High-risk cybercriminal networks: Strategies for combating them in cyberspace

Alp Cenk Arslan

https://doi.org/10.3013/g3vn9q76

Abstract

As cybercriminal networks grow increasingly complex and globalised, traditional cybersecurity measures struggle to address these sophisticated threats. This study examines the structures and strategies of high-risk cybercriminal networks, focusing on their technological, geopolitical and operational dynamics. Methodologically, the study employs a qualitative comparative analysis framework, utilising a 'most different systems design' to evaluate the strategic divergence between the United States and the European Union. The research contributes to the literature by establishing a theoretical nexus between 'state–cybercrime alignment' and current geopolitical security doctrines. Drawing on the US national cybersecurity strategy and the EU cybersecurity strategy, the research analyses their approaches to combating such networks and fostering international cooperation. Case studies of cyberattacks originating from China, North Korea and Russia highlight the global connections and state-sponsored elements of these networks. The study proposes an integrated framework combining advanced technologies and international collaboration to disrupt, predict and mitigate cybercriminal activities. Additionally, it underscores the importance of harmonised global laws and inter-agency partnerships to address jurisdictional and technological challenges. By comparing the US and EU strategies, this research provides policymakers and cybersecurity professionals with actionable insights and recommendations to navigate the evolving threat landscape and promote a secure digital ecosystem.

Keywords: high-risk cybercriminal networks, international cooperation, US cyber strategy, EU cyber strategy, cybersecurity, security strategies.

Introduction

High-risk cybercriminal networks represent one of the most formidable challenges to global cybersecurity in the digital age. These networks, often characterised by their sophistication, international reach and adaptability, pose significant threats to critical infrastructure, economic stability and national security. As technological advancements continue to evolve, so do the methods and tools employed by cybercriminals, making traditional cybersecurity measures increasingly inadequate. The nexus between cybercrime, geopolitical ambitions and state sponsorship further complicates the landscape, blurring the lines between criminal and strategic motives. Nations such as China, North Korea and Russia have been implicated in fostering or tolerating such activities, leveraging cybercrime for both financial gain and strategic advantage.

This study aims to explore the complex dynamics of high-risk cybercriminal networks and examine the strategic responses outlined in the cybersecurity frameworks of the United States and the European Union. By analysing the US national cybersecurity strategy (2023) and the EU cybersecurity strategy for the Digital Decade (2020), the study seeks to understand the underlying intentions, mechanisms and collaborative approaches adopted by these actors to combat cyber threats. Particular attention is paid to international cooperation, given the transnational nature of cybercrime and the challenges posed by jurisdictional boundaries.

This article makes three concrete contributions. First, it proposes a typology of the state–cybercrime nexus (state-operated, state-enabled and state-tolerated) tailored to high-risk cybercriminal networks. Second, it operationalises this typology through a qualitative comparative analysis and structured documentary coding to compare the United States' and the EU's strategic responses across three analytic nodes: operational disruption, regulatory resilience and diplomatic attribution. Third, it distils these findings into actionable implications for European law enforcement, particularly for cross-border investigations, evidence production and disruption coordination with the European Union Agency for Law Enforcement Cooperation (Europol) European Cybercrime Centre (EC3) and national cybercrime units.

The research also evaluates the operational and strategic advancements in cybersecurity, focusing on emerging technologies such as AI and quantum computing, and the frameworks designed to counteract their exploitation by cybercriminals. Additionally, the study highlights the importance of harmonising legal frameworks, strengthening public–private partnerships and fostering international collaboration to mitigate the risks posed by these networks. Despite the abundance of policy reports, scholarly literature lacks a systematic comparison of how transatlantic security architectures adapt to the industrialisation of cybercrime. This study addresses this gap by answering three core research questions (RQs). RQ1: How do the United States and the EU conceptualise the state–cybercrime nexus within their national security priorities? RQ2: To what extent do offensive strategies (United States) versus regulatory harmonisation (EU) provide more effective deterrence against high-risk networks? RQ3: What are the structural barriers to achieving a unified transatlantic response to state-sponsored cybercriminal activities? To address these questions, the study moves beyond a narrative comparison by specifying conditions and outcomes, thereby enabling a replicable assessment of strategic divergence. The practical focus is on how EU law enforcement can reduce jurisdictional 'grey zones' exploited by state-aligned networks. This work aims to provide policymakers, cybersecurity professionals and academics with actionable insights and strategies to address the evolving threat landscape effectively, while promoting a secure and resilient digital ecosystem.

