SJPS | Slovak Journal of Political Sciences
Scientific article
sjps.fsvucm.sk I ISSN 1335-9096 (online)
2022 The Faculty of Social Sciences
University of Ss. Cyril and Methodius, Trnava.
DOI: https://doi.org/10.34135/sjps.260105

CYBERCRIME AS A COMPONENT OF EUROPEAN SECURITY POLICY: AN ANALYSIS OF THE SECURITISATION OF DIGITAL THREATS IN EUROPE

Libor Klimek[1]

Abstract
This article analyses cybercrime as a component of European security policy, examining how digital criminality is constructed as a security threat within the political discourse and governance practices of the European Union and the Council of Europe. Rather than approaching cybercrime as a purely legal or technical problem, the article conceptualises it as a politically constructed issue embedded in broader processes of securitisation and security governance. The main objective is to explore how cybercrime is framed as a transnational and systemic threat and how this framing legitimises specific models of security intervention at the European level. The research is guided by the question of how cybercrime is securitised by different European institutions and what political implications follow from these securitisation strategies. Methodologically, the article employs a qualitative interpretative approach grounded in securitisation theory, combining political discourse analysis with a comparative institutional perspective. The analysis demonstrates that the European Union advances an integration-oriented model of securitisation based on regulatory harmonisation and resilience-building, while the Council of Europe promotes a norm-driven approach centred on treaty-based cooperation, human rights safeguards and capacity-building.

Keywords: *Cybercrime, European security policy, Securitisation, Security governance, European Union, Council of Europe*

INTRODUCTION

Digitalisation has profoundly transformed the social, economic and political foundations of contemporary European societies. The expansion of networked infrastructures, data-driven governance and digitally mediated forms of interaction has created new opportunities for economic growth and social connectivity, while simultaneously generating novel forms of vulnerability. Within this evolving environment, cybercrime has emerged as

[1] Faculty of Law, Matej Bel University in Banská Bystrica, Komenského 20, 974 01 Banská Bystrica, Slovak Republic, e-mail: libor.klimek@umb.sk, ORCID-ID: https://orcid.org/0000-0003-3826-475X.

a particularly salient phenomenon, not only as a form of criminal activity, but as a challenge that increasingly intersects with broader questions of security, governance and political authority.

In the European context, cybercrime has become closely intertwined with debates on internal security, resilience and the capacity of political institutions to govern transnational risks. Unlike traditional forms of crime, cybercrime operates in a deterritorialised digital space that undermines the effectiveness of state-centred enforcement mechanisms and exposes the limits of nationally bounded security responses. As a result, cybercrime has been progressively reframed as a transnational threat with systemic implications for critical infrastructure, economic stability and democratic governance. This reframing has unfolded particularly over the past two decades, coinciding with the European Union's deepening integration in the field of internal security and the Council of Europe's consolidation of treaty-based cooperation on cybercrime.

From a political science perspective, the growing prominence of cybercrime within European policy agendas cannot be explained solely by reference to technological change or rising crime rates. Rather, it reflects a broader process through which cybercrime has been constructed as a security-relevant issue requiring exceptional attention, coordinated action and new forms of governance. This process has been especially visible since the mid-2010s, as European institutions increasingly linked cybercrime to strategic vulnerability, societal resilience and the protection of the digital single market, situating it firmly within the evolving architecture of European security policy.

The main objective of this article is to analyse how cybercrime is constructed as a component of European security policy through political discourse and institutional practice. Specifically, the article seeks to examine how cybercrime is framed as a security threat by the European Union and the Council of Europe, and how these framings translate into distinct models of security governance. In addition to this primary objective, the article pursues two secondary objectives: first, to compare the securitisation strategies employed by these two organisations, and second, to assess the political implications of their respective approaches for legitimacy, authority and governance in the digital domain.

The central research question guiding this analysis is formulated as follows: How is cybercrime constructed as a security threat within the political discourse of the European Union and the Council of Europe, and what role does this construction play in shaping European security governance?

This question is justified by the observation that cybercrime increasingly serves as a justificatory resource for expanding regulatory, institutional and cooperative frameworks at the European level. By focusing on securitisation processes rather than on legal definitions or technical measures, the article seeks to uncover the political logic underpinning contemporary cybercrime governance in Europe.

Methodologically, the article adopts a qualitative and interpretative research design grounded in political discourse analysis and institutional comparison. It draws on securitisation theory as a conceptual framework to examine how cybercrime is framed as an existential or systemic threat and how such framings legitimise specific policy responses. The empirical material consists of key strategic documents, policy communications and legal instruments adopted by the European Union and the Council of Europe, supplemented by relevant academic literature. Rather than evaluating policy effectiveness, the analysis focuses on meaning-making processes, governance rationales and legitimacy claims.

Existing scholarship provides important insights into both European security governance and the political construction of digital threats, yet it remains fragmented across disciplinary boundaries. Research on European security governance has highlighted the EU's increasing role as a security actor and the expansion of integration-driven security policies beyond traditional domains (Kaunert and Léonard, 2013; Biscop, 2016; Galbreath, Mawdsley and Chappell, 2019). At the same time, legal and policy-oriented studies have examined the regulatory dimensions of cybersecurity and cybercrime governance within EU law (Porcedda, 2023; Karathanasis, 2024; Chiara, 2024), while criminological literature has explored the evolving nature of cybercrime as a social and technological phenomenon (Klimek, Záhora and Holcr, 2016; Rüdiger and Bayerl, 2020; Wernert, 2021).

