

Artificial Intelligence and Regional Cybersecurity Governance: Transforming Security Cooperation in the 21st Century

Dina F. Jaccob, Badr University in Cairo, Egypt

The European Conference on Arts & Humanities 2026
Official Conference Proceedings

Abstract

This study examines how artificial intelligence (AI) is reshaping regional cybersecurity governance, addressing a gap in understanding the causal mechanisms between AI-driven threats and regional cooperation. Using a comparative case study design, the study integrates regional security community theory with new regionalist literature. Methodologically, it employs qualitative document analysis of primary policy sources (EU cybersecurity strategies, ASEAN digital agreements, and Middle East security declarations) and secondary literature, combined with process tracing to assess how AI-powered threats trigger institutional responses. Three cases are systematically compared: the European Union (high institutional density, binding frameworks), ASEAN (consensus-based, soft law), and the Middle East (fragmented, high tension, with specific focus on Iran). Cross-case variation in political trust and institutional maturity enables controlled comparison, strengthening validity. Findings show that AI transforms cyber threats from isolated incidents into systemic challenges, making regional coordination imperative. However, outcomes diverge: the EU advances toward centralized defense mechanisms; ASEAN prioritizes normative information-sharing; the Middle East remains fragmented, with AI capabilities reinforcing offensive postures and securitization dynamics involving Iran. The study contributes a focused, empirically grounded argument: AI not only changes attack and defense strategies but also reshapes regional security logics, turning transnational threats into either opportunities for integration (EU, ASEAN) or drivers of conflict (Middle East). This study design ensures replicability and addresses the validity concerns typical of broad, descriptive abstracts. The findings underscore the necessity of linking technological transformations with institutional structures in contemporary international relations.

Keywords: artificial intelligence, cybersecurity governance, regional security cooperation, new regionalism, institutional adaptation

iafor

The International Academic Forum
www.iafor.org

Introduction

Artificial intelligence (AI) is changing the cyber threat environment by increasing the speed, scale, and sophistication of cyber operations. These developments have expanded cybersecurity beyond national borders and increased the need for regional coordination and institutional responses (Brundage et al., 2018; Chen & Yang, 2022). Regional responses, however, differ considerably. The European Union has developed binding regulatory and institutional mechanisms, while ASEAN relies primarily on consensus, voluntary cooperation, and regional guidelines (Keith, 2024; Novelli et al., 2024; Putra, 2024). In the Middle East, cybersecurity cooperation remains more fragmented, with national capabilities and strategic competition playing a significant role (Trigui et al., 2024).

These differences raise an important question: How does artificial intelligence reshape regional cybersecurity governance, and why do similar AI-driven cyber threats produce different patterns of regional security cooperation?

Existing research has examined AI governance, cybersecurity, and regional cooperation largely as separate fields. Less attention has been given to the institutional processes through which AI-related cyber risks affect regional governance. Regional Security Community Theory emphasizes the importance of trust, institutional development, and shared expectations in sustaining cooperation (Adler & Barnett, 1998; Deutsch et al., 1957). These factors provide a basis for explaining why similar technological pressures may produce different regional outcomes.

This study argues that AI acts as a catalyst for institutional change, while its effects depend on institutional capacity, political trust, and regional security norms. Stronger institutional environments are more likely to translate emerging cyber risks into coordinated governance, whereas fragmented environments are more likely to rely on national capabilities and competitive security responses.

The study makes three contributions. First, it brings together AI governance, cybersecurity, New Regionalism, and Regional Security Community Theory. Second, it examines the mechanisms connecting AI-related cyber risks with institutional adaptation rather than assuming that technological change automatically produces cooperation. Third, it uses a structured comparison of the European Union, ASEAN, and the Middle East to explain how differences in institutional capacity and political conditions shape regional responses.

The European Union represents a highly institutionalized model based on binding regulation and supranational coordination. ASEAN provides a contrasting model based on consensus and voluntary cooperation, while the Middle East represents a fragmented regional security environment characterized by geopolitical competition and uneven institutional development. Comparing these cases allows the study to examine how different institutional settings shape responses to similar technological pressures.

Methodologically, the study employs a qualitative comparative case-study design based on document analysis and process tracing. Primary sources include regional cybersecurity strategies, AI governance frameworks, official policy documents, and regional declarations, complemented by academic literature. This approach allows the study to identify the processes through which emerging cyber risks influence regional institutional responses and to explain the variation observed across the three cases.

Theoretical Framework: AI, Regionalism, and Cybersecurity Governance

The integration of artificial intelligence (AI) into cyber operations has changed the relationship between technology, security, and governance. AI increases the speed, scale, and complexity of cyber activities while expanding cybersecurity concerns to include economic resilience, political stability, and regional security (Novelli et al., 2024). As cyber threats increasingly cross-national borders, regional institutions have become important mechanisms for policy coordination, information sharing, and regulatory cooperation. This study therefore combines three perspectives: New Regionalism, Regional Security Community Theory, and Cybersecurity Governance. Together, they explain how technological developments interact with institutional capacity and political conditions to produce different regional governance outcomes. AI is consequently treated as a contextual factor whose effects depend on the characteristics of each regional system.