Methodology

This research utilises a qualitative comparative analysis and documentary research methodology. Three primary archetypes of high-risk networks (China, North Korea and Russia) were selected based on the 'most similar' and 'most different' case criteria. These cases represent the full spectrum of the state–cybercrime nexus, from direct state-operated units (Lazarus) to state-tolerated syndicates (Russian ransomware). The study analyses the US national cybersecurity strategy (2023) and the EU cybersecurity strategy (2020) using three thematic coding nodes: (1) operational disruption; (2) regulatory resilience; and (3) diplomatic attribution. Analysis is derived from primary legal documents, threat intelligence reports (2020–2024) and peer-reviewed security studies. The study acknowledges the limitations of using open-source intelligence, mitigating this by triangulating government reports with academic security discourse.

Theoretical framework: the industrialisation of cybercrime

High-risk cybercriminal networks are deeply intertwined with technological innovation, geopolitical motivations and criminal enterprise, creating a complex challenge for cybersecurity and law enforcement. These networks operate with industrialised processes that mirror corporate structures, characterised by specialisation, scalability and coordination (Luo, 2024). For instance, specialised teams handle malware development and phishing, while ransomware as a service enables global scalability (Meland et al., 2020). Collaboration through Dark Web forums further enhances their adaptability and resilience.

To understand high-risk networks, this study applies 'network governance theory' and 'routine activity theory' (RAT) adapted for digital spaces. These frameworks suggest that the convergence of 'motivated offenders' (cybercriminals), 'suitable targets' (critical infrastructure) and the 'absence of capable guardians' (jurisdictional gaps) creates the current techno-political threat environment. This lens directs attention to network chokepoints (infrastructure, financing and coordination layers) as the most disruptive intervention targets (Jones et al., 1997). Complementarily, RAT (Cohen et al., 1979) informs the comparative reading of US and EU strategies by mapping policy instruments onto the 'capable guardianship' function, such as mandatory reporting, public–private operational integration, certification regimes and financial disruption measures. Together, these frameworks explain why state-aligned networks exploit jurisdictional gaps and why a strategic divergence between disruption-oriented and regulation-oriented approaches produces persistent transatlantic grey zones.

State sponsorship significantly amplifies the threat posed by these networks. Countries like China, North Korea and Russia use cybercriminals for both financial gain and geopolitical strategy. North Korea's Lazarus Group exemplifies this dual purpose, conducting operations such as the USD 625 million Axie Infinity heist to finance nuclear ambitions. These actors also use cryptocurrency mixers to launder stolen funds, leveraging anonymity-enhancing technologies to obscure their tracks (O'Neill, 2024; Tidy, 2024).

Chinese networks, like the Vigorish Viper syndicate, operate at both the organisational and individual levels, targeting industries such as gambling and intellectual property theft (Lakshmanan, 2024). Innovative methods, such as Domain Name System (DNS) Canonical Name (CNAME) traffic distribution, and the use of underregulated regions like Zambian call centres, highlight the industrialisation of Chinese cybercrime (Muia, 2024).

Russian cybercriminals benefit from state protection, integrating ransomware operations into geopolitical strategies. Investigations like Operation Destabilise have exposed money-laundering networks linked to drug trafficking, ransomware and espionage (National Crime Agency, 2024). Russian actors have also targeted critical infrastructure and political systems, exemplified by interference in Ukrainian military systems and in US elections (Klepper, 2024; Euronews, 2024).

Technological advancements further complicate the landscape. Tools like AI and encrypted communication enhance operational capacity, while cryptocurrencies facilitate financial transactions. These dynamics underline the urgent need for international cooperation and robust strategies to combat the global nature of high-risk cybercrime (Leukfeldt et al., 2017).