Despite these contributions, there remains a relative lack of political science research that systematically compares how different European institutions securitise cybercrime and translate threat narratives into governance models. In particular, the contrast between the European Union's integration-oriented approach and the Council of Europe's norm-driven, treaty-based model has received limited analytical attention. This article contributes to the existing literature by addressing this gap and by demonstrating how cybercrime functions as a site of competing securitisation logics within Europe's fragmented yet interconnected security landscape.

The article is structured as follows. Section 1 conceptualises cybercrime as a political and security-relevant phenomenon from a political science

perspective. Section 2 introduces securitisation theory and discusses its relevance for analysing digital threats. Section 3 situates cybercrime within the broader framework of European security governance. Section 4 examines how cybercrime is framed and governed within the European Union's security discourse and regulatory practice. Section 5 analyses the Council of Europe's approach to cybercrime, with particular attention to normative constraints and external governance. Section 6 provides a comparative discussion of the two models of securitising cybercrime in Europe.

1 CYBERCRIME AND SECURITY: A POLITICAL SCIENCE PERSPECTIVE

From a political science perspective, cybercrime cannot be reduced to a category of unlawful behaviour addressed exclusively through criminal law. Rather, it should be understood as a broader socio-political phenomenon emerging from the structural transformation of contemporary societies driven by digitalisation. The expansion of digital infrastructures, transnational networks and data-dependent economies has fundamentally altered the context in which security threats are identified and governed. Within this environment, cybercrime increasingly transcends the boundaries of traditional criminal justice and enters the realm of security politics.

Unlike conventional forms of crime, cybercrime operates in a deterritorialised space where geographical borders lose much of their regulatory significance (Wernert, 2021). These characteristic challenges state-centred models of security and law enforcement, which were historically premised on territorial sovereignty and clearly defined jurisdictions. As a consequence, cybercrime becomes politically salient not merely because of its criminal nature, but because it exposes the limitations of existing security arrangements and generates pressure for new forms of political coordination and governance beyond the nation-state.

In contemporary studies, cybercrime is commonly conceptualised as a non-traditional or emerging security threat. Its defining features, including anonymity, speed, scalability and cross-border reach, distinguish it from classical military or criminal threats and complicate both attribution and response (Stephenson – Gilbert, 2004; Klimek – Záhora – Holcr, 2016; Rüdiger – Bayerl, 2020; Wernert, 2021; Bhushan – Jamshed, 2025). These characteristics contribute to the perception of cybercrime as an unpredictable and potentially systemic risk rather than as isolated instances of unlawful behaviour. As a result, cybercrime is increasingly framed as a

threat to economic stability, critical infrastructure, democratic institutions and societal trust in digital systems, thereby expanding its relevance within political security agendas.

Cybercrime becomes a security issue through narratives that link digital criminal activity to existential vulnerability and loss of control. Political actors, institutions and expert communities play a central role in shaping these narratives by presenting cybercrime as a pervasive and escalating threat that requires extraordinary attention and coordinated responses. Through such discursive framing, cybercrime is elevated from a technical or legal problem to a matter of security policy.

The securitisation of cybercrime has important implications for governance structures. Responses to cybercrime typically extend beyond traditional policing and judicial mechanisms and involve a wide range of actors, including security agencies, regulatory bodies, private technology companies and international organisations (Klimek – Záhora – Holcr, 2016). This reflects a shift towards networked and multi-level forms of security governance in which authority is dispersed and responsibility is shared across institutional boundaries. From a political science perspective, these arrangements raise critical questions about power, accountability and legitimacy within contemporary security policy.

Framing cybercrime as a security issue also carries significant normative consequences. Security-oriented approaches tend to prioritise effectiveness, anticipation and risk management, which may generate tensions with principles such as individual privacy, data protection and democratic oversight. Measures justified in the name of cyber security often expand institutional capacities for surveillance, information sharing and preventive intervention (Kaunert – Léonard, 2013; Biscop, 2016; Fahey, 2022; Porcedda, 2023; Karathanasis, 2024; Bhushan – Jamshed, 2025). In the European context, cybercrime occupies a particularly prominent position within security debates due to its inherently transnational nature. European political actors frequently invoke cybercrime to justify coordinated responses at the supranational level, arguing that individual states lack the capacity to address digital threats effectively on their own. In this sense, cybercrime functions not only as an object of security policy but also as a political resource that facilitates deeper cooperation and integration in the field of European security governance. From a political science perspective, cybercrime thus represents a constructed security threat that contributes to the evolving architecture of security policy in Europe and sets the stage for further analysis of its securitisation within European institutions.

2 SECURITISATION THEORY AND DIGITAL THREATS AND CYBERCRIME

Securitisation theory provides a particularly useful analytical framework for examining how cybercrime is transformed from a technical or criminal issue into a matter of security policy. Developed within political science and security studies, this approach shifts attention away from the material characteristics of threats and towards the political processes through which certain phenomena come to be framed as security concerns (Balzacq, 2010; Floyd, 2019). In the context of digitalisation and cybercrime, securitisation theory allows for a systematic analysis of how political actors construct digital threats, mobilise legitimacy for extraordinary measures and reshape governance structures at both national and European levels.

At its core, securitisation theory conceptualises security as the outcome of a political process rather than an objective condition. Issues become security issues when they are presented as existential threats that require urgent action beyond the normal bounds of politics. This process typically involves authoritative actors who articulate a threat narrative, an audience that accepts or tolerates this framing, and a set of proposed measures that are justified by reference to the perceived urgency of the threat.

