Artificial Intelligence, Cybersecurity, and Regional Security Governance: Rethinking Security Cooperation in the Era of New Regionalism

Dina Jaccob
PhD.Assistant Professor of International Relations School of Political Science& International Relations Badr University in Cairo

Abstract
This study explores the relationship between cyber threats, artificial intelligence (AI), and regional security cooperation in the contemporary international system. The rapid expansion of digital infrastructure and increasing reliance on cyberspace have transformed cyber threats from isolated criminal incidents into tools of strategic competition among states. The research examines whether AI-enhanced cyber threats are encouraging states to develop new forms of regional collective security mechanisms.
The study argues that the transnational nature of cyber threats limits the effectiveness of purely national responses, creating stronger incentives for regional cooperation. Drawing on perspectives from International Security Studies and the literature on new regionalism, the research connects technological change with evolving forms of regional security governance. It integrates insights from cybersecurity studies, complex interdependence, and regional cooperation theory to explain emerging patterns of coordination among states.
Using an analytical approach based on academic literature, policy reports, and international cybersecurity assessments, the study shows that AI strengthens defensive cyber capacities while also enabling more sophisticated offensive operations, increasing uncertainty in cyberspace. The findings suggest that regional coordination is becoming a practical necessity for managing shared digital risks and sustaining stability in an increasingly interconnected security environment.
Keywords: Artificial Intelligence; Cybersecurity; Regional Security Governance; Regional Security Complex Theory; New Regionalism; Cyber Cooperation; Digital Governance; Regional Stability.

1. INTRODUCTION

Over the past two decades, the international security environment has undergone a qualitative transformation due to the rapid expansion of the digital space and the increasing reliance of states on information infrastructure to manage vital sectors such as energy, telecommunications, and financial systems. This transformation has led to the emergence of complex and transnational cyber threats, no longer limited to individuals or non-state actors, but rather becoming part of the tools of strategic competition between states. Recent literature in international security studies indicates that cyberattacks have become one of the most significant security challenges in the contemporary international system, given their ability to produce broad economic and political impacts without resorting to traditional military force (Nye, 2017).
In this context, the rapid advancement of Artificial Intelligence (AI) technologies has fundamentally transformed the nature of cyber threats and how to address them. AI is increasingly used to analyze massive amounts of data, identify patterns associated with cyberattacks, and enhance digital defense capabilities. However, these technologies also provide advanced tools that can be employed to execute more sophisticated and effective cyberattacks, making threats more difficult to predict or contain (Horowitz, 2018).

Furthermore, the transnational nature of cyberattacks poses significant challenges for countries in addressing these threats individually. Cyberspace has no clear geographical boundaries, and the digital infrastructure in many countries is closely interconnected, making any cyber threat simultaneously regional and international in scope. This has led a growing number of researchers to emphasize the importance of collaborative frameworks in cybersecurity management, especially given the increasing interdependence of countries in the digital sphere (Singer & Friedman, 2014).

Within this context of transformations, regions have acquired an increasing role in addressing shared security challenges. This aligns with the new regionalism literature in the field of International Relations, which indicates that regional cooperation is no longer limited to economic issues but has expanded to include security, technology, and digital governance (Hettne, 2005). However, the relationship between artificial intelligence (AI), cybersecurity, and regional security arrangements remains an area requiring further analysis, particularly regarding how technologically enhanced cyber threats impact patterns of security cooperation among states within different regions.
Accordingly, the study seeks to analyze the role of AI in managing cyber threats within the framework of regional security arrangements by addressing the central research question: Do the rise of AI-enhanced cyber threats contribute to pushing states to develop new mechanisms for regional security cooperation? The study also aims to make a theoretical contribution to the international security literature by linking contemporary technological transformations with concepts of regional security governance, as well as shedding light on the practical dimensions of cooperation among states in confronting escalating cyber threats.
This study employs an analytical approach to international relations, drawing on theoretical literature related to cybersecurity and emerging regionalism, as well as an analysis of international policies and reports concerning cyber governance. The study is divided into several main sections: first, it reviews previous literature related to the research topic; second, it presents the theoretical framework of the study; third, it analyzes the relationship between artificial intelligence and the evolution of cyber threats, and their impact on the development of regional security arrangements; and finally, it discusses the findings and draws theoretical and practical implications of the study.

2. THEORETICAL FRAMEWORK

This study analyzes the relationship between artificial intelligence (AI), cyber threats, and the evolution of regional security arrangements through an integrated theoretical framework combining Regional Security Complex Theory (RSCT) and New Regionalism. The integration of these approaches enables a multidimensional understanding of how technological transformations reshape both threat perception and institutional responses at the regional level. Recent developments in cybersecurity governance and digital geopolitics suggest that security dynamics increasingly emerge at the intersection of technology, geography, and institutional cooperation rather than within purely national framework.