Artificial Intelligence as a Driver of Institutional Change

AI represents more than a technological innovation because its capacity for data processing, prediction, automation, and adaptive decision-making affects the environment in which cyber competition occurs (Novelli et al., 2024). AI-enabled malware, automated influence operations, and AI-assisted cyber espionage also connect cybersecurity with political stability, economic security, and digital sovereignty (Trigui et al., 2024). These developments create pressure for institutions to adapt. However, technological change does not produce identical outcomes across regions. Institutions with greater regulatory capacity, established mechanisms of cooperation, and higher levels of political trust are better positioned to incorporate emerging technologies into collective governance. Where these conditions are weaker, similar technological pressures may produce fragmented or nationally oriented responses.

New Regionalism and Regional Cybersecurity Governance

New Regionalism views regions as evolving political and institutional spaces through which states address challenges that cannot be managed effectively at the national level (Hettne, 2005; Söderbaum, 2016). Cybersecurity reflects this dynamic because interconnected digital infrastructures and cross-border cyber operations create shared vulnerabilities requiring cooperation in information sharing, incident response, capacity building, and regulatory coordination. Regional governance, however, is shaped by institutional capacity and political context. Differences in legal authority, institutional density, and patterns of cooperation affect how regional organizations respond to emerging security challenges (Fawcett, 2012).

The European Union represents a highly institutionalized model supported by supranational institutions and binding legislation, whereas ASEAN relies more heavily on consensus, non-interference, and voluntary coordination (Keith, 2024; Putra, 2024). These differences demonstrate that regional institutions actively mediate technological change rather than simply responding to it.

Regional Security Communities and Regional Cybersecurity Governance

Regional Security Community Theory complements New Regionalism by emphasizing the role of trust, shared norms, and institutionalized cooperation in sustaining regional security relations. Deutsch et al. (1957) associated security communities with dependable expectations of peaceful change, while Adler and Barnett (1998) further emphasized shared identities,

norms, and institutional mechanisms. These principles are relevant to cybersecurity because effective regional responses require continuous information exchange, coordinated risk management, and confidence among participating states. Technological capabilities alone are therefore insufficient to produce sustained cooperation. The European Union illustrates how established institutional relationships can facilitate collective cybersecurity policies. In contrast, geopolitical rivalry can limit cooperation when cyber capabilities are viewed primarily as instruments of strategic competition. The Middle East demonstrates this difficulty, particularly in relations involving Iran, Israel, and Gulf states, where national cyber capabilities have developed alongside persistent regional tensions (Trigui et al., 2024).

Cybersecurity Governance as Multi-level Governance

Cybersecurity governance increasingly involves multiple actors, including governments, regional institutions, private technology companies, international organizations, and civil society. The importance of this multi-level structure has increased with the expansion of AI because technological development is strongly influenced by private-sector actors, while regulation and national security remain largely governmental responsibilities. Regional organizations consequently perform an intermediary role by coordinating standards, facilitating information exchange, and supporting capacity building. Their effectiveness depends partly on their ability to adapt regulatory arrangements to rapidly changing technological risks. The EU follows a more legally binding and institutionally integrated approach, while ASEAN emphasizes flexible cooperation, ethical principles, and capacity building (Keith, 2024; Novelli et al., 2024; Putra, 2024). These differences illustrate how institutional traditions shape the governance of emerging technologies.

Analytical Framework

The framework developed in this study connects AI-related cyber pressures with regional institutional adaptation. It assumes that similar technological developments may generate different outcomes because regional institutions operate under different political and institutional conditions.

Three variables guide the comparison:

1. Institutional capacity: the strength and effectiveness of regional institutions and their ability to implement collective decisions.
2. Political trust: the willingness of member states to cooperate, exchange sensitive information, and coordinate security policies.
3. Regional governance norms: shared principles concerning sovereignty, decision-making, and collective action.

These variables help explain the expected differences among the three cases. The EU represents a high-capacity model associated with regulatory integration; ASEAN reflects gradual, consensus-based coordination; and the Middle East illustrates the effects of fragmented institutions and persistent strategic rivalry. Accordingly, AI is conceptualized as a contextual factor rather than a direct determinant of regional cooperation. Its effects are mediated by institutional capacity, political trust, and governance norms. This framework provides the basis for the comparative analysis that follows.

Literature Review

Artificial Intelligence and Cybersecurity Governance

The literature on artificial intelligence and cybersecurity has expanded rapidly as AI has become relevant to both cyber defense and offensive operations. Early research emphasized applications such as automated threat detection, anomaly identification, malware analysis, and predictive assessment (Brundage et al., 2018; Russell & Norvig, 2021). More recent research highlights the dual-use nature of AI. Machine learning and generative AI can improve threat intelligence, vulnerability assessment, and security monitoring while also facilitating phishing, malicious code generation, social engineering, and other cyber operations (Achuthan et al., 2024; Yigit et al., 2025). Large language models have further expanded these possibilities, creating new challenges for cyber resilience and regulatory oversight (Xu et al., 2025; Zhang et al., 2025).