From a political science perspective, securitisation is therefore understood as a performative act. By declaring something a security issue, political actors seek to legitimise particular policy responses and to prioritise certain values, such as protection and stability, over others, such as openness or procedural restraint. This insight is especially relevant in the digital domain, where threats are often abstract, invisible and difficult to verify, making them particularly susceptible to discursive construction.

Digitalisation has profoundly altered the environment in which security narratives are produced and disseminated. Cyberspace is frequently depicted as a domain characterised by uncertainty, vulnerability and constant exposure to risk. Within this context, cybercrime is not merely described as illegal activity but as a symptom of a broader loss of control over digital infrastructures, data flows and technological systems.

Cybercrime is portrayed as capable of causing systemic disruption, undermining critical infrastructure, destabilising economies and eroding public trust in democratic institutions (Rüdiger – Bayerl, 2020; Wernert, 2021; Bhushan – Jamshed, 2025). These narratives contribute to a sense of urgency and exceptionalism, which is central to the logic of securitisation.

By framing cybercrime as a threat that transcends traditional boundaries and capacities, political actors create a discursive environment in which extraordinary coordination, regulation and intervention appear both necessary and legitimate.

Within securitisation theory, cybercrime can be analysed as a paradigmatic example of a securitised non-traditional threat. Unlike conventional security challenges, cybercrime lacks a clearly identifiable enemy and operates through dispersed networks rather than hierarchical structures. This ambiguity enhances its suitability for securitisation, as the absence of a concrete adversary allows threat narratives to remain broad and flexible. The securitisation of cybercrime typically involves linking digital criminal activity to wider security concerns, such as national sovereignty, public order and geopolitical stability. Cybercrime is often discursively associated with hostile state behaviour, organised crime or hybrid threats, even when empirical evidence remains limited or contested. From a political science standpoint, the significance of this association lies not in its factual accuracy but in its political effects. By embedding cybercrime within broader security narratives, political actors expand the scope of security policy and justify the mobilisation of resources and authority.

A crucial element of securitisation is the role of the audience. For securitisation to be effective, threat narratives must resonate with relevant audiences, including political institutions, expert communities and the wider public. In the case of cybercrime, audience acceptance is often facilitated by widespread perceptions of technological vulnerability and limited public understanding of digital risks.

The securitisation of digital threats has far-reaching implications for policy-making and governance. Once cybercrime is framed as a security issue, policy responses tend to prioritise prevention, resilience and risk management. This often leads to the expansion of surveillance capacities, data-sharing arrangements and regulatory frameworks that extend beyond traditional criminal justice mechanisms.

From a political science perspective, these developments raise important questions about the boundaries of security policy and the normalisation of exceptional measures. Securitisation can blur the distinction between routine governance and emergency politics, making it more difficult to subject security measures to democratic scrutiny. In the digital context, where threats are ongoing rather than episodic, securitisation risks becoming a permanent condition rather than a temporary response.

3 EUROPEAN SECURITY POLICY AND THE GOVERNANCE OF CYBER THREATS

European security policy has undergone a gradual but significant transformation in response to the proliferation of cyber and digital threats. Cybercrime, in particular, has become a central reference point in debates on security governance, as it challenges traditional assumptions about territoriality, authority and the division of competences between national and supranational levels. The governance of cyber threats in Europe illustrates how security policy increasingly operates through coordination, standard-setting and strategic framing rather than through classic coercive instruments alone.

Historically, European security policy was shaped primarily by concerns related to military conflict, interstate relations and, later, internal security issues such as terrorism and organised crime. The rise of digital technologies has progressively expanded this agenda by introducing new categories of risk that are not easily addressed through existing security frameworks. Cybercrime exemplifies this shift, as it combines elements of criminal activity, economic risk and systemic vulnerability. In the digital age, European security policy has increasingly emphasised resilience, prevention and preparedness. Rather than reacting to isolated incidents, policy discourse focuses on the anticipation of threats and the management of long-term risks associated with digital dependence. This evolution reflects a broader reconceptualisation of security as a continuous process of governance rather than as an episodic response to clearly identifiable dangers.

The governance of cyber threats in Europe is inherently multi-level. Cybercrime operates across borders, affects multiple policy sectors and involves a wide range of public and private actors. As a result, security governance in this area cannot be monopolised by individual states (Rüdiger – Bayerl, 2020; Wernert, 2021). Instead, it is characterised by overlapping competences, shared responsibilities and coordinated action across different levels of authority. From a political science perspective, this multi-level governance structure raises important questions about who defines security priorities and how policy coherence is achieved. Cybercrime-related policies often emerge from complex interactions between national governments, supranational institutions, expert networks and private actors. European security policy thus functions as a space of negotiation in which different interests, threat perceptions and normative commitments are reconciled.

The EU has increasingly positioned itself as a central coordinator of cyber security policy, framing cybercrime as a shared security challenge that requires collective responses. Political discourse at the EU level frequently highlights the inadequacy of purely national approaches and emphasises the need for harmonised strategies, information sharing and common standards (Klimek – Záhora – Holcr, 2016). The EU's involvement in cyber security governance is not merely functional but also political. By defining cybercrime as a European security issue, EU institutions strengthen their role as legitimate security actors and expand the scope of supranational governance. Cyber threats thus become a vehicle through which the EU reinforces its capacity to act in areas traditionally associated with state sovereignty, including security and criminal justice.

