Middle East Journal of Humanities and Cultural Studies
Homepage: http://meijournals.com/ar/index.php/mejljs/index
ISSN: 2710-2238 (PRINT)
ISSN: 2788-4686 (ONLINE)
مجلة الشرق الأوسط
للعلوم الإنسانية والثقافية

Policies for Addressing Cybersecurity Challenges in the European Union

Asst. Prof. Dr. Senaa Ali Mahmood
Department of Political Systems and Public Policies College of Political Science Al-Nahrain University

استلام البحث:12-06-2026 مراجعة البحث :11-07-2026 قبول البحث:05-08-2026

الملخص

تتناول هذه الدراسة سياسات الاتحاد الأوروبي في مواجهة التحديات السيبرانية من خلال تحليل الإطار المؤسسي الذي تستند إليه هذه السياسات، وتقييم فاعلية السياسة العامة في التعامل مع التهديدات السيبرانية المتزايدة. وانطلاقًا من تزايد أهمية الأمن السيبراني بوصفه أحد المرتكزات الأساسية للاستقرار السياسي والاقتصادي والرقمي، عمل الاتحاد الأوروبي على تطوير إطار متكامل يضم المؤسسات والتشريعات والآليات التنظيمية الهادفة إلى تعزيز الأمن الرقمي، وتحسين مستوى التنسيق بين مؤسسات الاتحاد والدول الأعضاء، ورفع القدرة على الوقاية من المخاطر السيبرانية والاستجابة لها.

كما يوضح التحليل طبيعة التحديات السيبرانية وتأثيرها في عملية صنع السياسة العامة الأوروبية، مع التركيز على دور وكالة الاتحاد الأوروبي للأمن السيبراني (ENISA) في دعم الحوكمة الرقمية، وتعزيز التعاون المؤسسي، وتبادل المعلومات، وبناء القدرات اللازمة لمواجهة التهديدات الرقمية. فضلًا عن ذلك، تستعرض الدراسة أبرز التطورات التشريعية في هذا المجال، ولا سيما توجيه أمن الشبكات والمعلومات (NIS2 Directive) وقانون المرونة السيبرانية.(Cyber Resilience Act)

وتشير النتائج إلى أن الاتحاد الأوروبي نجح في بناء إطار مؤسسي وتشريعي متقدم نسبيًا في مجال الأمن السيبراني، إلا أن تحقيق مستويات أعلى من فاعلية السياسة العامة ما يزال يتطلب تعزيز التكامل المؤسسي، وتقليص الفجوات في القدرات بين الدول الأعضاء، وتطوير آليات التنسيق والاستجابة بما ينسجم مع التطور المتسارع للتهديدات السيبرانية.

الكلمات المفتاحية: الاتحاد الأوروبي، الأمن السيبراني، السياسة العامة، الحوكمة الرقمية.

Abstract:

This study examines the European Union's policies for addressing cybersecurity challenges through an analysis of the institutional framework underpinning these policies and an assessment of the effectiveness of public policy in responding to the growing spectrum of cyber threats. As cybersecurity has emerged as a fundamental pillar of political, economic, and digital stability, the European Union has progressively developed an integrated framework of institutions, legislation, and regulatory mechanisms aimed at strengthening digital security, enhancing coordination among EU institutions and Member States, and improving their capacities to prevent, mitigate, and respond to cyber risks.

The study further explores the nature of cybersecurity challenges and their influence on European public policymaking, with particular emphasis on the role of the European Union Agency for Cybersecurity (ENISA) in advancing digital governance, fostering institutional cooperation, facilitating information sharing, and strengthening institutional capabilities. It also reviews the most significant legislative developments in this field, particularly the Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive) and the Cyber Resilience Act. The findings indicate that the European Union has succeeded in establishing a relatively advanced institutional and legislative framework for cybersecurity. Nevertheless, achieving higher levels of policy effectiveness requires deeper institutional integration, reducing disparities among Member States, and further enhancing coordination and response mechanisms to keep pace with the rapidly evolving cyber threat landscape.