Analysis of the United States and European Union cybersecurity strategies

From a network governance perspective, high-risk cybercriminal activity is best understood not as a series of isolated operations but as a coordinated ecosystem of interdependent actors, including malware developers, access brokers, hosting providers, money launderers and state-linked facilitators. This lens highlights why strategies that focus solely on individual threat actors often fail to generate sustained disruption. Instead, effective intervention depends on identifying and targeting network-level chokepoints, particularly those enabling coordination, financing and scalability. This perspective provides an analytical foundation for assessing how the US and EU strategies conceptualise and intervene in cybercriminal ecosystems rather than in discrete incidents.

The United States national cybersecurity strategy

The US national cybersecurity strategy released in March 2023 outlines a multifaceted approach to addressing high-risk cybercriminal networks. Its intentions and strategies in this domain aim to strengthen national security by protecting critical infrastructure and sensitive data from increasingly sophisticated and damaging cybercriminal activities. High-risk cybercriminal networks, such as those engaging in ransomware, are recognised as threats to national security and economic stability. The United States seeks to lead globally in establishing norms of responsible state behaviours in cyberspace while holding states and actors accountable for cyber misconduct. By disrupting cybercriminal networks, the United States aims to safeguard not only its interests but also those of its allies, projecting global leadership. A key goal is to leverage public–private partnerships for intelligence sharing and operational collaboration to effectively dismantle threat actors. Building resilience into the digital ecosystem is a foundational objective, ensuring systems are defensible and that attacks have limited impact (The White House, 2023, p. 23).

The strategy emphasises disrupting and dismantling threat actors through integrated federal efforts. Federal agencies, led by the Department of Justice and supported by entities like the Cybersecurity Infrastructure Security Agency and the National Security Agency, coordinate campaigns targeting cybercriminal infrastructure such as botnets and ransomware servers (The White House, 2023, p. 14). The Department of Defense employs a 'defend forward' strategy to neutralise threats before they materialise (The White House, 2023, p. 14). Recognising that private companies often have better visibility into cybercriminal activities, the strategy calls for closer collaboration with private entities for threat intelligence. Rapid response cells, such as those within the National Cyber-Forensics and Training Alliance, are tasked with responding to active threats in real time.

Interpreted through a network governance lens, the United States' emphasis on persistent engagement and defend-forward operations reflects an effort to destabilise the coordination mechanisms of cybercriminal networks rather than merely neutralising individual nodes. By targeting infrastructure, financial intermediaries and communication channels, the US strategy seeks to increase systemic friction across the network, thereby raising operational costs and reducing regenerative capacity. This approach aligns with governance-based disruption logic, where weakening connective tissue is prioritised over episodic actor removal.

Specific actions against ransomware include applying economic pressure by targeting cryptocurrency platforms used for laundering funds. The Counter Ransomware Initiative, an international coalition of over 30 countries, shares intelligence and disrupts ransomware campaigns globally. Legal and regulatory measures, such as enhancing the security of cloud services and mandating critical infrastructure entities to report cyber incidents, strengthen the broader cybersecurity framework. The strategy also prioritises intelligence sharing through automated, real-time data exchange and enhanced declassification policies to facilitate actionable intelligence sharing with private entities (The White House, 2023, p. 30).

Global partnerships are a central element of the strategy, with alliances such as the North Atlantic Treaty Organization (NATO) and the Quadrilateral Security Dialogue (the Quad) playing critical roles in addressing transnational cyber threats. Collaborative efforts with organisations like Europol's EC3 strengthen cross-border law enforcement. These international coalitions are designed to address shared cybersecurity challenges and hold malicious actors accountable (The White House, 2023, p. 1).

The strategy reflects a proactive, deterrent and collaborative approach to cybersecurity. It emphasises shifting the burden of cybersecurity from individual end users and small organisations to more capable actors, such as infrastructure operators and technology providers, promoting long-term resilience and equitable risk distribution (The White House, 2023, p. 30). The multilayered defence mechanism combines technological innovation, such as zero trust architecture, with operational coordination. The focus on sustained disruption campaigns signifies a shift from reactive to persistent offensive actions against cybercriminals, aiming to make cybercrime economically unviable (The White House, 2023, p. 14). The integration of international law, sanctions and diplomatic tools to isolate and penalise states that harbour cybercriminals highlights a comprehensive geopolitical strategy.