2.1 Regional Security Complex Theory (RSCT)

Regional Security Complex Theory, developed by Barry Buzan and Ole Wæver (2003), provides a foundational framework for understanding how security interdependence develops among geographically proximate states. RSCT argues that security threats travel

more easily across short distances, creating patterns of mutual vulnerability that bind states into regional clusters where national security cannot be understood independently from neighboring actors. Security dynamics therefore become regionally structured, shaped by patterns of amity, rivalry, and shared threat perception (Buzan, Wæver, & de Wilde, 1998).

While RSCT was originally formulated in the context of traditional military and political threats, contemporary scholarship has expanded its applicability to non-traditional security domains, including cyberspace. Cyber threats challenge classical territorial assumptions because digital infrastructures are interconnected across borders, yet their consequences remain geographically concentrated within regions sharing infrastructure networks, supply chains, and regulatory environments (Kello, 2017). As Nye (2017) argues, cyber power introduces a form of "diffused vulnerability," whereby even technologically advanced states remain exposed through regional digital interdependence.

The integration of artificial intelligence further intensifies this dynamic. AI-driven cyber capabilities enhance speed, automation, and scale in both offensive and defensive operations, reducing decision time and increasing uncertainty among states (Horowitz, 2018; Payne, 2021). Within an RSCT perspective, such developments deepen regional security interdependence by making cyber incidents rapidly spill over across neighboring states' infrastructures, financial systems, and communication networks. Consequently, cyber stability increasingly depends on coordinated regional responses rather than isolated national strategies.

Recent empirical studies also support the regionalization of cyber security practices. For example, the emergence of coordinated cyber defense initiatives within the European Union and ASEAN demonstrates how shared threat environments encourage institutionalized cooperation at the regional level (Christou, 2016; Klimburg, 2020). These developments reinforce RSCT's core assumption that security responses tend to consolidate regionally when threats become mutually embedded.

2.2 New Regionalism

The New Regionalism literature complements RSCT by explaining how regions evolve institutionally in response to shared challenges. Unlike earlier forms of regionalism focused primarily on economic integration, new regionalism conceptualizes regions as multidimensional governance spaces shaped by globalization, technological change, and transnational risks (Hettne, 2005; Söderbaum, 2016).

New regionalism emphasizes three central dynamics particularly relevant to cybersecurity: institutional flexibility, functional cooperation, and governance beyond the nation-state. As Fawcett (2016) notes, contemporary regional organizations increasingly expand into nontraditional policy domains, including security coordination, technological regulation, and digital governance frameworks. Cybersecurity cooperation reflects this evolution, as states seek collective mechanisms to manage risks that cannot be effectively regulated domestically.

Digital governance has therefore become a core component of regional cooperation agendas. Regional organizations now develop shared cyber norms, information-sharing mechanisms, and joint incident response frameworks to address common vulnerabilities (Segal, 2016; Klimburg & Zylberberg, 2019). These initiatives illustrate how technological threats act as functional drivers of institutional innovation,a central claim of new regionalism theory.

Moreover, scholars argue that emerging technologies reshape regional identities by creating shared technological dependencies. AI development ecosystems, data flows, and cloud infrastructures increasingly operate at regional scales, encouraging policy harmonization and cooperative regulation (Farrell & Newman, 2019). This suggests that cybersecurity cooperation is not merely reactive but also structurally embedded within broader processes of regional governance transformation.

2.3 Artificial Intelligence, Cyber Threats, and Regional Security Arrangements

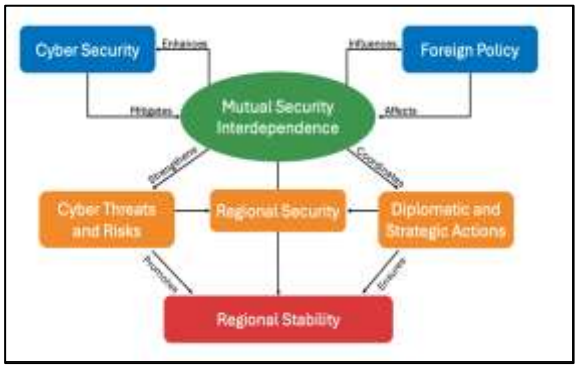
Building on RSCT and new regionalism, this study posits that AI-enhanced cyber threats act as catalysts for the evolution of regional collective security mechanisms. From an RSCT perspective, AI intensifies security interdependence by accelerating threat diffusion and increasing uncertainty among geographically connected states. Simultaneously, new regionalism explains how these pressures translate into institutional responses through the creation of cooperative frameworks, regulatory coordination, and shared cyber defense mechanisms.

Artificial intelligence alters the strategic environment in three keyways. First, it lowers barriers to sophisticated cyber operations through automation and machine learning tools, enabling both state and non-state actors to conduct high-impact attacks (Singer & Friedman, 2014; Brundage et al., 2018). Second, AI enhances defensive capabilities such as predictive threat detection and automated response systems, creating a technological arms dynamic in cyberspace. Third, AI amplifies ambiguity regarding attribution and escalation, complicating traditional deterrence models and encouraging cooperative risk-management approaches (Libicki, 2021).