Despite this expanding literature, much of the research remains focused on technical capabilities and operational performance. Comparatively less attention has been given to how AI-related cyber risks affect regional institutions, cooperation, and governance. This gap is important because technological developments occur within different political and institutional environments. Understanding these differences requires connecting AI and cybersecurity research with regional governance scholarship.

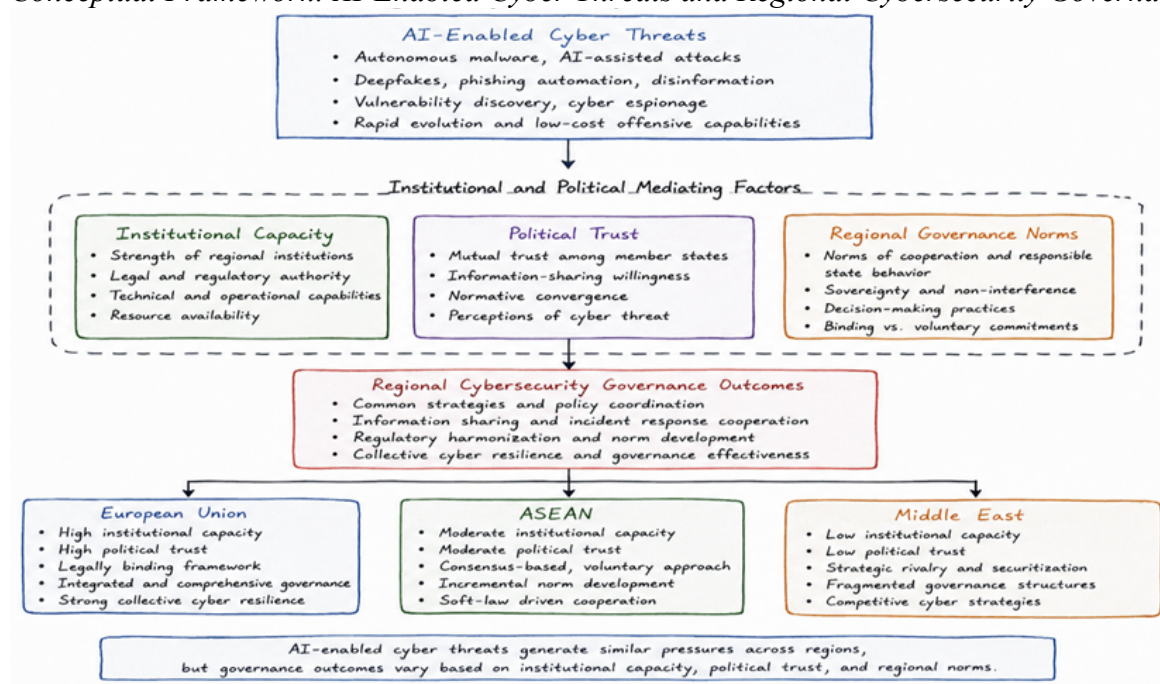
Regional Cybersecurity Governance

Regional cybersecurity governance has received increasing attention as cyber threats have become more transnational. The literature emphasizes institutional coordination, information sharing, regulatory cooperation, and collective resilience as important components of regional responses (Buzan & Wæver, 2003; Christou, 2016).

The European Union provides the most developed example of regional cybersecurity governance. Its combination of supranational institutions, binding legislation, and common cybersecurity policies has enabled greater regulatory coordination across member states (Christou, 2016; Novelli et al., 2024). The EU's cybersecurity framework has increasingly been connected with wider digital and AI governance.

ASEAN follows a different model based on consensus, non-interference, and voluntary cooperation. Regional initiatives have expanded cybersecurity and AI cooperation through policy guidelines, capacity building, and confidence-building measures, but implementation remains primarily dependent on national governments (Acharya, 2014a; Keith, 2024; Putra, 2024).

The Middle East presents a more fragmented environment. Existing scholarship focuses largely on cyber conflict, deterrence, and strategic competition, with less emphasis on region-wide institutional governance. Differences in national capabilities and persistent geopolitical tensions have constrained broader cybersecurity cooperation (Trigui et al., 2024). Taken together, the literature demonstrates substantial variation in regional cybersecurity governance but provides limited comparative explanation of why similar technological pressures generate different institutional responses. This study addresses this gap by comparing the EU, ASEAN, and the Middle East through a common framework centered on institutional capacity, political trust, and regional governance norms.

Figure 1*Conceptual Framework: AI-Enabled Cyber Threats and Regional Cybersecurity Governance*

Source: Designed by the author.