European security policy addressing cyber threats relies on a diverse set of governance instruments. These include strategic frameworks, action plans, coordination mechanisms and regulatory initiatives that seek to align national policies and facilitate cooperation. Importantly, these instruments are often justified through a security-oriented rationale that emphasises urgency, interdependence and shared vulnerability. Cybercrime occupies a strategic position within this rationale because it can be linked simultaneously to internal security, economic stability and external relations. This multifunctional character allows cybercrime to serve as a bridge between different policy domains and to legitimise integrated approaches to security governance. This illustrates how security policy increasingly operates through cross-sectoral coordination rather than through isolated policy silos.

The expansion of European security policy into the domain of cyber threats also raises questions of legitimacy and accountability. Governance arrangements that rely on expert knowledge, technical coordination and preventive action tend to reduce the visibility of political choice and contestation. Cyber security policies are frequently presented as technical necessities rather than as politically contingent decisions. This depoliticisation poses a challenge for democratic governance. While coordinated responses to cybercrime may enhance effectiveness, they can also obscure lines of responsibility and limit opportunities for public debate. Political science analysis therefore pays close attention to how security governance balances efficiency with transparency and how legitimacy is constructed in the absence of direct democratic engagement.

4 THE EUROPEAN UNION: CYBERCRIME IN SECURITY AND POLICY DISCOURSE

The European Union's engagement with cybercrime is best understood as a discursive and institutional process through which digital criminality is positioned within a wider European security agenda (Kaunert – Léonard, 2013; Biscop, 2016; Galbreath – Mawdsley – Chappell, 2019). Rather than treating cybercrime primarily as a narrow criminal justice problem, EU-level policy discourse increasingly presents it as a structural threat, intertwined with economic stability, critical infrastructure protection, societal resilience, and the integrity of democratic institutions. This section analyses how that framing is produced and stabilised through key EU strategic texts and legal instruments, and how these outputs collectively contribute to a particular model of cyber threat governance.

4.1 Preliminary descriptive comparisons

A pivotal reference point for the contemporary EU security framing is the *Security Union Strategy for 2020–2025*[2], which explicitly adopts an integrated understanding of security across physical and digital environments and emphasises coordinated action at EU level (Porcedda, 2023; Herlin-Karnell – Conway – Ganesh, 2021). The strategy's underlying political logic is that the interdependence of Member States – especially in digital infrastructures and data flows – creates shared vulnerabilities that cannot be addressed effectively through nationally bounded approaches. Cybercrime, within this framing, functions as a paradigmatic cross-border threat that both justifies and requires deeper cooperation in the Area of Freedom, Security and Justice. This is visible in the Commission's own articulation of the Security Union approach as responding to a rapidly changing threat landscape through coordinated and integrated action.

This security framing is not merely descriptive. It implicitly redefines the legitimate scope of EU action by positioning cybercrime as a threat that is simultaneously internal and external, criminal and geopolitical, technical and societal. The consequence is a narrative in which cybercrime becomes a political resource: it legitimises not only operational cooperation, but also

[2] European Commission (2020) Communication from the Commission on the EU Security Union Strategy, COM(2020) 605 final. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605 (Accessed: 5 February 2026).

regulatory initiatives and institutional strengthening at EU level. In that sense, cybercrime is discursively mobilised to support the EU's broader claim to be a security actor capable of producing collective protection.

the European Commission explicitly situates cyber threats and cyber-attacks alongside other evolving risks in the digitally mediated security environment. The strategy notes that "cyber-attacks and cybercrime continue to rise" and underscores that the connectivity of physical and digital systems increases vulnerabilities, as digital infrastructures underpin essential services such as energy, transport and finance. The Commission's analysis further highlights that malicious cyber activities exploit the blurring of boundaries between digital and physical domains, enabling criminals and hostile actors to act swiftly across borders and complicating traditional security responses. In particular, cybercrime is framed as part of a broader transformation in the threat landscape that demands coordinated action at EU level, recognising that reliance on national responses alone is insufficient to protect citizens and critical infrastructures effectively. This framing supports the strategic priority of enhancing EU-wide cooperation in prevention, detection and response to digital threats, and positions cybercrime as a central element of the Security Union's integrated approach to contemporary security challenges.

4.2 Strategic Narratives Linking Cybercrime, Resilience and European Capacity to Act

The *EU's Cybersecurity Strategy for the Digital Decade*[3] of 2020 further consolidates mentioned logic by embedding cyber threats within a comprehensive agenda centred on resilience, capability-building, and European strategic autonomy in the digital domain. The strategy frames cybersecurity as a foundational condition for the functioning of contemporary European societies and economies, thereby expanding the meaning of security beyond traditional categories. Within such a framework, cybercrime is not an isolated phenomenon but part of a broader environment of malicious activity targeting digital systems and trust in digital governance. The political implication is that "security" becomes increasingly intertwined with governance of technology, standards, and systemic resilience, rather than confined to reactive enforcement.

[3] European Commission (2020) EU Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020JC0018 (Accessed: 5 February 2026).

The Cybersecurity Strategy further consolidates the framing of cybercrime as a core component of the European security agenda by explicitly linking malicious cyber activities to systemic risks affecting the Union's economy, democratic institutions and societal resilience. The strategy identifies cybercrime as a persistent and evolving threat that exploits the increasing digitalisation of public and private sectors, emphasising that criminal actors benefit from anonymity, scale and cross-border reach in cyberspace. Importantly, the document situates cybercrime within a broader threat environment that includes state-sponsored activities and hybrid threats, thereby blurring the distinction between criminality and security in the traditional sense. This discursive move reinforces the securitisation of cybercrime by embedding it within a narrative of strategic vulnerability and collective exposure, which in turn legitimises enhanced coordination, capacity-building and regulatory intervention at EU level. By framing effective action against cybercrime as essential for safeguarding trust in digital transformation, the strategy positions cybercrime governance as a prerequisite for the Union's long-term security and competitiveness, rather than as a narrow issue of criminal enforcement alone.