Keywords : European Union, Cybersecurity, Public Policy, Digital Governance.

Introduction

Cybersecurity challenges have become one of the most prominent issues on the European Union's policy agenda. They are no longer perceived merely as technical threats but as multidimensional challenges that directly affect the Union's political and institutional structures, as well as the resilience and responsiveness of the European governance system. Consequently, the European Union has adopted a comprehensive cybersecurity public policy aimed at strengthening resilience, enhancing prevention and response capabilities, and improving coordination among European institutions and Member States.

The significance of this topic stems from the fact that cybersecurity has evolved beyond a narrowly defined technical policy domain to become an integral component of the European Union's broader public policy framework. Its growing importance is closely linked to the continuity of critical services, public trust, the protection of the digital economy, and the cohesion of the European political and digital space. Accordingly, examining cybersecurity policy from both institutional and public policy perspectives provides a deeper understanding of how policy decisions are formulated, institutional responsibilities are allocated, and cyber threats are transformed into coordinated and actionable collective responses

Research Problem

The research problem lies in the gap between the European Union’s ambition to establish a unified cybersecurity policy and the practical realities of its implementation, which continue to be constrained by disparities in the capabilities of Member States, the complexity of coordination processes, and the multi-level governance structure of the European Union. Despite significant institutional efforts, the persistence of cybersecurity challenges indicates that the practical effectiveness of the Union’s cybersecurity policy still requires greater institutional integration and policy cohere

Significance of the Study

This study is significant because it addresses one of the most critical and sensitive areas of contemporary public policy: cybersecurity, which has become a key component of governance and institutional capacity within the European Union. It also examines the relationship between institutional structures and public policy effectiveness, demonstrating how cyber threats can serve as catalysts for strengthening coordination mechanisms, improving institutional resilience, and enhancing collective response capabilities.

Objectives of the Study

The study seeks to achieve the following objectives:

1.To analyze the institutional framework underpinning the European Union's policies for addressing cybersecurity challenges.

2.To examine the mechanisms of decision-making and coordination between European institutions and Member States.

3.To evaluate the effectiveness of European public policy in responding to cybersecurity challenges.

4.To identify the principal determinants of policy success, highlight existing shortcomings, and explore future prospects for the development of European cybersecurity policy.

Research Hypothesis

The study is based on the hypothesis that, although the European Union possesses a relatively advanced institutional framework for cybersecurity governance, the effectiveness of its cybersecurity policy remains constrained by disparities in national capabilities, the complexity of multi-level decision-making processes, and the challenges of reconciling the Union's common strategic vision with the practical requirements of implementation across Member States.

Research Methodology

This study adopts a descriptive-analytical approach, complemented by an institutional perspective to examine coordination mechanisms and decision-making processes within the European Union. It further relies on the analysis of official documents, legislative instruments, policy strategies, and reports issued by the European Union and the European Union Agency for Cybersecurity (ENISA). In addition, comparative reports are utilized to assess the effectiveness of European cybersecurity policy and identify the principal challenges affecting its implementation.

Research Problem

The research problem lies in the gap between the European Union's ambition to establish a unified cybersecurity policy and the practical realities of its implementation, which continue to be constrained by disparities in the capabilities of Member States, the complexity of coordination processes, and the multi-level governance structure of the European Union. Despite significant institutional efforts, the persistence of cybersecurity challenges indicates

that the practical effectiveness of the Union's cybersecurity policy still requires greater institutional integration and policy coherence.

Significance of the Study

This study is significant because it addresses one of the most critical and sensitive areas of contemporary public policy: cybersecurity, which has become a key component of governance and institutional capacity within the European Union. It also examines the relationship between institutional structures and public policy effectiveness, demonstrating how cyber threats can serve as catalysts for strengthening coordination mechanisms, improving institutional resilience, and enhancing collective response capabilities.

Objectives of the Study

The study seeks to achieve the following objectives:

1.To analyze the institutional framework underpinning the European Union's policies for addressing cybersecurity challenges.

