2022).

18. Dmitri. (2023). How decentralization saved the Ukrainian internet: lessons from 2022, government officials and telecom industry reflect in Kyiv. eQualitie. https://equalit.ie/decentralization-saved-the-ukrainian-internet/

19. European Council on Refugees and Exiles. (2024). BALKAN ROUTE: Significant decrease in irregular border crossings via Balkan route. https://ecre.org/balkan-route-significant-decrease-in-irregular-border-crossings-via-balkan-route-%E2%80%95-

croatian-border-police-accused-of-pushbacks-and-burning-peoples-belongings-%E2%80%95-ecre-member-organisat/#:~:text=*%20BALKAN%20ROUTE:%20Decrease%20in%20Number%20of,Signs%20New%20”ront’x%2DSerbia%20Cooperation%20Agreement%20(July%202024)

20. European Parliament. (2024). Schengen: enlargement of Europe’s border-free area. https://www.europarl.europa.eu/topics/en/article/20180216STO98008/schengen-enlargement-of-europe-s-border-free-area#:~:text=Enlargement%20of%20Schengen,lifted%20on%201%20January%20202
21. European Union. (2025). Facts and figures on the European Union. https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_en
22. European Union Agency for Cybersecurity (ENISA). (2025a). Call for Expression of Interest for Seconded National Experts (SNEs) In.
23. European Union Agency for Cybersecurity (ENISA). (2025b). CSIRTs by Country. https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map
24. Europol. (2025a). The changing DNA of serious and organized crime (Serious and Organised Crime Threat Assessment (SOCTA), Issue.
25. Europol. (2025b). Partners & Collaboration. Liaison officers. https://www.europol.europa.eu/partners-collaboration
26. Government of the Republic of Croatia. (2025). e-Consultation Portal launched for citizens to take more active part in law

making. https://vlada.gov.hr/e-consultation-portal-launched-for-citizens-to-take-more-active-part-in-law-making/16865

27. Information Security Act [Zakon o informacijskoj sigurnosti], Narodne novine (2007).
28. Information Systems Security Bureau (ZSIS). (2025). Cybersecurity certification. https://www.zsis.hr/default.aspx?id=516
29. Katulić, T., & Lisicar, H. (2024). The current and developing regulatory framework of information security in the EU and the Republic of Croatia. 13, 25-51.
30. Lawless, J. (2025). Western Balkans leaders meet in London for talks on migration and security. The Washington Post. https://www.washingtonpost.com/world/2025/10/22/western-balkans-summit-uk-migration/996e7f28-aeff-11f0-ab72-a5fffa9bf3eb_story.html
31. Maurer, T. (2018). Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press. https://doi.org/DOI: 10.1017/9781316422724
32. Ministry of Interior (MUP). (2025). Uprava kriminalističke policije. https://policija.gov.hr/uprava-kriminalisticke-policije/415
33. Ministry of the Interior (MUP). (2025). About the Police. https://mup.gov.hr/footer-111/about-the-police-120/120
34. Missiroli, A. (2021). Hybrid CoE Paper 7. Geopolitics and strategies in cyberspace: Actors, actions, structures and responses (978-952-7282-82-3). (Hybrid CoE Papers, Issue.

35. Morgus, R., Skierka, I., Hohmann, M., & Maurer, T. (2015). National CSIRTs and their Role in Computer Security Incident Response (Transatlantic Dialogues on Security and Freedom in the Digital Age, Issue. https://gppi.net/2015/11/19/national-csirts-and-their-role-in-computer-security-incident-response

36. The National Cyber Security Strategy of the Republic of Croatia (2015).

37. National Cybersecurity Centre (NCSC-HR). (2025). About us. https://ncsc.hr/en/about-us

38. NKS/NCC-HR. (2025). About Us. https://nks.hr/en/o-nama/

39. Patton, M. Q. (2014). Qualitative Research & Evaluation Methods: Integrating Theory and Practice. SAGE Publications. https://books.google.be/books?id=ovAkBQAAQBAJ

40. Pitu, L. (2025). What is the Berlin Process summit for the Western Balkans? Deutsche Welle. https://www.dw.com/en/london-2025-berlin-process-summit-for-the-western-balkans-explained/video-74437882

41. Polic, I. (2021). Three Decades On, War's Legacy Still Overshadows. BalkanInsight. https://balkaninsight.com/2021/03/31/three-decades-on-wars-legacy-still-overshadows-croatia/

42. Pusić, V. (2022). War and hate: Lessons for the Balkans from the invasion of Ukraine. European Council on Foreign Relations (ECFR). https://ecfr.eu/article/war-and-hate-lessons-for-the-balkans-from-the-invasion-of-ukraine/#top

43. Raymond, M. (2016). Managing Decentralized Cyber Governance

44. The Responsibility to Troubleshoot. Strategic Studies Quarterly, 10(4), 123-149. http://www.jstor.org/stable/26271532

45. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), European Parliament & Council (2019).

46. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, European Parliament & Council (2021).

47. Salipur, I. (2024). Delivery Deception: Escalating cybercriminal tactics in the Balkan region. Group-IB. https://www.group-ib.com/blog/cybercriminal-tactics-in-the-balkan-region/?utm_source=chatgpt.com

48. Smeets, M. (2025). Ransom War. How Cyber Crime Became a Threat to National Security. C Hurst & Co Publishers Ltd.

49. Stevens, T. (2017). Cyberweapons: an emerging global governance architecture. Palgrave Communications, 3(1), 16102. https://doi.org/10.1057/palcomms.2016.102

50. Stoddart, K. (2022). Cyberwarfare. Threats to Critical Infrastructure. Palgrave Macmillan Cham. https://doi.org/https://doi.org/10.1007/978-3-030-97299-8

51. Trimintzios, P., Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). Cybersecurity in the EU

Common Security and Defence Policy (CSDP). Challenges and risks for the EU. European Union. https://doi.org/10.2861/853031

52. Van der Walt, C. (2024). As four cyber trends increased in 2023/24, one victim profile stood out… [Interview]. CyberSecAsia. https://cybersecasia.net/blackberry/featured-content-2022/as-four-cyber-trends-increased-in-2023-24-one-victim-profile-stood-out/?utm_source=sociabbleapp&utm_medium=social&utm_campaign=__campaign_soc__&utm_term=w4aUTZqJiHcF&socid=w4aUTZqJiHcF