A complementary strand of EU discourse is visible in the *EU Strategy to tackle Organised Crime 2021–2025*[4], which explicitly identifies cyber-enabled criminality as a structural component of contemporary organised crime markets. The strategy frames cybercrime not merely as a discrete category of offences, but as an enabling infrastructure that facilitates a wide range of criminal activities, including fraud, money laundering, trafficking and illicit financial flows. By emphasising the convergence between traditional organised crime and digital tools, the document constructs cybercrime as a multiplier of criminal capacity and a key driver of cross-border criminality. This framing situates cybercrime within a broader threat environment characterised by adaptability, networked organisation and exploitation of technological innovation, thereby reinforcing its security relevance beyond the confines of criminal justice. Crucially, the strategy links the cyber dimension of organised crime to the necessity of enhanced EU-level operational and judicial coordination, arguing that fragmented national responses are structurally ill-suited to address digitally mediated criminal ecosystems (Pilniok – Dietrich, 2024). In political terms, this discursive move embeds cybercrime within an expansive "threat ecology"

[4] European Commission (2021) EU Strategy to tackle Organised Crime, COM(2021) 170 final. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021DC0170 (Accessed: 5 February 2026).

that connects economic harm, societal vulnerability and internal security risks. As a result, cybercrime is mobilised as a justificatory element for deepening cooperation, approximation and capacity-building within the Security Union framework, supporting an integrated vision of European security governance in which digital criminality is treated as a systemic challenge requiring collective action at Union level.

4.3 Legal and Regulatory Instruments as Security Governance

While the EU's strategic texts articulate the security framing, legal instruments operationalise it by translating threat narratives into governance requirements. Here, it is crucial to note that the political function of these instruments is not reducible to their technical provisions. They also signal a particular understanding of how security should be produced: through harmonised obligations, standardised reporting, and institutionalised coordination across Member States and sectors.

The *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union*[5] (also known as NIS 2 Directive) is illustrative in this respect. By setting out EU-wide measures aimed at achieving a high common level of cybersecurity, it embeds cyber threats within a governance model that relies on mandatory risk management, incident reporting, and supervisory frameworks across a broad set of entities (Durand – Gilbert-d'Halluin, 2024; Chiara, 2024). From a political science perspective, this reflects a shift towards preventive and managerial forms of security, where compliance and resilience obligations become core tools of security policy. Such instruments contribute to the normalisation of "security-by-regulation" as a mode of governing cyber risk in Europe.

A related logic is visible in the *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*[6] (also known as Digital

[5] 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 (NIS 2 Directive). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Accessed: 1 February 2026). See also: Cybersecurity of network and information systems: Summary of Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the EU. Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32022L2555 (Accessed: 1 February 2026).

[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (Accessed: 5 February 2026). Available at: https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng (Accessed: 1 February 2026). See also: Digital operational resilience for the

Operational Resilience Act), which focuses on the financial sector and institutionalises digital resilience as a regulatory priority. Although it is not a cybercrime instrument in a narrow sense, it aligns with the EU's broader security framing by treating digital disruption and cyber incidents as systemic risks to economic and societal stability. The political meaning lies in expanding the security agenda into sector-specific regulatory regimes, thereby extending security governance through the architecture of the internal market.

4.4 Access to Data, E-evidence and the Politics of Effective Enforcement

Alongside resilience-oriented governance, EU discourse also develops a distinct enforcement-oriented strand centred on operational capability and access to data. This becomes particularly salient in debates about encrypted communications, cross-border data access, and the evidentiary demands of digital investigations. In this area, the EU's framing often relies on the argument that effective law enforcement must adapt to the digital environment, and that the EU level can add value by enabling cooperation and interoperability.

The *EU's progress reporting on the Security Union Strategy*[7] of 2020 points to practical steps aimed at strengthening law enforcement capabilities, including initiatives linked to Europol and the broader law enforcement training ecosystem. The political significance lies in the normalisation of capacity-building and technical tooling as integral components of security policy, presented as necessary adaptations to an environment in which digital investigations increasingly depend on access to data.

The e-evidence package, particularly *Regulation (EU) 2023/1543 on European Production and Preservation Orders*[8] represents a further

financial sector: Summary of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32022R2554 (Accessed: 1 February 2026).

[7] European Commission (2020) Communication from the Commission to the European Parliament and the Council – First Progress Report on the EU Security Union Strategy, COM(2020) 797. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0797 (Accessed: 5 February 2026).

[8] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng (Accessed: 5 February 2026).

institutionalisation of this enforcement logic. Although formally a legal framework for cross-border access to electronic evidence, its political rationale is rooted in the idea that digital criminality and cybercrime require faster, more direct channels of cooperation that reduce dependence on slower mutual legal assistance processes. From a governance perspective, this instrument illustrates how the EU seeks to reconfigure the practical conditions of enforcement in response to digitalisation, and how cross-border data access becomes a central site where security, sovereignty, and rights-sensitive governance intersect.

4.5 Cybercrime, Hybrid Threat Narratives and Institutional Role ExpansionEnforcement

A further dimension of EU discourse is the tendency to situate cybercrime within a broader landscape of hybrid threats, sabotage, and hostile influence. This is politically consequential because it blurs the boundary between "crime" and "security" in the stronger sense, allowing cybercrime to be linked to geopolitical contestation and systemic destabilisation. This, in turn, supports arguments for expanding the mandates and operational roles of EU agencies and for strengthening EU-level internal security capacities.