However, the strategy also faces challenges, including overcoming implementation barriers such as bureaucratic inertia, the complexity of public–private collaboration and the evolving tactics of cybercriminals. Balancing national security measures with civil liberties will be critical in maintaining public trust (The White House, 2023, p. 26). Despite these challenges, the 2023 US national cybersecurity strategy represents a robust framework for combating high-risk cybercriminal networks. By integrating technical innovation, policy reforms and international cooperation, the strategy seeks to create a digital ecosystem where cyberattacks are both costly and less impactful.

The European Union cybersecurity strategy for the Digital Decade

The EU cybersecurity strategy for the Digital Decade, dating from December 2020, addresses high-risk cybercriminal networks through an integrated framework encompassing resilience-building, operational capacity, international cooperation and technological leadership. The strategy aims to enhance cyber resilience by building robust defences

for critical infrastructures and digital services, ensuring they are secure by design (European Commission, 2020, p. 5). The revised directive on the security of network and information systems (NIS2 Directive) plays a crucial role in harmonising regulatory frameworks to strengthen the cyber resilience of key sectors such as energy, healthcare and finance. It also emphasises operational preparedness by establishing mechanisms like the Joint Cyber Unit to detect, prevent and respond to large-scale cyber incidents through cross-border and cross-sector collaboration.

From a RAT perspective, the EU strategy primarily seeks to strengthen the 'capable guardianship' component of the cybercrime equation. Regulatory harmonisation, mandatory incident reporting, certification frameworks and sectoral resilience measures are designed to reduce target suitability and increase guardianship density across critical infrastructures. Rather than directly confronting motivated offenders, the EU approach aims to structurally constrain opportunity spaces by embedding security obligations throughout the digital ecosystem.

The strategy seeks to deter malicious cyber activities and hold perpetrators accountable by integrating law enforcement, judicial cooperation and diplomatic tools. This includes improving digital investigations, evidence gathering and partnerships with Europol and the European Union Agency for Cybersecurity (ENISA). International cooperation is a key element in recognising the global nature of cyber threats and promoting responsible state behaviours and global norms. The strategy prioritises technological sovereignty to reduce dependency on non-EU suppliers, emphasising investment in cybersecurity technologies like AI, quantum computing and 5G infrastructure (European Commission, 2020, p. 8).

The strategy employs regulatory frameworks, including the NIS2 Directive, to enforce strict security requirements on critical sectors and strengthen incident reporting obligations. The Cybersecurity Act introduces a European cybersecurity certification framework to ensure stringent security standards for digital products and services. To build operational capacity, initiatives like the Joint Cyber Unit promote real-time information sharing among national computer security incident response teams, law enforcement and private stakeholders. AI-enabled security operations centres enhance threat detection and response capabilities (European Commission, 2020, pp. 6–13).

Cooperation between Europol and ENISA enhances law enforcement's ability to investigate cybercrime, including Dark Web marketplaces and ransomware attacks (European Commission, 2020, p. 10). The e-evidence framework facilitates cross-border access to electronic evidence, critical for prosecuting cybercriminal networks. Financial and technological investment through programmes like Horizon Europe and digital Europe fund research and development for advanced cybersecurity solutions and capacity building, particularly for small and medium-sized enterprises, which are often targeted by cybercriminals. The strategy also addresses supply chain vulnerabilities and ensures the resilience of emerging technologies like 5G and quantum communication (European Commission, 2020, p. 7).

Global cyber diplomacy plays a significant role in the strategy, with the EU promoting frameworks like the Budapest Convention on Cybercrime and using the Cyber Diplomacy Toolbox to impose sanctions against entities responsible for cyberattacks. The EU advocates for its values in international standardisation processes to prevent the proliferation of insecure technologies. Public–private partnerships are encouraged, with information sharing and analysis centres facilitating intelligence sharing and collaboration. Small and medium-sized enterprises receive tools and training to strengthen their cyber defences (European Commission, 2020, p. 7).

Despite its comprehensive approach, the strategy faces challenges. Fragmented implementation across EU Member States could hinder a unified response to high-risk cybercriminal networks. The effective attribution of cyberattacks remains difficult, particularly with respect to state-sponsored actors. Rapid technological advancements like deepfakes and AI-generated cyber tools necessitate constant adaptation of strategies. Additionally, the shortage of skilled cybersecurity professionals poses a barrier to effective implementation.