Consequently, regional arrangements emerge as intermediate governance levels capable of balancing sovereignty concerns with collective security needs. Examples include regional cyber capacity-building programs, joint cyber exercises, and shared norms for responsible state behavior in cyberspace, reflecting what Nye (2020) describes as the gradual institutionalization of cyber stability mechanisms.

The integration of RSCT and new regionalism therefore provides a comprehensive analytical lens linking technological transformation to institutional evolution. Technological change does not operate independently from political geography; rather, AI-driven cyber threats reshape patterns of cooperation, redefine regional security priorities, and encourage the development of collective governance structures. This intersection constitutes the central research gap addressed by the study: understanding how emerging technologies transform not only threats themselves but also the regional architectures through which states seek security in the digital age.

figure1: Cyber–Foreign Policy Security Interdependence Model



Source : compiled by the author

This model illustrates the interconnected relationship between cyber security, foreign policy, and regional security outcomes within the contemporary international system. It

explains how cyber threats are no longer isolated technical challenges but have become strategic factors influencing diplomatic behavior and state decision-making.
At the center of the model is Mutual Security Interdependence, which represents the idea that states' security environments are increasingly linked through digital networks and shared vulnerabilities. Cyber security capabilities help mitigate cyber risks, while foreign policy decisions shape how states cooperate, respond, or compete in cyberspace.

3. METHODOLOGY

The study aims to study the impact of artificial intelligence (AI) on cyber threats and the evolution of regional security arrangements within the framework of new regionalism. To achievez this, the study employs a multi-level comparative analytical methodology that combines the analytical approach in security studies with a case study approach across different regions.

3.1 Analytical Method

The analytical method was used to understand the relationship between the key variables: artificial intelligence, cyber threats, and regional security arrangements. This approach allows for linking technological transformations to political and security practices and analyzing how innovations in AI affect regional security policies (Buzan & Wæver, 2003). The analytical method also enables the identification of recurring patterns of security cooperation among states within the framework of new regionalism and explores how new institutional arrangements are emerging to address cyber risks.

3.2 Case Study and Regional Comparison

The study relies on case studies of selected regions that demonstrate differences in states' responses to AI-enhanced cyber threats. These cases include:
The European Union, as a model of advanced regional cooperation in cybersecurity (European Union Agency for Cybersecurity, 2021). Also, regional alliances in Asia, such as ASEAN, where strategies for security coordination and AI adoption vary. This approach allows for a comparison of outcomes across regions and an understanding of how cultural, political, and technological factors influence the design of regional security arrangements (Hettne, 2005; Fawcett, 2016). It also reveals the strengths and weaknesses of different regions' responses to digital threats.

3.3 Data Sources

The study relies on a variety of sources to ensure the reliability of its findings:

- International and institutional reports: such as reports from the Stockholm International Peace Research Institute and the International Institute for Strategic Studies on cybersecurity and artificial intelligence.
- Regional policies and guidelines: including European Union documents on cybersecurity and Asian countries' strategies on digital security cooperation.
- Cyberattack databases: such as national network penetration data and international cyberattack reports, to assess the scale of AI-enhanced cyber threats and analyze their patterns (Singer & Friedman, 2014; Nye, 2017).
- Academic literature: to support the theoretical analysis and integrate the findings of previous studies with the current conclusions.

Advantages of the Integrated Approach

This methodological design combines theoretical analysis with applied data, allowing for a deeper understanding of the interactions between technology, cyber threats, and regional security policies. The methodology also supports the research's ability to provide practical recommendations for levels of regional cooperation, and allows for conclusions that can be generalized within similar contexts.

4. Artificial Intelligence and the Transformation of Cyber Threats

Recent years have witnessed a qualitative transformation in the nature, scale, and strategic implications of cyber threats driven by rapid advances in artificial intelligence (AI) technologies. Unlike earlier forms of cyber operations that relied heavily on manual intrusion techniques, AI enables automated vulnerability discovery, adaptive malware behavior, and real-time decision-making during cyber operations. Machine learning algorithms and big data analytics allow malicious actors to analyze massive datasets, identify system weaknesses, and execute highly targeted attacks capable of bypassing conventional signature-based defense mechanisms (Horowitz, 2018; Brundage et al., 2018).

One of the most significant developments is the emergence of AI-enhanced spear-phishing and social engineering campaigns. By leveraging natural language processing (NLP) and behavioral data analysis, attackers can generate highly personalized communications that significantly increase success rates compared to traditional phishing methods (Kello, 2017; Payne, 2021). Moreover, AI facilitates simultaneous multi-vector attacks on critical infrastructure systems—including energy grids, transportation networks, water systems, and healthcare databases—where algorithms autonomously map network dependencies and exploit cascading vulnerabilities across interconnected platforms (ENISA, 2021; CISA, 2023).