Research Gap and Contribution

The existing literature highlights significant advances in the study of AI, cybersecurity, and regional governance. Nevertheless, these three areas of research have generally evolved as separate fields with limited theoretical integration. The first limitation concerns the relationship between technology and institutions. Research on AI primarily examines technological capabilities, ethical governance, and regulatory challenges, whereas cybersecurity studies focus on operational resilience, cyber defense, and threat management. By contrast, International Relations scholarship emphasizes regional institutions, security cooperation, and governance mechanisms without systematically incorporating AI as a factor influencing institutional adaptation (Adler & Barnett, 1998; Buzan & Wæver, 2003). Consequently, current scholarship provides only a partial understanding of how technological transformation reshapes regional governance.

A second limitation relates to comparative analysis. Much of the existing research relies on single-case studies of the European Union, ASEAN, China, or the United States. Although these studies provide detailed insights into specific institutional settings, they offer limited explanations for why comparable technological pressures produce different governance outcomes across regions with contrasting political and institutional characteristics.

The third and most significant limitation concerns causal explanation. Existing studies frequently describe developments in AI governance and cybersecurity regulation but devote less attention to the mechanisms through which AI-related cyber challenges influence institutional adaptation. As a result, technological change is often treated as an external driver of governance reform rather than as a factor whose effects are conditioned by institutional capacity, political trust, and regional governance norms.

This study addresses these limitations by integrating insights from AI governance, New Regionalism, Regional Security Community Theory, and cybersecurity governance within a unified analytical framework. Instead of examining technology and institutions separately, the study explains how their interaction shapes regional cybersecurity governance. Through a structured comparative analysis of the European Union, ASEAN, and the Middle East, it identifies the institutional conditions under which AI-related cyber challenges encourage regulatory cooperation, strengthen regional governance, or reinforce strategic competition.

This perspective extends the existing literature in two respects. Theoretically, it connects technological transformation with regional institutional adaptation, offering an integrated explanation of how emerging technologies influence regional security governance. Empirically, it provides a comparative assessment of three contrasting regional contexts, demonstrating that differences in institutional capacity and political trust play a central role in shaping regional responses to AI-enabled cyber challenges.

Research Methodology

Research Design

This study employs a qualitative comparative case study design to examine how AI-related cyber challenges influence regional cybersecurity governance under different institutional conditions. A qualitative approach is appropriate because the study seeks to explain differences in institutional responses rather than measure statistical relationships (Yin, 2017).

The research uses a structured, focused comparison in which all cases are examined through the same analytical framework. This approach facilitates systematic comparison and helps identify the institutional factors associated with different governance outcomes (George & Bennett, 2005).

Case Selection

The study applies a most-different systems design to compare three contrasting regional contexts: the European Union (EU), the Association of Southeast Asian Nations (ASEAN), and the Middle East, with particular attention to Iran's role in regional cyber dynamics. The EU represents a highly institutionalized model based on supranational institutions and binding regulations. ASEAN reflects a consensus-based model emphasizing sovereignty, non-interference, and voluntary cooperation. The Middle East represents a fragmented security environment characterized by geopolitical rivalry and limited regional institutionalization. This variation provides a basis for examining why similar technological challenges produce different governance responses (George & Bennett, 2005).

Data Collection

The study relies primarily on qualitative document analysis. Primary sources include regional cybersecurity strategies, regulatory frameworks, official declarations, policy documents, and institutional reports produced by the EU, ASEAN, and relevant Middle Eastern institutions.

These sources are complemented by peer-reviewed articles, academic books, and reports from international organizations. Using multiple categories of evidence enables cross-checking and strengthens the credibility of the findings (Bowen, 2009).

Data Analysis

The study combines comparative case analysis with process tracing. Comparative analysis identifies differences and similarities across the three cases, while process tracing examines how technological developments are followed by institutional and policy responses (Beach & Pedersen, 2019).

The analysis focuses on three dimensions derived from the theoretical framework:

1. Institutional capacity: the strength and regulatory authority of regional institutions.
2. Political trust: the willingness of states to cooperate, exchange information, and coordinate policies.
3. Governance norms: principles concerning sovereignty, decision-making, and regional cooperation.

These dimensions are used consistently across the EU, ASEAN, and the Middle East to explain variation in regional cybersecurity governance.

Research Validity and Limitations

The study strengthens validity through structured comparison, data triangulation, and process tracing. Applying the same analytical criteria across all cases improves comparability, while combining official documents with academic and institutional sources reduces reliance on individual sources (Bowen, 2009; George & Bennett, 2005). Process tracing further supports causal analysis by examining the sequence connecting technological developments with institutional responses (Beach & Pedersen, 2019).

The study has two principal limitations. First, qualitative design supports analytical rather than statistical generalization. Second, cybersecurity policies and technologies are evolving rapidly, meaning that regional governance arrangements may continue to change beyond the period examined. Despite these limitations, the research design provides an appropriate basis for explaining differences in regional cybersecurity governance.

AI and the Transformation of Regional Cyber Threats

AI-Driven Cyber Threats

Artificial intelligence has changed the speed, scale, and adaptability of cyber operations. Machine learning, generative AI, and large language models can support activities such as phishing, malware development, vulnerability discovery, reconnaissance, and influence operations. At the same time, these technologies improve threat detection, incident response, and risk assessment (Achuthan et al., 2024; Brundage et al., 2018; European Union Agency for Cybersecurity [ENISA], 2024).