The EU cybersecurity strategy for the Digital Decade demonstrates a thorough approach to combating high-risk cybercriminal networks by integrating regulatory measures, operational frameworks, international cooperation and technological investment. Its success will depend on consistent implementation across Member States, effective public–private collaboration, and the ability to address emerging threats. This strategy positions the EU as a global leader in cybercrime prevention while ensuring economic, social and political stability.

Findings and comparative analysis: the European Union cybersecurity strategy versus the United States national cybersecurity strategy

The comparative analysis reveals a clear divergence in the strategic orientation underpinning the US and EU cybersecurity frameworks when confronting high-risk cybercriminal networks. The US national cybersecurity strategy is fundamentally oriented toward operational disruption and cost imposition, reflecting a security logic that treats cybercriminal infrastructures as active battlefields. Within this approach, cybercrime is framed not merely as a law enforcement issue but as a national security threat requiring persistent engagement. As a result, the US strategy normalises proactive interventions against adversary infrastructure, including pre-emptive actions designed to degrade capabilities before attacks materialise. By contrast, the EU cybersecurity strategy prioritises regulatory resilience and harmonised governance mechanisms, positioning cybersecurity as a systemic risk management challenge. The EU approach focuses on ensuring that critical sectors, digital services and supply chains are resilient by design, emphasising uniform standards, compliance obligations and coordinated preparedness across Member States. This divergence reflects deeper differences in strategic culture: the US privileges deterrence through disruption, while the EU privileges stability through institutional harmonisation.

When read jointly through network governance theory and RAT, the strategic divergence between the US and EU becomes analytically clearer. The US model prioritises network disruption by targeting coordination and enablement layers, whereas the EU model prioritises guardianship by reducing systemic vulnerability and opportunity structures. This divergence explains why both strategies generate partial effectiveness while simultaneously leaving jurisdictional and operational grey zones that high-risk networks continue to exploit.

These contrasting orientations are further reflected in the instruments each of them deploys to counter high-risk cybercriminal activity. The US strategy explicitly institutionalises persistent operational campaigns against adversarial networks, integrating intelligence, law enforcement and military capabilities to dismantle botnets, ransomware infrastructure and financial enablers. Offensive cyber operations, economic sanctions and coordinated takedowns are treated as complementary tools within a single disruption ecosystem. In the EU framework, however, the emphasis shifts toward coordinated preparedness, incident response and post-incident management. Mechanisms such as certification schemes, sector-specific security requirements and cross-border incident handling are designed to reduce systemic vulnerability rather than to actively pursue adversaries in cyberspace. While these measures

significantly enhance resilience, they tend to operate reactively, engaging once an incident has occurred rather than shaping the threat environment upstream.

Attribution practices constitute another area of convergence in principle but are divergent in execution. Both the United States and the EU recognise attribution as essential for accountability and deterrence, yet they embed it within different consequence structures. The US strategy more directly links attribution to operational and economic consequences, including sanctions, indictments, asset seizures and follow-on cyber operations. Attribution thus functions as a trigger for action, enabling rapid escalation across legal, financial and cyber domains. In contrast, the EU embeds attribution within a broader framework of diplomatic coordination and collective response, most notably through the Cyber Diplomacy Toolbox. Here, attribution serves to build consensus among Member States and partners before sanctions or diplomatic measures are applied. While this approach enhances legitimacy and unity, it can also introduce delays that reduce the immediacy of deterrent effects, particularly against agile and state-aligned cybercriminal networks.

A critical structural finding concerns the persistent exploitation of jurisdictional grey zones by high-risk cybercriminal networks. These actors consistently leverage the asymmetry between their rapid operational tempos and the comparatively slower legal, evidentiary and diplomatic processes governing transatlantic cooperation. Differences in legal thresholds, evidence standards and procedural timelines create enforcement gaps that criminal networks exploit to relocate infrastructure, launder proceeds and reconstitute operations before coordinated responses can be executed. This challenge is especially pronounced in cases involving state-aligned actors, where political sensitivities further complicate attribution and enforcement. The analysis suggests that these grey zones are not incidental but structural, arising from the misalignment between cyber operational speed and institutional response mechanisms. In RAT terms, these grey zones represent persistent gaps in capable guardianship across jurisdictions, enabling motivated offenders to operate transnationally with minimal disruption.