2.To examine the mechanisms of decision-making and coordination between European institutions and Member States.

3.To evaluate the effectiveness of European public policy in responding to cybersecurity challenges.

4.To identify the principal determinants of policy success, highlight existing shortcomings, and explore future prospects for the development of European cybersecurity policy.

Research Hypothesis

The study is based on the hypothesis that, although the European Union possesses a relatively advanced institutional framework for cybersecurity governance, the effectiveness of its cybersecurity policy remains constrained by disparities in national capabilities, the complexity of multi-level decision-making processes, and the challenges of reconciling the Union's common strategic vision with the practical requirements of implementation across Member States.

Research Methodology

This study adopts a descriptive-analytical approach, complemented by an institutional perspective to examine coordination mechanisms and decision-making processes within the European Union. It further relies on the analysis of official documents, legislative instruments, policy strategies, and reports issued by the European Union and the European Union Agency for Cybersecurity (ENISA). In addition, comparative reports are utilized to assess the

effectiveness of European cybersecurity policy and identify the principal challenges affecting its implementation.

First Section

The Institutional Framework of European Union Policies for Addressing Cybersecurity Challenges

Over the past two decades, the European Union has undergone a significant transformation in its understanding of cybersecurity. Rather than being viewed solely as a specialized technical issue, cybersecurity is now recognized as a fundamental component of security, stability, and digital governance.

The rapid evolution of the digital environment, the growing dependence on information infrastructure, and the increasing frequency of cross-border cyberattacks have created an urgent need for an institutional framework capable of managing cyber risks, enhancing resilience, and ensuring the continuity of critical services.

Within this context, the European Union has developed an integrated institutional framework based on close cooperation between EU institutions and Member States. This framework is designed to formulate public policies that are better equipped to address cybersecurity challenges while strengthening coordination, cooperation, and collective response capabilities across the Union.

First Subsection

Cybersecurity Challenges as a Critical Input to the European Political System

In recent years, cyberspace has emerged as one of the most rapidly expanding domains of security threats within the European Union. Cyberattacks are no longer regarded as isolated technical incidents; rather, they have evolved into strategic pressures that shape public policymaking, influence priority setting, and redefine the relationship between security, stability, and interdependence within the European governance system[1].

This transformation demonstrates that cybersecurity challenges are no longer confined to the technical sphere. Instead, they constitute political and institutional threats that directly affect the European Union's capacity to perform its core functions. Large-scale cyber intrusions, disruptions of digital infrastructure, and attacks targeting critical services have immediate

[1].European Commission, The EU's Cybersecurity Strategy for the Digital Decade, Brussels: European Commission, 2020, pp. 1-7.

consequences for public trust, the continuity of essential services, and the European Union's credibility as an actor capable of safeguarding its societies and digital economy[2].

The significance of these challenges has further increased because cyberspace is intrinsically linked to critical sectors, including energy, transportation, telecommunications, financial services, and digital public administration. Consequently, safeguarding these sectors has become a central objective of the European Union's strategy to protect the digital economy, ensure the uninterrupted provision of public services, and strengthen resilience against increasingly sophisticated cyber threats[3].

Moreover, the rapid advancement of digital technologies—including artificial intelligence (AI), cloud computing, and the Internet of Things (IoT)—has significantly increased the complexity of the cyber environment. This evolution has generated new categories of cyber threats that require more sophisticated and coordinated responses at both the national and European levels[4].

From an institutional and political perspective, cybersecurity threats constitute critical inputs that place considerable pressure on the European political system. They compel European institutions and Member States to formulate public policies capable of responding rapidly to emerging risks while strengthening coordination, information sharing, and institutional cooperation. As the scale and sophistication of cyber threats continue to increase, so does the need for more effective mechanisms for prevention, preparedness, incident response, and post-incident recovery[5].