Taken together, strategic and legal developments indicate that the EU's approach to cybercrime is constructed through an interplay of securitising narratives and governance instruments. Cybercrime is framed as a cross-border security problem requiring coordinated European action; resilience is institutionalised through regulatory obligations; and enforcement capacity is enhanced through cross-border evidence tools and institutional strengthening (Karathanasis, 2024). In political science terms, this produces a distinctly EU-style model of cyber threat governance in which security is achieved through a combination of integration, regulation, and capability-building – a model that can be contrasted with the Council of Europe's more explicitly normative approach in the next section.

5 THE COUNCIL OF EUROPE: NORMATIVE SECURITY AND CYBERCRIME

The Council of Europe's approach to cybercrime is anchored in a distinctive model of European security politics in which "security" is articulated through norms, standards, and rights-sensitive governance. Unlike the European Union, which often frames cybercrime through the lens of a Security Union logic and capability-driven security governance, the

Council of Europe tends to construct cybercrime as a challenge to democratic order and fundamental rights that must be addressed through legally and institutionally constrained cooperation. In political terms, the Council of Europe's cybercrime agenda exemplifies "normative security", that is, a security practice premised on the diffusion of common standards, the consolidation of rule-of-law commitments, and the management of cross-border threats through treaty-based cooperation rather than supranational authority.

5.1 The Budapest Convention as a Normative Infrastructure of Cybercrime Governance

The Council of Europe's central contribution to cybercrime governance is the *Convention on Cybercrime*[9] of 2001 (also known as the Budapest Convention). As a treaty-based instrument, it has long functioned as a normative infrastructure that shapes how cybercrime is defined, discussed, and governed across Europe and beyond (Carr, 2009; Funta, 2021). The Convention's political significance lies not only in its substantive catalogue of cyber-related offences and procedural tools, but also in its underlying governance rationale: it frames cybercrime as a transnational threat that requires rapid and effective international cooperation, while situating that cooperation within a framework compatible with rule-of-law standards. From a political science perspective, this treaty-based approach produces a specific form of authority. Rather than centralising enforcement powers, the Council of Europe stabilises cooperation by promoting a shared baseline of expectations and practices among states. Cybercrime, in this model, becomes a policy domain where legitimacy is generated through common standards and mutual trust, rather than through institutional capacity at a supranational level. The Convention thereby contributes to the construction of cybercrime as a governance problem that is solved through harmonised norms, coordinated procedures, and institutionalised cooperation.

The *Second Additional Protocol to the Cybercrime Convention*[10] further illustrates how the Council of Europe responds to digital threats by adapting normative instruments to the realities of platform-driven communication

[9] Convention on Cybercrime, Council of Europe, ETS No. 185. Available at: https://rm.coe.int/1680081561 (Accessed: 5 February 2026).

[10] Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence, Council of Europe, ETS No. 224. Available at: https://rm.coe.int/1680a49dab (Accessed: 5 February 2026).

and cross-border data. Politically, the Protocol can be read as an attempt to reconcile two pressures that define contemporary cybercrime governance: the demand for faster and more direct forms of international cooperation in obtaining electronic evidence, and the demand for credible safeguards grounded in human rights and data protection standards. The Council of Europe explicitly presents the Protocol as providing tools for enhanced cooperation, including forms of direct cooperation with service providers, while simultaneously emphasising the embedding of these tools within a safeguards framework.

The Protocol's drafting history is also politically revealing. The Council of Europe highlights the prolonged and consultation-intensive nature of the negotiation process, signalling an effort to build legitimacy through procedure, stakeholder engagement, and deliberation. In political science terms, this can be interpreted as a throughput legitimacy strategy: the Council of Europe seeks to defend the acceptability of more intrusive cooperation tools by demonstrating that their design emerged from a constrained and participatory process rather than from executive urgency alone.

5.2 Human Rights, Rule-of-Law Framing and Normative Constraints

A further distinguishing feature of the Council of Europe's cybercrime agenda is its consistent integration of human rights concerns into its broader approach to digital governance. While cybercrime governance often tends towards securitising dynamics that normalise exceptional measures, the Council of Europe's normative ecosystem provides discursive and institutional resources that can constrain such dynamics. The Committee of Ministers' *Recommendation on the roles and responsibilities of internet intermediaries*[11] of 2018 exemplifies how the Council of Europe frames digital governance through an explicit human rights lens, insisting that regulatory and policy measures in the digital environment should effectively safeguard rights and maintain guarantees against arbitrary application.

In the context of cybercrime, this rights-oriented framing has an important political implication: it reshapes what can be presented as legitimate policy action. Rather than treating effectiveness and speed as overriding imperatives, the Council of Europe's discourse keeps open the normative question of proportionality, safeguards, and accountability. This does not

[11] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, Council of Europe, CM/Rec(2018)2. Available at: https://rm.coe.int/0900001680790e14 (Accessed: 5 February 2026).

eliminate securitisation dynamics, but it alters the justificatory terrain in which cybercrime policies are debated, designed, and implemented.

5.3 Capacity Building and the Externalisation of European Cybercrime Governance

The Council of Europe's cybercrime activities also demonstrate how European security governance increasingly extends beyond Europe in practice, even when it remains normatively anchored in European legal and political standards. Through the work of the *Cybercrime Programme Office of the Council of Europe* (also known as C-PROC) and its associated initiatives, the Council of Europe has positioned itself as a key global actor in the governance of cybercrime. Capacity-building programmes such as GLACY+ and related regional projects illustrate how the Council's cybercrime agenda operates well beyond the geographical boundaries of its membership, targeting regions including Africa, Latin America, the Asia-Pacific and Eastern Europe. These initiatives focus on strengthening legislative frameworks, enhancing institutional capacity, and improving international cooperation mechanisms in line with the standards of the Budapest Convention system.