The integration of AI into cyber operations has also altered the temporal dynamics of conflict in cyberspace. Automated attack systems drastically reduce response time between detection and exploitation, compressing strategic decision-making cycles for states and increasing escalation risks. Scholars describe this phenomenon as "algorithmic acceleration," whereby the speed of cyber engagement challenges traditional deterrence and crisis-management frameworks in international security (Nye, 2017; Johnson, 2021). Consequently, cyber conflict increasingly resembles continuous competition rather than discrete incidents.

On the defensive side, states and international organizations are increasingly deploying AI-driven cybersecurity architectures designed to enhance predictive defense capabilities. AI systems are used to monitor anomalous behavior, conduct threat intelligence fusion, and prioritize incident response through automated risk assessment models. For example, cybersecurity initiatives within the European Union rely on intelligent monitoring networks capable of processing large-scale data flows across critical sectors to anticipate potential threats before operational disruption occurs (European Union Agency for Cybersecurity [ENISA], 2021). Similarly, NATO and several regional cyber defense initiatives have adopted AI-assisted situational awareness platforms to improve collective cyber resilience (Klimburg, 2020).

Empirical evidence further demonstrates the operational effectiveness of AI-enabled cyber threats. The 2021 Colonial Pipeline cyberattack in the United States illustrated how vulnerabilities in detection and response systems can generate large-scale economic and societal disruption, force the shutdown of major fuel supply infrastructure and trigger regional economic instability (CISA, 2022). Comparable incidents targeting financial institutions and digital payment infrastructures across Europe highlight how automated attack coordination can amplify systemic risks within highly interconnected economies (Singer & Friedman, 2014; Farrell & Newman, 2019).

Beyond tactical improvements, AI is fundamentally reshaping the strategic character of cyberspace conflict. Cyber power increasingly depends not only on technological infrastructure but also on data access, algorithmic capability, and analytical superiority. This shift blurs the distinction between civilian and military domains, as private technology firms, cloud providers, and data platforms become integral components of national security ecosystems (Segal, 2016; Libicki, 2021). As a result, cyber threats are evolving into persistent, low-intensity forms of strategic competition operating below the threshold of conventional warfare.

From an international relations perspective, the growing complexity and transnational nature of AI-driven cyber risks reinforce arguments advanced within new regionalism literature. Shared digital infrastructures and cross-border data flows create collective vulnerabilities that individual states struggle to manage independently. Consequently, regional cooperation mechanisms, such as information-sharing arrangements, joint cyber exercises, and harmonized regulatory frameworks, are increasingly viewed as necessary responses to technologically amplified threats (Hettne, 2005; Fawcett, 2016; Nye, 2020). AI therefore acts not only as a technological multiplier of cyber threats but also as a structural driver encouraging deeper regional security coordination.

5. Cybersecurity as a Regional Security Issue

Cybersecurity has increasingly emerged as a central component of contemporary regional security studies, reflecting a broader transformation in the understanding of security beyond traditional military threats. The expansion of digital infrastructures and the integration of cyberspace into critical national sectors, including energy systems, financial markets, telecommunications networks, and defense operations, have elevated cyber vulnerabilities to the level of strategic security concerns. Unlike conventional threats, cyber risks operate simultaneously across civilian and military domains, blurring established distinctions between internal and external security and redefining the scope of regional stability (Kello, 2017; Nye, 2020). Consequently, cybersecurity is no longer treated as a technical policy field but as a structural dimension of geopolitical competition and security governance.

Within international relations scholarship, cyberspace is increasingly conceptualized as a domain of strategic rivalry in which states compete over technological superiority, data control, and digital resilience. AI-driven capabilities further intensify this competition by enabling both persistent surveillance and scalable disruption, allowing states to exert influence below the threshold of armed conflict (Horowitz, 2018; Payne, 2021). Scholars argue that cyber operations represent a form of "gray-zone conflict," where coercion occurs without triggering traditional military escalation, thereby complicating deterrence and crisis management frameworks (Libicki, 2021). This transformation reinforces the importance of examining cybersecurity through regional analytical lenses rather than purely national ones.

From the perspective of Regional Security Complex Theory (RSCT), cybersecurity aligns closely with patterns of geographically concentrated security interdependence. Buzan and Wæver (2003) argue that security dynamics tend to cluster regionally because threats travel more rapidly among neighboring states sharing political, economic, and infrastructural linkages. In cyberspace, this regional interconnectedness is amplified through shared digital ecosystems such as cross-border energy grids, regional financial payment systems, cloud infrastructures, and telecommunications networks. Cyber incidents affecting one state can therefore generate cascading regional consequences, producing what scholars describe as "networked vulnerability" (Farrell & Newman, 2019).