The significance of these developments lies in the increasing interaction between offensive and defensive capabilities. AI allows cyber operations to adapt more rapidly to changing technical environments, making attribution, prevention, and response more difficult. Consequently, cybersecurity increasingly requires institutional capacity to anticipate and manage continuously evolving risks rather than simply respond to individual incidents.

From Cyber Incidents to Systemic Regional Security Risks

AI-enabled cyber threats increasingly affect interconnected digital systems rather than isolated networks. Energy, finance, telecommunications, healthcare, transportation, and government services depend on infrastructures that cross national boundaries. Disruption in one system or jurisdiction can therefore produce wider regional consequences, particularly through interconnected supply chains and digital services (ENISA, 2024).

The expansion of generative AI has also broadened the security dimension of these risks. Synthetic media and automated influence operations can affect public trust, political communication, and social stability, linking cybersecurity with wider concerns of economic and political resilience (European Commission, 2024).

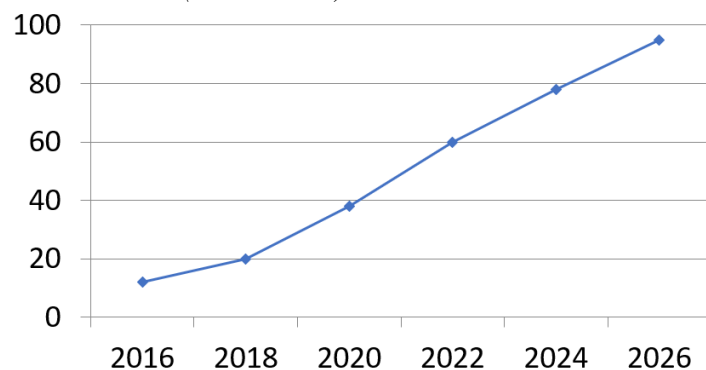
These developments strengthen the regional dimension of cybersecurity. As digital interdependence increases, national responses alone become less sufficient, creating greater demand for information sharing, coordinated incident response, and common standards. However, the ability to develop such mechanisms depends on the institutional conditions of each region.

Implications for Regional Security Cooperation

The changing nature of cyber threats increases the importance of regional cooperation in areas such as information sharing, incident response, capacity building, regulatory coordination, and critical infrastructure protection (ENISA, 2024). However, similar technological pressures do not necessarily produce similar forms of cooperation. Institutional capacity and political conditions shape how regions respond. The European Union has translated emerging cyber risks into stronger regulatory and institutional coordination. ASEAN has pursued gradual cooperation through consensus and voluntary policy coordination, while the Middle East remains more affected by geopolitical rivalry and fragmented regional institutions (Keith, 2024; Putra, 2024; Trigui et al., 2024).

The central implication is therefore that technological change does not determine a single pattern of regional governance. AI creates common security pressures, but institutional capacity, political trust, and regional governance norms influence whether these pressures lead to deeper cooperation or continued strategic competition. The following comparative analysis examines these differences across the European Union, ASEAN, and the Middle East.

Figure 2
Threat Index (2016–2026)



Source: Data compiled by the author (2026).

Comparative Regional Analysis

European Union: Institutional Integration and Regional Cybersecurity Governance

The European Union represents the most institutionally developed case examined in this study. Its cybersecurity governance combines supranational institutions, binding legislation, common standards, and coordinated implementation. This structure enables Member States to address cyber risks through collective regulatory mechanisms rather than relying exclusively on national policies (Christou, 2016; ENISA, 2024).

Institutional Capacity and Governance Structure

EU cybersecurity governance involves the European Commission, ENISA, the NIS Cooperation Group, the CSIRTs Network, and national cybersecurity authorities. Although Member States retain important operational responsibilities, these institutions facilitate policy coordination, information exchange, technical support, and cross-border cooperation (Christou, 2016; ENISA, 2024).

This institutional density is particularly relevant to AI-related cyber risks because it allows existing governance mechanisms to adapt to emerging technologies. Cybersecurity is increasingly connected with critical infrastructure protection, digital resilience, supply-chain security, and broader digital governance (European Commission, 2024).

Regulatory Development

The EU has developed a relatively coherent regulatory framework through complementary legislation. The NIS2 Directive establishes common cybersecurity requirements for essential and important entities, while the Cyber Resilience Act introduces cybersecurity requirements for digital products throughout their lifecycle. Together, these measures strengthen common cybersecurity standards across the Union (ENISA, 2024; European Commission, 2024).

The AI Act adds an important AI-specific dimension to this framework. Its risk-based approach includes requirements related to cybersecurity, robustness, risk management, and monitoring for high-risk AI systems. This illustrates the increasing convergence between AI governance and cybersecurity regulation (European Parliament & Council of the European Union, 2024).