Finally, the comparative coding indicates that financial disruption tools, such as anti-money-laundering measures, cryptocurrency tracing and sanctions, are now widely adopted across both the US and EU strategies. However, their presence alone does not appear sufficient to achieve sustained disruption of high-risk networks. Instead, effective and durable disruption correlates with the conjunction of three conditions: a clearly articulated operational disruption doctrine, coordinated and credible attribution mechanisms and structured public–private operational integration. Where these elements reinforce one another, disruption efforts impose higher costs on adversaries and reduce their capacity to regenerate. Where they are absent or weakly coupled, enforcement efforts tend to remain episodic, allowing cybercriminal ecosystems to adapt and persist. This finding underscores the importance of integrated strategic design rather than isolated policy instruments in confronting industrialised, state-aligned cybercrime.

The EU cybersecurity strategy for the Digital Decade and the US national cybersecurity strategy of 2023 offer distinct approaches to addressing cybersecurity challenges, including high-risk cybercriminal networks. The EU strategy emphasises a comprehensive regulatory framework, digital sovereignty, resilience-building, cyber diplomacy and capacity building for Member States. Its advantages include the strong cybersecurity and data protection standards provided by the General Data Protection Regulation and the NIS2 Directive, a focus on reducing reliance on foreign technologies through initiatives like Gaia-X, and the promotion of responsible state behaviours via international norms. The strategy also prioritises resilience across critical infrastructures and digital services, emphasising

cybersecurity-by-design principles. However, it faces challenges such as implementation complexity due to disparities in Member State capabilities, a limited focus on offensive cyber capabilities and potential dependency risks associated with strict regulatory measures.

The US strategy takes a proactive and forward-looking approach, emphasising the need to prepare for emerging threats like quantum computing and AI vulnerabilities while employing offensive cyber operations to dismantle high-risk networks. It introduces a shared responsibility model, shifting the burden from individuals to large corporations and technology providers, and incentivises secure-by-design practices through liability measures. The strategy is supported by broad regulatory frameworks for critical infrastructure protection. Nevertheless, its reliance on the private sector may encounter resistance due to increased regulation, and fragmentation risks arise from the diversity of stakeholders across the federal, state and private sectors. Additionally, the strategy's occasional prioritisation of unilateral actions may alienate international partners.

In terms of targeting threat actors, the EU strategy focuses on state-sponsored threats, ransomware operators and transnational criminal networks, relying on defensive measures such as harmonised frameworks and the EU Cyber Diplomacy Toolbox for imposing sanctions and attributing attacks. The US strategy targets both state and non-state actors, leveraging offensive capabilities like the 'defend-forward' approach to neutralise threats proactively and employing economic and legal tools to impose consequences on cybercriminals.

International collaboration is a cornerstone of both strategies, but their approaches differ significantly. The EU strategy emphasises global cooperation through legal frameworks like the Budapest Convention on Cybercrime, which facilitates international coordination. It also prioritises norm-setting through partnerships with organisations like the United Nations and the Organization for Security and Cooperation in Europe while advocating for cybersecurity certification standards and regional cybersecurity hubs. Collaboration with NATO and capacity-building initiatives in developing countries are key components of its global approach. The US strategy, on the other hand, leverages multilateral initiatives like the Counter Ransomware Initiative and builds regional alliances through frameworks such as the Quad, Aukus (a trilateral security partnership between Australia, the United Kingdom and the United States) and the EU–US Trade and Technology Council. It focuses on countering the abuse of cryptocurrencies by cybercriminals through anti-money laundering and countering the financing of terrorism standards and fosters bilateral collaboration with allies like the United Kingdom and Israel for joint cyberdefence exercises.

The EU strategy employs legal instruments such as the NIS2 Directive to enforce uniform cybersecurity measures across Member States and uses cyber diplomacy tools like sanctions to coordinate EU-wide responses to cyberattacks. Public–private partnerships are encouraged through platforms like ENISA. The US strategy emphasises public–private operational models for disrupting adversaries, such as the Joint Cyber Defence Collaborative, and promotes real-time intelligence sharing between private entities and federal agencies. Offensive cyber operations are also integrated into its international collaboration efforts to dismantle high-risk networks.