Empirical evidence demonstrates that cyber disruptions frequently produce spillover effects beyond national borders. Attacks targeting logistics systems, banking networks, or digital supply chains can interrupt regional economic flows and undermine collective stability. This interconnected exposure encourages states within a region to perceive cyber risks as collective rather than individual security challenges, reinforcing RSCT's core proposition that security threats create shared regional agendas (Klimburg, 2020; ENISA, 2023).

The rise of cyber threats has simultaneously generated new forms of strategic dependence among states. Effective cybersecurity increasingly requires intelligence sharing, coordinated incident response mechanisms, harmonized regulatory frameworks, and joint capacity-building initiatives. Nye (2017) emphasizes that deterrence in cyberspace differs fundamentally from nuclear or conventional deterrence because resilience and collective defense depend on cooperation rather than unilateral capability accumulation. In this context, cybersecurity cooperation becomes both a defensive necessity and a mechanism for building trust and institutionalized interaction among regional actors.

Moreover, the borderless nature of cyberspace challenges traditional sovereignty-based security models. No state possesses full control over digital infrastructures operating within its territory, as data flows, cloud services, and software supply chains are inherently transnational (Segal, 2016; Mueller, 2022). This structural condition increases reliance on regional organizations and multilateral governance frameworks to establish norms, coordinate responses, and reduce systemic risks. Regional institutions such as the European Union, ASEAN, and NATO cyber initiatives increasingly function as platforms for cyber governance, standard-setting, and collective resilience-building (Christou, 2016; Klimburg & Zylberberg, 2019).

At a broader strategic level, the integration of artificial intelligence into military and security sectors deepens regional security interdependence. AI enhances cyber capabilities related to intelligence analysis, autonomous defense systems, and predictive threat modeling, thereby accelerating technological competition among states. However, technological competition simultaneously encourages cooperation among allies seeking interoperability and shared technological standards (Johnson, 2021; Scharre, 2023). This dual dynamic, competition alongside cooperation, reflects emerging patterns of regional security governance shaped by technological transformation.

Recent international security literature increasingly frames cybersecurity as an element of balance-of-power politics in the digital age. Cyber capabilities allow states to project influence asymmetrically, disrupt adversaries' economic systems, and shape information environments without direct military confrontation (Singer & Friedman, 2014; Lindsay, 2020). As a result, regional cyber cooperation initiatives can be interpreted not only as defensive arrangements but also as strategic instruments through which states collectively enhance bargaining power and technological resilience.

Therefore, cybersecurity should be understood as a foundational pillar of contemporary regional security architectures rather than a supplementary technical concern. The growing dependence on interconnected digital systems compels states to institutionalize cooperation mechanisms, deepen information-sharing practices, and coordinate technological governance at the regional level. As digital transformation accelerates, cybersecurity is likely to play an increasingly decisive role in shaping regional security

complexes, redefining deterrence logics, and transforming patterns of cooperation and competition within the international system.

6. Regional Cooperation in Cybersecurity: Case Studies

The transnational nature of cyber threats, coupled with the reliance of critical infrastructure on interconnected networks, has elevated regional cooperation to a strategic necessity. Such cooperation enables states to share intelligence, harmonize regulatory frameworks, and coordinate responses to sophisticated AI-driven attacks, transforming cybersecurity from a technical concern into a core element of regional security governance. This trend aligns with new regionalism theory, which emphasizes that regions are increasingly institutional actors capable of responding to complex transnational challenges (Hettne, 2005; Söderbaum, 2016).

6.1 The European Union as a Leading Model of Cybersecurity Cooperation

The European Union (EU) exemplifies advanced regional cybersecurity coordination. Through the European Union Agency for Cybersecurity (ENISA), member states have established integrated mechanisms for real-time threat intelligence sharing, coordinated incident response, and harmonized digital security standards. The EU's NIS2 Directive and the CSIRTs network provide not only technical defense but also strategic frameworks for cross-border resilience, reflecting a shift toward collective regional governance (European Commission, 2022; ENISA, 2023).

The EU has also explicitly incorporated Iranian cyber threats into its risk assessments. EU intelligence reports highlight Iran's targeting of European energy and industrial sectors, prompting joint exercises and AI-enhanced monitoring systems to anticipate and mitigate such attacks (European External Action Service, 2024). By linking regional cybersecurity to broader geopolitical risk management, the EU illustrates how AI-driven threats from middle powers like Iran influence institutional evolution, emphasizing the practical relevance of new regionalism in shaping both policy and technology deployment.

6.2 Digital Security Cooperation in Other Regional Frameworks

In Asia, ASEAN has increasingly recognized cybersecurity as a regional security priority. Initiatives such as the ASEAN Cybersecurity Cooperation Strategy and regional simulation exercises foster information exchange, develop joint protocols, and build capacity to respond to cross-border threats (ASEAN Secretariat, 2022). ASEAN's framework explicitly considers the risks posed by Iran-aligned APT groups targeting financial, energy, and maritime systems, highlighting the need for intelligence sharing and early warning systems (Kshetri, 2021).