Institutional Response to Emerging Cyber Risks

The European approach relies largely on adapting existing institutions to emerging risks rather than creating separate governance structures for every technological development. Coordinated incident reporting, risk assessment, technical guidance, and cooperation among national authorities contribute to this process (ENISA, 2024). However, implementation remains uneven because Member States differ in administrative capacity, cybersecurity maturity, and national implementation practices. The continuing interaction between the AI Act, NIS2, the Cyber Resilience Act, and other digital regulations therefore requires sustained institutional coordination.

Regional Cybersecurity Effectiveness

The EU demonstrates how institutional capacity can strengthen regional cyber resilience through information sharing, coordinated incident management, common standards, and collective preparedness. Its effectiveness, however, should be understood in terms of resilience and response capacity rather than the elimination of cyber threats.

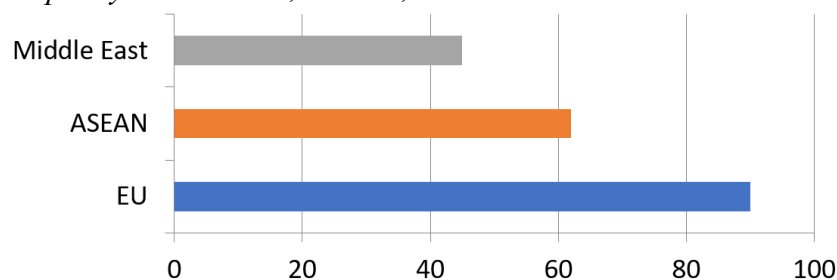
AI-related risks continue to evolve, including AI-assisted social engineering, automated vulnerability discovery, supply-chain risks, and synthetic content. Consequently, European cybersecurity governance requires continuous risk assessment and regulatory adaptation (ENISA, 2024).

Comparative Assessment

The EU case supports the central argument of this study: technological pressure alone does not determine regional governance outcomes. Existing institutional capacity enables AI-related cyber risks to be translated into coordinated regulatory and policy responses. AI therefore acts as a catalyst for institutional adaptation, while the strength of regional institutions determines the extent of collective action.

Figure 3

Capacity Score in EU, ASEAN, and the Middle East



Source: Data compiled by the author (2026).

ASEAN: Consensus-Based Cooperation and Incremental Cybersecurity Governance

ASEAN represents a substantially different model of regional cybersecurity governance. Its approach is based on consultation, consensus, non-interference, and gradual cooperation rather than supranational authority. These principles have shaped cybersecurity cooperation around capacity building, policy coordination, confidence building, and information sharing (Acharya, 2014b).

Institutional Structure and Cybersecurity Cooperation

ASEAN has developed cybersecurity cooperation through regional mechanisms rather than a centralized regulatory authority. The ASEAN Cybersecurity Cooperation Strategy 2021–2025 focuses on advancing cyber readiness, strengthening regional policy coordination, building trust, developing capacity, and expanding international cooperation (ASEAN, 2022). (ASEAN Main Portal)

This approach allows states with different levels of technological and administrative capacity to participate without transferring significant authority to regional institutions. The main consequence is greater flexibility but less uniformity in implementation.

AI Governance and Regional Coordination

ASEAN has also begun addressing AI governance through regional guidelines. The ASEAN Guide on AI Governance and Ethics, adopted in 2024, provides principles and practical guidance for the responsible development and use of AI. Its role is primarily coordinative rather than regulatory, reflecting ASEAN's preference for non-binding regional frameworks (ASEAN, 2024). (ASEAN Main Portal)

For cybersecurity, this distinction is important. The regional AI framework can promote common expectations concerning responsible AI development, but it does not create a centralized system for managing AI-related cyber incidents. Cybersecurity cooperation therefore remains dependent on national capabilities and voluntary regional coordination.

Regional Cybersecurity Capacity

ASEAN has nevertheless strengthened regional cyber capacity through information-sharing mechanisms, training, confidence-building initiatives, and cooperation among national authorities. The ASEAN Cybersecurity Cooperation Strategy provides an institutional framework for these activities (ASEAN, 2022). (JAIF ASEAN)

The principal limitation is the absence of binding enforcement mechanisms comparable to those found in the EU. Implementation consequently varies according to national priorities and institutional capacity.

Comparative Assessment

ASEAN demonstrates that regional cooperation can develop without supranational integration. However, its consensus-based structure produces a gradual form of governance in which technological pressures encourage coordination without fundamentally changing the underlying institutional model. AI therefore strengthens the need for cooperation while remaining filtered through ASEAN's established norms of sovereignty and consensus.

The Middle East: Geopolitical Rivalry and Fragmented Cybersecurity Governance

The Middle East presents a different institutional environment. Unlike the EU, the region does not possess a single organization with comprehensive authority over cybersecurity. Cooperation exists through sub-regional arrangements, particularly the Gulf Cooperation Council (GCC), but broader regional governance remains constrained by geopolitical rivalry, divergent national priorities, and limited political trust.