Both strategies address emerging challenges in their own ways. The EU strategy focuses on building resilience by addressing supply chain vulnerabilities and promoting digital sovereignty while prioritising ethical AI and data privacy. Long-term capacity-building efforts aim to harmonise cybersecurity capabilities across Member States. The US strategy takes a forward-looking approach by preparing for quantum computing risks with quantum-resistant cryptography

and targeting ransomware ecosystems by addressing financial enablers and supply chains. It also places significant emphasis on securing critical infrastructure and emerging technologies like the internet of things (IoT) and AI.

While both strategies aim to strengthen cybersecurity and combat high-risk cybercriminal networks, their approaches reflect their respective political, economic and technological contexts. The EU strategy leans heavily on regulatory measures and harmonisation, focusing on resilience and sovereignty, whereas the US strategy adopts a proactive stance with offensive capabilities, public–private collaboration and a focus on emerging threats. Both face challenges in implementation, but their combined efforts contribute significantly to global cybersecurity advancements.

The analysis reveals a fundamental strategic divergence. While the US strategy is rooted in 'realist deterrence' (utilising offensive 'defend-forward' operations to raise costs for adversaries), the EU strategy leans towards 'institutional liberalism' (emphasising norm-setting and regulatory sovereignty). However, the findings suggest that the US model faces challenges in legitimacy and private sector compliance, whereas the EU model is hampered by the 'capability-expectations gap' among its Member States. This divergence explains why high-risk networks continue to exploit the jurisdictional 'grey zones' between these two major powers.

Table 21.1. Comparison of EU cybersecurity strategy and US national cybersecurity strategy

Aspect	EU cyber strategy	US cyber strategy
Advantages	Strong regulatory frameworks, emphasis on digital sovereignty, harmonised standards and proactive cyber diplomacy.	Forward-looking, offensive capabilities, shared responsibility, strong focus on market incentives and resilience.
Disadvantages	Implementation challenges, limited offensive measures and risk of innovation slowdown.	Over-reliance on the private sector, complex implementation and potential unilateralism.
International collaboration	Emphasises legal frameworks, norm-setting and capacity building through multilateral institutions.	Focuses on multilateral disruption campaigns, offensive collaboration and real-time intelligence sharing.
Emerging threats	Addresses supply chain risks, promotes digital sovereignty and focuses on AI ethics and resilience.	Prepares for quantum threats, targets ransomware ecosystems and emphasises IoT and AI security.

Source: Created by the author.

Conclusion

This study highlights the evolving complexities of high-risk cybercriminal networks and the critical need for comprehensive strategies to combat their growing threat. The comparison between the US National Cybersecurity Strategy (2023) and the EU cybersecurity strategy for the Digital Decade (2020) reveals distinct approaches shaped by differing political, technological and economic priorities. By combining network governance and routine activity perspectives, the study demonstrates that the sustainable disruption of high-risk cybercriminal networks requires both ecosystem-level intervention and the systematic strengthening of capable guardianship across jurisdictions.

The US strategy demonstrates a proactive stance, emphasising offensive cyber operations, public–private collaboration and the integration of emerging technologies to disrupt cybercriminal networks. By shifting the responsibility of cybersecurity from individuals to large corporations and infrastructure providers, the US promotes resilience while leveraging its global alliances to counter transnational threats. However, the strategy's reliance on private-sector cooperation and occasional unilateral actions could limit its global efficacy.

Conversely, the EU strategy focuses on building a robust regulatory framework, harmonising cybersecurity capabilities across Member States and advancing digital sovereignty. Its emphasis on defensive measures, norm-setting and international cooperation through legal frameworks like the Budapest Convention highlights a more collaborative and resilience-oriented approach. Nonetheless, challenges such as fragmented implementation and limited offensive capabilities may hinder its effectiveness against sophisticated and state-sponsored cybercriminal networks.

Both strategies underscore the importance of international collaboration, leveraging alliances such as NATO and multilateral initiatives like the Counter Ransomware Initiative to address global cybercrime. The study also identifies emerging technologies, such as AI, quantum computing and IoT, as both threats and opportunities in the fight against cybercrime, emphasising the need for continuous adaptation and innovation.