The implications of these challenges extend well beyond the immediate security dimension. They directly influence confidence in the European digital environment and affect the European Union's ability to safeguard its economic and political interests within an increasingly competitive and complex international system. Consequently, cybersecurity challenges have become an important driver in redefining the balance between national sovereignty and the requirements of collective action within the European Union[6].

[2] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, Athens: ENISA, 2023, pp. 9-15.

[3] P. W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford: Oxford University Press, 2014, pp. 67-74.

[4]Myriam Dunn Cavelty, Cybersecurity: Politics, Governance and Cooperation, London: Routledge, 2018, pp. 145-152.

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, 2022.

[6] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, Athens: ENISA, 2023, pp. 20-25. .

Accordingly, examining cybersecurity challenges as a critical input to the European political system provides deeper insight into the formulation of public policy within the European Union It also illustrates how pressures arising from the digital environment are translated into institutional and legislative responses designed to strengthen resilience, enhance preparedness, and reinforce cybersecurity across the Union[7].

Accordingly, examining cybersecurity challenges as a critical input to the European political system provides deeper insight into the formulation of public policy within the European Union It also illustrates how pressures arising from the digital environment are translated into institutional and legislative responses designed to strengthen resilience, enhance preparedness, and reinforce cybersecurity across the Union[8].

Second Subsection

Decision-Making and Coordination Mechanisms within the European Union

European cybersecurity policy is founded upon a complex network of institutions and stakeholders. Rather than being governed by a single centralized authority, cybersecurity governance within the European Union operates through a multi-level institutional framework that encompasses the European Commission, the European Council, the European Parliament, the Member States, and the European Union Agency for Cybersecurity (ENISA)[9].

This institutional arrangement gives European cybersecurity policy a collaborative character that reflects the fundamental nature of the European Union as a political entity based on the shared exercise of competences between the supranational and national levels of governance[10].

The European Commission plays a central role in proposing cybersecurity policies and legislative initiatives while developing comprehensive strategies aimed at strengthening digital security and protecting critical infrastructure. In addition, it oversees the implementation of

[7] . European Commission, The EU's Cybersecurity Strategy for the Digital Decade, op. cit., pp. 8-12.
[8]Myriam Dunn Cavelty, Cybersecurity: Politics, Governance and Cooperation, op. cit., pp. 145-152. .
[9] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, op. cit., pp. 15-20.
[10] Simon Hix and Bjørn Høyland, The Political System of the European Union, London: Palgrave Macmillan, 2022, pp. 180-188.

these policies and monitors Member States' compliance with the relevant European regulatory frameworks[11].

The European Union Agency for Cybersecurity (ENISA) constitutes one of the Union's principal specialized institutions in this field. It supports Member States and European institutions by providing technical expertise, preparing analytical studies and strategic reports, facilitating the exchange of information and best practices, and strengthening preparedness and incident-response capabilities across the European cybersecurity ecosystem[12].

The European institutional framework has undergone significant development following the adoption of the Cybersecurity Act, which considerably strengthened ENISA's mandate and consolidated its position as the central institution supporting the European Union's cybersecurity architecture and policy implementation[13].

In parallel, the European Union has established a range of coordination mechanisms and cooperative networks designed to enhance collaboration among Member States. Among the most significant are the National Coordination Centres for Cybersecurity, which serve as institutional links between national authorities and European institutions. These centres contribute to strengthening national capabilities, promoting the exchange of expertise, and coordinating responses to shared cybersecurity threats[14].

Within the broader development of European cyber governance, the NIS2 Directive has emerged as one of the Union's most significant contemporary regulatory instruments. The Directive broadens the range of sectors covered by cybersecurity obligations, reinforces risk-management requirements, strengthens incident-reporting obligations, and harmonizes core cybersecurity standards across Member States.In doing so, it reduces regulatory fragmentation and promotes greater institutional coherence throughout the European Union[15].