Institutional Fragmentation and Gulf Cooperation

The GCC provides the clearest example of structured cybersecurity cooperation within the region. Its member states have developed mechanisms for coordination, joint exercises, policy development, and information sharing. The Gulf Cybersecurity Strategy 2024–2028 and its implementation mechanisms demonstrate continuing efforts to strengthen cooperation among GCC members (Gulf Cooperation Council, 2024). However, GCC cooperation should not be equated with a comprehensive Middle Eastern cybersecurity regime. It remains subregional and does not encompass the broader strategic divisions involving Iran, Israel, and other regional actors.

Iran and Regional Cyber Competition

Iran is particularly relevant to understanding the relationship between cyber capabilities and regional security competition. Iranian cyber capabilities have developed as part of broader national security strategies and have contributed to the wider cyber competition involving regional and external actors.

In such an environment, cybersecurity is frequently treated as a national security capability rather than a domain for broad regional institutionalization. Concerns regarding sensitive information, attribution, strategic vulnerability, and deterrence can therefore limit incentives for extensive information sharing and common regulatory arrangements.

AI Governance and Uneven Institutional Development

AI governance across the Middle East remains uneven. States differ significantly in technological capacity, regulatory development, national AI strategies, and institutional readiness. These differences make the development of a comprehensive regional governance framework difficult.

Consequently, AI development has largely progressed through national strategies and initiatives, while regional cooperation remains selective. Where common interests exist, cooperation is possible, particularly within sub-regional arrangements such as the GCC. However, geopolitical competition continues to constrain broader institutional integration.

Regional Governance Outcome

The Middle Eastern case therefore represents neither complete institutional absence nor effective region-wide governance. Instead, it demonstrates selective cooperation within particular institutional settings alongside broader strategic fragmentation. This pattern supports the study's theoretical argument that technological pressures are filtered through existing political relationships and institutional structures. Compared with the EU and ASEAN, the Middle Eastern response remains more state-centered, with national AI and cybersecurity capabilities developing faster than comprehensive regional governance mechanisms.

Comparative Discussion

The comparison demonstrates that the three regions face broadly similar challenges associated with AI-enabled cyber risks but respond through different institutional mechanisms.

The EU represents the strongest form of institutional integration. Binding legislation, specialized institutions, and coordinated implementation allow technological pressures to be translated into regional regulatory responses.

ASEAN follows a more flexible model. Consensus, voluntary cooperation, capacity building, and common guidelines allow regional coordination while preserving national sovereignty. Its main limitation is the absence of strong enforcement and uniform implementation mechanisms.

The Middle East presents the most fragmented pattern. sub regional cooperation, particularly within the GCC, demonstrates that institutional coordination is possible, but geopolitical rivalry and limited regional trust constrain the development of broader governance

arrangements. Overall, the comparison confirms the central proposition of this study: AI creates common strategic pressures, but it does not produce a uniform model of regional cybersecurity governance. Institutional capacity, political trust, and governance norms determine whether technological pressures generate regulatory integration, incremental coordination, or fragmented and predominantly national responses.

Conclusion

This study examined how artificial intelligence has influenced regional cybersecurity governance and why comparable technological challenges have produced different patterns of regional cooperation. The comparative analysis demonstrates that the effects of AI cannot be explained by technological change alone. Instead, regional responses are shaped by the institutional capacity of regional organizations, the degree of political trust among member states, and the governance norms that structure regional cooperation.

The findings indicate that AI has expanded the scope of cybersecurity beyond the protection of digital infrastructure. Cybersecurity has become an issue of regional governance that requires coordinated regulatory frameworks, institutional adaptation, and sustained cross-border cooperation. As AI-enabled cyber threats continue to evolve, regional institutions increasingly face the challenge of responding to technological change while maintaining effective governance arrangements.

The three case studies illustrate distinct institutional trajectories. The European Union has developed the most comprehensive regional governance model by combining supranational institutions with legally binding regulatory frameworks that support coordinated cybersecurity policies (Christou, 2016; European Union Agency for Cybersecurity [ENISA], 2024). ASEAN has adopted a more gradual approach based on consultation, consensus, and voluntary coordination, reflecting the principles that have traditionally shaped regional cooperation (Keith, 2024). In contrast, the Middle East continues to experience fragmented regional governance, where geopolitical rivalry limits institutional cooperation and encourages nationally driven cybersecurity strategies (Grand-Clément, 2023).

Comparing these regional experiences demonstrates that similar technological pressures do not produce uniform governance outcomes. AI has acted as a catalyst that exposes differences in institutional preparedness rather than determining a single path of regional development. Regions with stronger institutional arrangements have generally been more capable of translating common cybersecurity challenges into coordinated governance, whereas weaker institutional settings have struggled to move beyond fragmented national responses.

The study also contributes to the literature by connecting AI governance, cybersecurity governance, New Regionalism, and Regional Security Community Theory within a single analytical framework. This integrated perspective explains regional variation by emphasizing the interaction between technological change and institutional context, offering a broader explanation than approaches that focus exclusively on technology or national cybersecurity capabilities.