While the US and EU approaches differ in focus, their complementary strengths – offensive measures from the United States and robust regulation from the EU – offer valuable insights for a global framework to combat high-risk cybercriminal networks. A unified, cooperative effort combining offensive capabilities, regulatory harmonisation and technological innovation will be essential to navigating the increasingly complex landscape of cybercrime. This study provides a foundation for further research and policy development aimed at fostering a secure and resilient digital ecosystem worldwide.

Future research should focus on the impact of large language models on the automation of the cybercriminal life cycle. A significant limitation of this study is the rapid evolution of crypto-mixer technologies, which may bypass the current US and EU financial sanctions. Policymakers must move beyond static strategies towards a 'dynamic defence' model that integrates AI-driven attribution with real-time transatlantic intelligence sharing.

References

Cohen, L. E. and Felson, M. (1979), 'Social change and crime rate trends: A routine activity approach', *American Sociological Review*, Vol. 44, No 4, August, pp. 588–608, https://doi.org/10.2307/2094589.

Euronews (2024), 'Russia increasingly using cybercriminals to target adversaries, Microsoft says', Euronews, 16 October, https://www.euronews.com/next/2024/10/16/russia-increasingly-using-cybercriminals-to-target-adversaries-microsoft-says.

European Commission (2020), Joint Communication to the European Parliament and the Council – The EU's cybersecurity strategy for the Digital Decade, JOIN(2020) 18 final of 16 December, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018.

Felbab-Brown, V., Paz García, D. and Bajji, V. (2024), 'Chinese crime and geopolitics in 2024', Brookings, 29 January, https://www.brookings.edu/articles/chinese-crime-and-geopolitics-in-2024/.

Jones, C., Hesterly, W. S. and Borgatti, S. P. (1997), 'A general theory of network governance: Exchange conditions and social mechanisms', Academy of Management Review, Vol. 22, No 4, October, pp. 911–945, https://doi.org/10.2307/259249.

Klepper, D. (2024), 'Cyber criminals are increasingly helping Russia and China target the US and allies, Microsoft says', AP News, 15 October, https://apnews.com/article/microsoft-russia-china-iran-israel-cyberespionage-cyber-d3a22dd2dcea32615ac15ed4fb951541.

Lakshmanan, R. (2024), 'Experts uncover Chinese cybercrime network behind gambling and human trafficking', The Hacker News, 22 July, https://thehackernews.com/2024/07/experts-uncover-chinese-cybercrime.html.

Leukfeldt, E. R., de Poot, C. J., Verhoeven, M. A., Kleemans, E. R. and Lavorgna, A. (2017), 'Cybercriminal networks', in: Leukfeldt, E. R. (ed.), The Human Factor in Cybercrime and Cybersecurity: Research agenda, Eleven International Publishing, The Hague, pp. 33–42.

Luo, Q. (2024), 'Cybercrime as an industry: Examining the organisational structure of Chinese cybercrime', *Humanities and Social Sciences Communications*, Vol. 11, p. 1554. https://doi.org/10.1057/s41599-024-04042-w.

Meland, P. H., Bayoumy, Y. F. F. and Sindre, G. (2020), 'The ransomware-as-a-service economy within the darknet', *Computers and Security*, Vol. 92, February, 101762, https://doi.org/10.1016/j.cose.2020.101762.

Muia, W. (2024), 'Zambia uncovers "sophisticated" Chinese cybercrime syndicate', *BBC News*, 10 April, https://www.bbc.com/news/world-africa-68777137.

National Crime Agency (2024), 'Operation Destabilise: NCA disrupts multi-billion Russian money laundering networks with links to drugs, ransomware and espionage, resulting in 84 arrests', National Crime Agency, https://www.nationalcrimeagency.gov.uk/news/operation-destabilise-nca-disrupts-multi-billion-russian-money-laundering-networks-with-links-to-drugs-ransomware-and-espionage-resulting-in-84-arrests.

O'Neill, A. (2024), 'Countering North Korean cybercrime and its enablers', *Lawfare Media*, 2 May, https://www.lawfaremedia.org/article/countering-north-korean-cybercrime-and-its-enablers.

The White House (2023), *National Cybersecurity Strategy*, March, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Tidy, J. (2024), 'Firm hacked after accidentally hiring North Korean cyber criminal' *BBC News*, 16 October, https://www.bbc.com/news/articles/ce8vedz4yk7o.