From a political perspective, this outward-oriented capacity-building strategy is highly significant because it frames cybercrime governance primarily as a process of institutional development and norm socialisation rather than as a matter of coercive enforcement. By emphasising training, technical assistance, legislative alignment and peer-to-peer cooperation, the Council of Europe promotes a model of security governance that relies on persuasion, expertise and shared standards. Cybercrime is thus constructed not only as a threat to be countered, but as a governance challenge that can be addressed through the diffusion of best practices and the gradual internalisation of normative frameworks.

This approach reinforces the Council of Europe's identity as a standards-setting organisation whose influence is exercised through knowledge production, treaty-based cooperation and sustained engagement with domestic institutions in partner countries. Unlike security actors that derive authority from operational capacity or enforcement power, the Council of Europe builds legitimacy by presenting its cybercrime framework as compatible with the rule of law, human rights and democratic accountability. In doing so, it seeks to stabilise a particular understanding of legitimate cybercrime governance that balances effectiveness with normative restraint.

These activities can be understood as a form of external governance. European norms related to cybercrime, electronic evidence and procedural safeguards are translated into templates that are adopted, adapted and localised in diverse political and institutional contexts. This externalisation of European cybercrime standards contributes to the construction of a broader transnational governance space in which European security norms exert influence without formal supranational authority. As such, the Council of Europe's cybercrime activities illustrate how security governance in the digital domain increasingly operates through normative projection and capacity-building, complementing the more integration-driven and regulatory approaches characteristic of the European Union.

6 COMPARATIVE DISCUSSION: TWO MODELS OF SECURITISING CYBERCRIME IN EUROPE

The preceding analysis has demonstrated that both the European Union and the Council of Europe treat cybercrime as a security-relevant phenomenon that necessitates coordinated responses extending beyond the capacities of individual states. In both institutional settings, cybercrime is framed as transnational, complex and capable of generating systemic harm, thereby justifying governance arrangements that operate across borders and policy sectors. This shared framing reflects a common European threat environment shaped by digitalisation, interdependence and the growing reliance of societies on networked infrastructures. In securitisation terms, both organisations participate in the construction of cybercrime as an urgent and exceptional problem, even though the intensity and form of that exceptionalism differ significantly.

Despite this shared threat narrative, the two organisations securitise cybercrime through distinct political and institutional logics. The European Union's approach is grounded in an integration-oriented model of security governance in which cybercrime is positioned as a policy problem requiring supranational coordination, regulatory harmonisation and the strengthening of European-level capacities. Cybercrime is discursively mobilised to support the expansion of EU action in areas traditionally associated with state sovereignty, particularly internal security and criminal justice (Klimek – Záhora – Holcr, 2016). In this model, securitisation operates as a mechanism that legitimises deeper integration and the consolidation of EU authority through regulatory and operational instruments.

By contrast, the Council of Europe's approach is rooted in a treaty-based and norm-driven model of governance. Cybercrime is framed as a serious challenge to democratic order and the rule of law, but the preferred response emphasises convergence around shared standards rather than the centralisation of enforcement powers. The Council of Europe securitises cybercrime in a manner that foregrounds legal certainty, procedural safeguards and compatibility with human rights obligations. In political terms, this produces a form of securitisation that seeks to contain security imperatives within a normative framework designed to preserve institutional restraint and legitimacy.

These divergent approaches are also reflected in the legitimising strategies employed by each organisation. The European Union tends to rely primarily on output-oriented legitimacy, presenting its cybercrime policies as necessary to deliver effectiveness, resilience and operational capability in the face of cross-border digital threats (Fahey, 2016; Fahey 2022). The promise of efficiency and coordinated action serves as a central justificatory narrative for expanding EU involvement in cyber security governance. Where concerns about democratic accountability arise, they are often addressed through references to necessity, urgency and the technical complexity of digital threats.

The Council of Europe, by contrast, places greater emphasis on throughput legitimacy and rights-sensitive governance. Its cybercrime discourse consistently highlights the importance of inclusive procedures, deliberation and safeguards as sources of legitimacy. Rather than framing security effectiveness as the overriding value, the Council of Europe's approach insists that cybercrime governance must remain embedded in rule-of-law commitments and subject to normative constraints. This does not eliminate securitisation dynamics, but it reshapes the political conditions under which security measures can be justified and accepted.

A particularly revealing point of comparison concerns the politics of cross-border access to electronic evidence and the role of private actors. In both models, cybercrime governance increasingly depends on cooperation with service providers and technology companies, reflecting the centrality of private infrastructure in the digital environment. The European Union approaches this challenge through mechanisms designed to accelerate and standardise cooperation, emphasising operational effectiveness and the reduction of procedural barriers. The Council of Europe similarly seeks to enhance cooperation but places stronger discursive emphasis on safeguards, proportionality and compatibility with human rights standards.

This difference highlights how similar governance problems are addressed through distinct normative vocabularies and institutional strategies.