The NIS2 Directive therefore represents a major step toward establishing a more integrated European framework for cybersecurity governance. It strengthens the responsibilities of national authorities, increases the legal obligations imposed on operators of essential and

[11] Liesbet Hooghe and Gary Marks, Multi-Level Governance and European Integration, Lanham: Rowman & Littlefield, 2001, pp. 25-40.
[12] European Commission, Cybersecurity Policies, Brussels: European Commission, 2024.
[13] European Union Agency for Cybersecurity (ENISA), About ENISA – The EU Agency for Cybersecurity, Athens: ENISA, 2024.
[14]European Union Agency for Cybersecurity (ENISA), National Coordination Centres and Cybersecurity Governance in the EU, Athens: ENISA, 2023.
[15] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, 2022.

important entities, and provides a more robust foundation for cross-border cooperation in addressing common cyber risks[16].

Overall, this institutional architecture demonstrates that the European Union does not rely on a model of strict centralized control. Instead, it adopts a network governance approach founded on knowledge sharing, policy coordination, institutional cooperation, and the distribution of responsibilities among a diverse range of actors. This governance model is particularly well suited to the dynamic, complex, and transnational nature of contemporary cybersecurity threats[17].

Accordingly, the European Union's decision-making and coordination mechanisms constitute the cornerstone of its cybersecurity public policy. They provide the institutional framework through which strategic objectives are translated into practical policies and operational measures while ensuring coherence between the Union's common strategic vision and the diverse national capabilities of its Member States.[18].

Second Section

The Effectiveness of European Public Policy in Addressing Cybersecurity Challenges

European public policy in the field of cybersecurity has undergone significant development in recent years, reflecting the growing awareness among European institutions and Member States of the increasing risks posed by the contemporary digital environment. This evolution has been manifested in the adoption of comprehensive strategies, legislative instruments, and institutional initiatives aimed at strengthening capabilities for prevention, response, and recovery, while fostering higher levels of coordination and cooperation among the various actors involved.

This development also reflects the European Union's transition from a narrow focus on protecting digital systems to a broader approach centered on building cyber resilience and enhancing the capacity of institutions and societies to adapt to an evolving cyber threat landscape.

Nevertheless, evaluating the effectiveness of this policy requires an examination of both its determinants of success and the challenges that continue to impede its practical implementation.

[16] European Commission, NIS2 Directive: Strengthening Cybersecurity across the EU, Brussels: European Commission, 2023.
[17] Simon Hix and Bjørn Høyland, The Political System of the European Union, op. cit., pp. 180-188. .
[18] 7.Myriam Dunn Cavelty, Cybersecurity: Politics, Governance and Cooperation, op. cit., pp. 145–152.

The existence of sophisticated legislative and institutional frameworks alone cannot guarantee cybersecurity unless they are accompanied by effective implementation capacities and sustained coordination across all levels of governance.

First Subsection

Determinants of the Effectiveness of European Public Policy in Addressing Cybersecurity Challenges

The effectiveness of European public policy in the field of cybersecurity depends largely on the ability of European institutions and Member States to translate strategic objectives into measurable and sustainable outcomes. The existence of strategies and legislative frameworks alone does not ensure cybersecurity unless these are supported by effective implementation capacities and clearly defined coordination mechanisms across different institutional levels[19].

Institutional preparedness constitutes one of the most important determinants of policy effectiveness. The European Union's ability to address cybersecurity threats depends on the existence of institutions capable of assessing risks, developing policies, providing technical assistance, and managing cyber crises effectively. Within this framework, the European Union Agency for Cybersecurity (ENISA) plays a pivotal role in strengthening the institutional capacities of Member States while promoting the exchange of expertise, knowledge, and best practices across the Union[20].

Another decisive factor is the degree of integration among the various levels of governance within the European Union. The greater the coordination between European institutions and national authorities, the stronger the Union's capacity to mount a coherent and collective response to cybersecurity threats. Conversely, institutional fragmentation or weak coordination may create vulnerabilities that undermine both prevention and response efforts[21].