Similarly, in the Middle East, emerging alliances such as the Bab el-Mandeb Digital Security Alliance illustrate regional collaboration on maritime infrastructure protection, particularly against AI-enhanced cyber campaigns that could originate from Iran or affiliated actors. These initiatives integrate AI analytics to detect anomalies and simulate potential attack scenarios, demonstrating how technology and regional governance intersect to address both immediate and systemic cyber risks (Singer & Friedman, 2014; Microsoft Threat Intelligence, 2024).

These cases illustrate that regional cooperation is not limited to operational coordination; it functions as a strategic buffer against technologically sophisticated actors whose actions transcend borders. By pooling expertise and leveraging AI-based detection, regional frameworks can reduce vulnerability to asymmetric threats, particularly from Iran, where cyber operations are increasingly used as instruments of both disruption and influence.

6.3 The Importance of Regional Cooperation within the New Regionalism

From a theoretical perspective, regional cooperation under new regionalism extends beyond the technical domain to encompass political, strategic, and technological dimensions. AI-driven cyber threats, particularly those associated with Iran, reinforce interdependence among regional actors and incentivize the development of institutional mechanisms to share intelligence, standardize defenses, and conduct joint exercises (Hettne, 2005; Nye, 2020). EU and ASEAN experiences demonstrate that regions facing shared vulnerabilities are more likely to transform cyber threats into opportunities for institutional innovation, resilience, and strategic integration

Moreover, the Iranian case underscores how cyber interdependence shapes regional security calculus. AI-enhanced cyber-attacks can produce cascading effects across energy, finance, and maritime networks, compelling states to coordinate policies and develop joint deterrence strategies. Regional cooperation thus emerges as both a defensive necessity and a strategic tool, mitigating risk while promoting broader integration of security governance in line with new regionalism principles (Klimburg, 2020; Rid, 2020).

In conclusion, empirical evidence suggests that regional cooperation is essential in addressing the complexity of AI-driven cyber threats. Institutions such as the EU and ASEAN not only enhance operational resilience but also illustrate how strategic adaptation to Iranian cyber activity fosters regional interdependence, technological innovation, and the evolution of collective security mechanisms.

7. ANALYSIS OF RESULTS AND DISCUSSION

The findings of this study confirm that artificial intelligence (AI) has fundamentally transformed the nature of cyber threats, compelling states to reconsider and reformulate their regional security frameworks. AI-driven cyberattacks possess unprecedented precision, predictive capability, and propagation speed across complex digital networks, making isolated national responses insufficient and often ineffective (Horowitz, 2018; Singer & Friedman, 2014; Kshetri, 2021). This technological shift amplifies the strategic significance of regional collaboration, particularly in geographically interconnected and economically interdependent regions.

From the perspective of Regional Security Complex Theory (RSCT), the interdependence among states is intensified by the transnational character of AI-enhanced cyber operations. A single cyber incident, such as attacks on energy grids or financial infrastructure, can produce cascading effects that affect multiple countries simultaneously, necessitating coordinated strategies for defense, mitigation, and resilience (Buzan & Wæver, 2003; Buchanan, 2020). Evidence from the European Union (EU) demonstrates that institutionalized cooperation, including cyber emergency response teams, real-time intelligence sharing, and AI-driven threat analytics, enhances collective situational awareness and strengthens resilience against Iranian cyber campaigns targeting European critical infrastructure (European Union Agency for Cybersecurity [ENISA], 2021; European External Action Service, 2024).

Similarly, ASEAN exemplifies the regionalization of cyber defense within a diverse technical and political landscape. Its initiatives to establish regional information-sharing systems, organize joint simulations, and harmonize incident response reflect a strategic adaptation to the risks posed by AI-augmented cyber operations, including those attributed to Iranian actors targeting maritime, energy, and financial sectors (ASEAN Secretariat,