The findings have practical implications for policymakers. Investments in AI technologies alone are unlikely to strengthen regional cybersecurity if they are not accompanied by institutional coordination, regulatory coherence, information sharing, and mechanisms that

encourage sustained regional cooperation. Strengthening these institutional foundations is essential for improving regional resilience as cyber threats continue to evolve.

The study is subject to several limitations. It examines three regional cases through a qualitative comparative design and therefore seeks to provide analytical rather than statistical generalization. In addition, the rapid pace of technological and regulatory change means that regional cybersecurity governance will continue to evolve beyond the period covered by this research. Future studies may extend the comparative analysis to other regional organizations, incorporate quantitative indicators of cybersecurity governance, or examine the growing role of private technology companies in regional AI governance.

Overall, the findings suggest that the future of regional cybersecurity governance will depend less on the pace of technological innovation than on the ability of regional institutions to adapt to that innovation. As AI becomes more deeply integrated into cyber operations, institutional resilience, regulatory coordination, and political cooperation are likely to become the principal factors shaping regional cybersecurity governance.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

The authors declare that no Generative Artificial Intelligence (GenAI) tools were used in the development of this manuscript.

References

- Acharya, A. (2014a). *Constructing a security community in Southeast Asia: ASEAN and the problem of regional order*. Routledge.
- Acharya, A. (2014b). *The end of American world order*. Polity Press.
- Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions. *Frontiers in Big Data*, 7, 1497535.
- Adler, E., & Barnett, M. N. (1998). *Security communities*. Cambridge University Press.
- ASEAN. (2022). *ASEAN cybersecurity cooperation strategy 2021–2025*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf
- ASEAN. (2024). *ASEAN guide on AI governance and ethics*. ASEAN Secretariat. https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf
- Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines*, 2nd Ed. University of Michigan Press.
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó hÉigartaigh, S. S., Beard, S., Belfield, H., Farquhar, S., ... Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv.
- Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.
- Chen, X., & Yang, Y. (2022). Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance. *The International Spectator*, 57(3), 48–65.
- Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Springer.
- Deutsch, K. W., Burrell, S. A., Kann, R. A., Lee, M., Lichterman, M., Lindgren, R. E., Loewenheim, F. L., & van Wagenen, R. W. (1957). *Political community and the North Atlantic area: International organization in the light of historical experience*. Princeton University Press.
- European Commission. (2024). *Artificial Intelligence Act: Regulation (EU) 2024/1689*. European Union.

- European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*. Official Journal of the European Union, L, 2024/1689, 12.7.2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- European Union Agency for Cybersecurity (ENISA). (2024). 2024 Report on the State of the Cybersecurity in the Union. In cooperation with the NIS Cooperation Group and the European Commission, in accordance with Article 18 of the Directive (EU) 2022/2555 (NIS2). Available at: <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union>
- Fawcett, L. (2012). The History and Concept of Regionalism (2012). *European Society of International Law (ESIL) Conference Paper Series No. 4/2012*.
- George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. MIT Press.
- Grand-Clément, S. (2023). *Artificial intelligence beyond weapons: Application and impact of AI in the military domain*. Report. UNIDIR.
- Gulf Cooperation Council. (2024). *Gulf cybersecurity strategy 2024-2028*. General Secretariat of the Gulf Cooperation Council.
- Hettne, B. (2005). Beyond the ‘new’ regionalism. *New Political Economy*, 10(4), 543–571.
- Keith, A. J. (2024). Governance of artificial intelligence in Southeast Asia. *Global Policy*, 15(5), 937–954.
- Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2024). A robust governance for the AI Act: AI office, AI board, scientific panel, and national authorities. *European Journal of Risk Regulation*, 16(2), 566–590.
- Putra, B. A. (2024). Governing AI in Southeast Asia: ASEAN’s way forward. *Frontiers in Artificial Intelligence*, 7, 1411838.
- Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach*, 4th Ed. Pearson.
- Söderbaum, F. (2016). *Rethinking regionalism*. Palgrave Macmillan.
- Trigui, H., Guerfali, F., Harigua-Souiai, E., Qasrawi, R., Atri, C., Salem Sokhn, E., El Morr, C., Hammami, K., Souiai, O., Wu, J., Kong, J. D., Rousseau, J. J., & Znaidi, S. (2024). Exploring AI governance in the Middle East and North Africa (MENA) region: Gaps, efforts, and initiatives. *Data & Policy*, 6, e83.
- Xu, H., Wang, S., Li, N., Wang, K., Zhao, Y., Chen, K., Yu, T., Liu, Y., & Wang, H. (2025). *Large language models for cyber security: A systematic literature review*. arXiv.

Yigit, Y., Buchanan, W. J., Tehrani, M. G., & Maglaras, L. (2025). Review of generative AI methods in cybersecurity. *Internet of Things and Cyber-Physical Systems*.

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods*. SAGE Publications.

Zhang, J., Bu, H., Wen, H., Liu, Y., Fei, H., Xi, R., ... & Meng, D. (2025). When LLMs meet cybersecurity: A systematic literature review. *Cybersecurity*, 8(1), 55.