Information sharing and early warning mechanisms also constitute fundamental components of successful European cybersecurity policy. The rapid detection of cyber risks and the timely dissemination of relevant information significantly reduce potential damage and improve collective response capabilities. Consequently, the European Union has developed common

[19].European Commission, The EU's Cybersecurity Strategy for the Digital Decade, op. cit., pp. 10- 15.
[20] Directive (EU) 2022/2555 of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive), Official Journal of the European Union, 2022.
[21] European Union Agency for Cybersecurity (ENISA), 4.ENISA Annual Report 2023, Athens: ENISA, 2024, pp. 10–20.

mechanisms for cybersecurity information sharing and has strengthened cooperation among competent authorities at both the national and European levels[22].

Institutional trust represents another essential determinant of policy effectiveness. Given that cybersecurity inherently depends upon continuous cooperation and the exchange of sensitive information, mutual trust among institutional actors is indispensable for effective governance. Higher levels of transparency and institutional confidence enhance collective resilience and improve the effectiveness of coordinated responses to cyber threats[23].

The effectiveness of European public policy is also shaped by the broader international environment and rapidly evolving geopolitical dynamics. Cyber threats have increasingly become instruments of international competition and hybrid conflict, requiring the European Union to continuously strengthen its institutional and technological capabilities in order to safeguard its digital security and strategic interests[24].

The transformation of the international system and the growing use of cyberspace as a domain of strategic competition have elevated cybersecurity from a purely technical issue to a core component of national security, political stability, and economic resilience. Consequently, the European Union has intensified its efforts to reinforce both its defensive and regulatory capacities through legislative reforms, deeper cooperation among Member States, and the development of more adaptive mechanisms capable of addressing emerging cyber risks[25].

Accordingly, the effectiveness of European public policy in addressing cybersecurity challenges is determined by several interrelated factors, including the strength of the institutional framework, the degree of integration among governance actors, the efficiency of information-sharing mechanisms, the level of institutional trust, and the capacity to adapt to the continuously evolving digital environment[26].

Second Subsection

[22] Liesbet Hooghe and Gary Marks, Multi-Level Governance and European Integration, op. cit., pp. 33–45.
[23].European Union Agency for Cybersecurity (ENISA), Cybersecurity Cooperation: Information Sharing and Situational Awareness, Athens: ENISA, 2023.
[24] Myriam Dunn Cavelty, Cybersecurity: Politics, Governance and Cooperation, op. cit., pp. 145–152.
[25] .P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What 9.Everyone Needs to Know, op. cit., pp. 150–160.
[26] Everyone Needs to Know, op. cit., pp. 150–160.

Future Challenges and Prospects for the Development of European Public Policy

Despite the substantial progress achieved in European cybersecurity policy, the European Union continues to face a range of future challenges arising from the rapid pace of technological advancement, the increasing sophistication of cyber threats, and the expanding reliance on emerging digital technologies across critical sectors[27].

The continuously evolving digital environment requires the European Union to update and refine its cybersecurity policies on an ongoing basis. Cyber threats are inherently dynamic and adaptive, making effective policy responses dependent upon the capacity of European institutions to innovate, anticipate emerging risks, and adjust their regulatory and operational frameworks accordingly.

One of the most pressing challenges is the widening gap between the rapid evolution of cyber threats and the comparatively slower pace at which public institutions are able to develop legislation and policy responses. Threat actors increasingly employ advanced technologies—including artificial intelligence (AI), big data analytics, and hybrid cyber operations—whereas governmental institutions often require considerably more time to formulate and implement appropriate legal and regulatory measures[28].

Another significant challenge lies in the disparities among Member States regarding technological capabilities, human resources, and institutional preparedness. While some Member States possess highly advanced cybersecurity infrastructures and expertise, others continue to face structural limitations related to technical capacity, financial resources, and specialized personnel. These disparities inevitably affect the consistency and effectiveness of implementing common European cybersecurity policies[29].