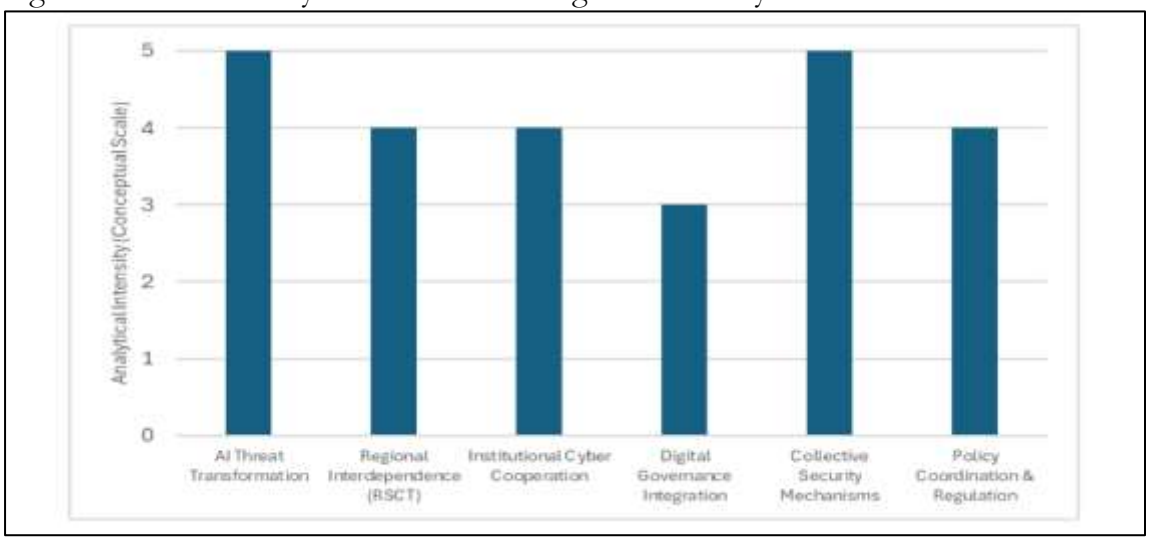
2022; Microsoft Threat Intelligence, 2024). These measures indicate that regional cooperation is not merely reactive but functions as a proactive mechanism to transform asymmetric technological threats into a coordinated security strategy, enhancing both institutional capacity and strategic deterrence.

The integration of AI into cybersecurity reshapes not only technical defense measures but also the institutional foundations of regional security governance. Mechanisms developed under the EU and ASEAN frameworks extend beyond immediate incident response to include predictive threat assessment, regulatory harmonization, and the development of common standards for data sharing. Such systemic coordination illustrates how technological innovation interacts with political and organizational structures, confirming the theoretical synthesis of RSCT and new regionalism in explaining collective security evolution (Hettne, 2005; Nye, 2020; Klimburg, 2020).

The Iranian cyber dimension further accentuates the urgency of these developments. Iran's AI-assisted cyber operations, ncluding automated reconnaissance, AI-generated spear-phishing, and hybrid campaigns combining information operations and infrastructure attacks, highlight the asymmetric capabilities middle powers can deploy to challenge regional security (Bradshaw & Howard, 2019; Rid, 2020). The persistent threat posed by Iranian actors has incentivized the EU and ASEAN states to develop institutionalized cooperation mechanisms, demonstrating that collective regional governance is essential for maintaining strategic stability and mitigating cascading cyber risks.

In conclusion, the evidence confirms that AI-driven cyber threats function as a catalyst for regional security innovation. The study supports the central hypothesis that the rise of these technologically sophisticated threats drives states toward the formation of formal regional collective security mechanisms. By combining RSCT with new regionalism, this research highlights the critical role of institutional, technological, and strategic cooperation in enhancing resilience against complex, cross-border cyber threats. The EU and ASEAN cases illustrate that regional cooperation, particularly in response to Iranian cyber operations, is increasingly a structural necessity rather than a discretionary choice, reinforcing the notion that AI is not only altering cyberattack techniques but reshaping the architecture of regional security itself (Singer & Friedman, 2014; European External Action Service, 2024).

Figure 2: AI-Driven Cyber Threats and Regional Security Transformation



Source : compiled by the author

The analytical figure translates the discussion findings into conceptual analytical dimensions that support the theoretical interpretation of the study. The values presented in the figure do not represent statistical data; rather, they reflect an analytical intensity scale (1–5) indicating the relative prominence of each dimension within the study's results.
It demonstrates how AI-driven cyber threats reshape regional security through six interconnected dimensions: the transformation of cyber threats, regional security interdependence within the framework of Regional Security Complex Theory (RSCT), institutional cybersecurity cooperation, digital governance integration, regional collective security mechanisms, and policy coordination and regulation.

8. CONCLUSION

The study concluded that artificial intelligence (AI) has fundamentally transformed the nature of cyber threats, making digital security management more complex and transnational. It demonstrated that these transformations have prompted states to reconsider their national security strategies, enhance regional cooperation through the establishment of joint information-sharing mechanisms, develop cyber emergency response teams, and adopt AI technologies for monitoring and preventative analysis (Horowitz, 2018; European Union Agency for Cybersecurity, 2021).

From the perspective of Regional Security Clusters Theory (RSCT), the findings reflect the interconnected nature of security interdependencies among states within a region. Any cyber threat to one state has repercussions for neighboring states, making regional cooperation a crucial element in maintaining shared security (Buzan & Wæver, 2003). In light of the literature on New Regionalism, it is clear that regional cooperation is not limited to defense but also includes developing unified institutional policies, information-sharing standards, and joint strategies to counter transnational threats (Hettne, 2005; Fawcett, 2016).