Taken together, these contrasting approaches suggest that European security politics in the digital domain is characterised by institutional pluralism rather than convergence around a single security model. Cybercrime governance emerges from the interaction of integration-driven and norm-driven securitisation processes, each shaping how threats are understood, managed and legitimised. This underscores that Europe cannot be treated as a unitary security actor; instead, it is a fragmented yet interconnected security space in which multiple institutions contribute to the construction of digital threats and responses. The comparison illustrates that securitisation is not a uniform or deterministic process, but one that is deeply shaped by institutional design, authority structures and legitimising practices. Cybercrime thus provides a particularly instructive case for analysing how security governance evolves under conditions of digital interdependence and how European institutions navigate the tension between security imperatives and democratic legitimacy.

CONCLUSION

The article examines how cybercrime is constructed and governed as a security issue within the European political space, focusing on the European Union and the Council of Europe as two central, yet distinct, institutional actors. Drawing on securitisation theory, the analysis has shown that cybercrime does not enter European security policy merely as a response to technological change or rising criminal activity, but as the outcome of political processes through which digital threats are framed as systemic risks requiring coordinated intervention beyond the nation-state.

The European Union and the Council of Europe securitise cybercrime through different, though partially overlapping, governance logics. The EU predominantly advances an integration-oriented model of securitisation, in which cybercrime is embedded within a broader Security Union agenda and addressed through regulatory harmonisation, resilience-building and sector-specific governance instruments. In contrast, the Council of Europe promotes a norm-driven model centred on treaty-based cooperation, human rights safeguards and the diffusion of common standards, extending its influence through capacity-building and external governance rather than supranational authority. These divergent approaches reveal that European security governance in the digital domain is characterised by institutional

pluralism rather than convergence around a single security paradigm.

By framing cybercrime as a transnational and cascading risk, European institutions justify preventive, managerial and regulatory forms of intervention that reshape the boundaries between security, regulation and rights. At the same time, the comparison underscores the importance of legitimacy strategies, showing how different institutional designs produce distinct balances between effectiveness, accountability and normative restraint. Cybercrime offers a revealing case for understanding broader transformations in European security politics under conditions of digital interdependence.

REFERENCES

Balzacq, T. (2010) Securitization Theory: How Security Problems Emerge and Dissolve. London and New York: Taylor & Francis. ISBN: 9781135246143.

Bhushan, M. & Jamshed, A. (2025) Cybercrime and Digital Security: Understanding threats, attacks, and defenses in the connected world. New Delhi: BPB Publications. ISBN: 978-93-6589-582-7.

Biscop, S. (2016) The European Security Strategy: A Global Agenda for Positive Power. London and New York: Taylor & Francis. ISBN: 9781351890236.

Carr, I. (2009) Computer Crime. London: Routledge. ISBN: 9780754628354.

Chiara, P.G. (2024) The Internet of Things and EU Law: Cybersecurity, Privacy and Data Protection Challenges. Cham: Springer Nature Switzerland. ISBN: 9783031676635.

Durand, P. & Gilbert-d'Halluin, A. (2024) Directive (EU) 2022/2464 as Regards Corporate Sustainability Reporting (CSRD): Texts and Comments. London: Larcier-Intersentia. ISBN: 9781839704574.

Fahey, E. (2016) The Global Reach of EU Law. London and New York: Taylor & Francis. ISBN: 9781315524085.

Fahey, E. (2022) The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity. London: Bloomsbury Publishing. ISBN: 9781509957064.

Floyd, R. (2019) The Morality of Security: A Theory of Just Securitization. Cambridge: Cambridge University Press. ISBN: 978-1108493895.

Funta, R. (2021) Komentár k Dohovoru Rady Európy o počítačovej kriminalite (Budapeštiansky dohovor). Bratislava: Wolters Kluwer. ISBN: 978-80-571-0365-3.

Galbreath, D.J., Mawdsley, J. & Chappell, L. (2019) Contemporary European Security. London and New York: Taylor & Francis. ISBN: 9781351235617.
Herlin-Karnell, E., Conway, G. & Ganesh, A. (2021) European Union Law in Context. London: Bloomsbury Publishing. ISBN: 9781509901401.
Karathanasis, T. (2024) Cybersecurity and EU Law: Adopting the Network and Information Security Directive. London: Taylor & Francis. ISBN: 9781040229682.
Kaunert, C. & Léonard, S. (2013) European Security Governance and the European Neighbourhood after the Lisbon Treaty. London and New York: Taylor & Francis. ISBN: 9781135740443.
Klimek, L., Záhora, J. & Holcr, K. (2016) Počítačová kriminalita v európskych súvislostiach. Bratislava: Wolters Kluwer. ISBN: 978-80-8168-538-5.
Pilniok, A. & Dietrich, J.-H. (2024) European Security Union: Law and Policies. Munich: C.H. Beck. ISBN: 9783406833441.
Porcedda, M.G. (2023) Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis. London: Bloomsbury Publishing. ISBN: 9781509939404.
Rüdiger, T.-G. & Bayerl, P.S. (2020) Cyberkriminologie: Kriminologie für das digitale Zeitalter. Wiesbaden: Springer VS. ISBN: 978-3-658-28506-7.
Stephenson, P. & Gilbert, K. (2004) Investigating Computer-Related Crime. 2nd edn. London: Taylor & Francis. ISBN: 9780849319730.
Wernert, M. (2021) Internetkriminalität: Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen. Stuttgart: Richard Boorberg Verlag. ISBN: 9783415068919.

ACKNOWLEDGEMENT

The contribution was elaborated as a part of the research project VEGA No. 1/0100/24 ‘Implementation of European Crimes into the Legal Order of the Slovak Republic’ [Slovak: Zavedenie európskych trestných činov do právneho poriadku Slovenskej republiky].