The findings also indicate that integrating artificial intelligence (AI) into cybersecurity systems enhances states' ability to predict and respond to threats more quickly, thereby reducing individual risks and strengthening regional collective security. The study further confirms that regional cooperation is a strategic tool for reshaping regional security in the face of modern technological challenges, reflecting the gap identified in previous literature regarding the relationship between AI, cyber threats, and regional security arrangements.

Recommendations:
1. Enhance the exchange of cyber information and data among states within regions, while establishing clear regulatory frameworks to ensure transparency and confidentiality.
2. Invest in AI tools for preventative and offensive cyber analysis, while developing shared capabilities among regional states. • Focus on building institutional frameworks within the new regional context to enhance security cooperation and coordination, including joint training and the exchange of expertise.
3. Encourage future research to examine the impact of other technological developments, such as deep learning and the Internet of Things, on regional security arrangements, to ensure the continued relevance of security policies in the future.

References:

1. Allen, G., & Chan, T. (2017). Artificial intelligence and national security. Center for a New American Security.
2. ASEAN Secretariat. (2022). ASEAN *cybersecurity cooperation strategy report.* ASEAN Secretariat.
3. Bradshaw, S., & Howard, P. N. (2019). The global disinformation order. Oxford Internet Institute.
4. 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., Steinhardt, J., Flynn, C., Ó hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. Future of Humanity Institute, University of Oxford.
5. Buchanan, B. (2020). The hacker and the state: *Cyber attacks and the new normal of geopolitics*. Harvard University Press.
6. Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge University Press.
7. Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.
8. Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. European Politics and Society, 17(3), 346–361. https://doi.org/10.1080/23745118.2016.1154198
9. Cybersecurity and Infrastructure Security Agency. (2022). *Colonial pipeline cyber incident review*. U.S. Department of Homeland Security.
10. Cybersecurity and Infrastructure Security Agency. (2023). *AI and cybersecurity risk landscape report*. U.S. Department of Homeland Security.
11. European Commission. (2022). *NIS2 directive and EU cybersecurity framework*. European Commission.
12. European External Action Service. (2024). Cyber threat assessments and strategic guidance. European External Action Service.
13. European Union Agency for Cybersecurity. (2021). ENISA threat landscape 2021: *Cybersecurity challenges and trends in the EU*. Publications Office of the European Union.
14. European Union Agency for Cybersecurity. (2023). *Cybersecurity threat landscape 2023*. Publications Office of the European Union.
15. Fawcett, L. (2016). *International relations of the Middle East* (4th ed.). Oxford University Press.
16. Hettne, B. (2005). Beyond the "new" regionalism. New Political Economy, 10(4), 543–571. https://doi.org/10.1080/13563460500344484
17. Horowitz, M. C. (2018). *Artificial intelligence, international competition, and the balance of power*. Texas National Security Review, 1(3), 36–57.
18. International Institute for Strategic Studies. (2021). *Cyber power index 2021*. IISS.
19. Johnson, J. (2021). *Artificial intelligence and the future of warfare*. Journal of Strategic Studies, 44(4), 593–618. https://doi.org/10.1080/01402390.2020.1780815
20. Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
21. Klimburg, A. (2020). The darkening web: The war for cyberspace. Penguin Press.
22. Klimburg, A., & Zylberberg, H. (2019). *Cyber security capacity building and regional organizations*. Global Policy, 10(1), 45–58. https://doi.org/10.1111/1758-5899.12635
23. Kshetri, N. (2021). *Artificial intelligence in cybersecurity: Opportunities and challenges*. IEEE Security & Privacy, 19(2), 55–63. https://doi.org/10.1109/MSEC.2020.3040357
24. Libicki, M. C. (2021). *Cyberspace in peace and war*. Naval Institute Press.
25. Lindsay, J. R. (2020). *Cyber operations and strategic stability. International Security*, 45(1), 7–49. https://doi.org/10.1162/isec_a_00377

26. Microsoft Threat Intelligence. (2024). *Iranian cyber operations and regional security dynamics*. Microsoft.
27. Nye, J. S. (2017). *Deterrence and dissuasion in cyberspace.* International Security, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266
28. Nye, J. S. (2020). *Power and interdependence with cyberspace*. Foreign Affairs, 99(6), 64–75.
29. Payne, K. (2021). *Artificial intelligence: A revolution in strategic affairs? Survival*, 63(5), 7–32. https://doi.org/10.1080/00396338.2021.1989368
30. Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare*. Farrar, Straus and Giroux.
31. Scharre, P. (2023). *Four battlegrounds: Power in the age of artificial intelligence*. W. W. Norton.
32. Segal, A. (2016). *The hacked world order*. PublicAffairs.
33. Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
34. Stockholm International Peace Research Institute. (2019). *Artificial intelligence, strategic stability and nuclear risk*. SIPRI.