To address these challenges, the European Union adopted the Cyber Resilience Act, representing a major legislative milestone in strengthening the security of digital products and services within the European internal market. The Act establishes harmonized cybersecurity

[27] European Commission, Cybersecurity Policies, Brussels: European Commission, 2024.
[28] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2023, op. cit., pp. 40–45.
[29] European Union Agency for Cybersecurity (ENISA), National Cybersecurity Strategies in the EU, Athens: ENISA, 2023, pp. 30–35.

requirements applicable throughout the lifecycle of products with digital elements, thereby enhancing protection and reducing vulnerabilities associated with cybersecurity risks[30].

The Cyber Resilience Act also reflects a significant shift in the philosophy of European public policy. Rather than focusing primarily on responding to cyber incidents after they occur, the legislation emphasizes the integration of cybersecurity requirements from the earliest stages of product design, development, and production. This preventive and proactive approach substantially strengthens the resilience of the European digital ecosystem[31].

Furthermore, the evolving international digital environment requires the European Union to reinforce the concept of digital sovereignty by investing in innovation, advanced technologies, and highly skilled human capital while reducing dependence on external suppliers in strategically important sectors related to digital security[32].

The future development of European public policy also requires strengthening network governance, expanding cooperation between European institutions and Member States, improving information-sharing and early-warning mechanisms, and enhancing education, training, and capacity-building initiatives. These measures will contribute to higher levels of institutional preparedness and more effective collective responses to emerging cyber threats[33].

Accordingly, the future of European public policy in addressing cybersecurity challenges will depend largely on the European Union's ability to develop a more integrated, resilient, and proactive governance model that combines institutional, legislative, and technological

[30] Regulation (EU) 2024/2847 of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act), Official Journal of the European Union, 2024.

[31] European Commission, Cyber Resilience Act: Protecting Consumers and Businesses from Cyber Threats, Brussels: European Commission, 2024.

[32] European Commission, 2030 Digital Compass: The European Way for the Digital Decade, Brussels: European Commission, 2021, pp. 10–15.

[33] European Union Agency for Cybersecurity (ENISA), ENISA Work Programme 2024, Athens: ENISA, 2024.

advancement while maintaining an appropriate balance between digital security, innovation, and sustainable development[34].

Conclusion

This study concludes that cybersecurity challenges have become one of the most significant pressures confronting the European Union, not merely as digital security concerns but as strategic factors that directly influence governance structures, coordination mechanisms, and the capacity of the European political system to respond effectively to contemporary challenges.

The findings demonstrate that the European Union no longer regards cybersecurity as an isolated technical issue. Instead, it has become an integral component of the Union's public policy framework, within which European institutions and Member States interact through a system of multi-level governance.

The study further reveals that the European institutional framework—particularly the European Union Agency for Cybersecurity (ENISA)—has played a crucial role in enhancing coordination, facilitating information sharing, strengthening preparedness, and building institutional capacity. Nevertheless, the practical effectiveness of European cybersecurity policy continues to be influenced by disparities in national capabilities and variations in technological and institutional development across Member States.

The research also indicates that the success of European cybersecurity policy depends not only on the existence of advanced legislative and strategic frameworks but, more importantly, on the ability of European and national institutions to translate these strategies into effective, sustainable, and adaptable policy measures capable of responding to the evolving digital environment.

Furthermore, recent legislative initiatives, particularly the NIS2 Directive and the Cyber Resilience Act, represent significant advances toward establishing a more integrated European cybersecurity framework by strengthening digital governance, enhancing protection standards, and improving coordination and collective response mechanisms.

[34] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, op. cit., pp. 20–25

Ultimately, the future effectiveness of European public policy in addressing cybersecurity challenges will depend upon the European Union's capacity to achieve deeper institutional integration, reduce disparities among Member States, strengthen cooperation and information sharing, and invest strategically in innovation, advanced technologies, and human capital to create a more secure, resilient, and sustainable digital environment.

Findings

1.Cybersecurity challenges have become a central component of the European Union's public policy agenda.

2.The European institutional framework has contributed significantly to the development of a relatively comprehensive system for addressing cybersecurity threats.

3.The European Union Agency for Cybersecurity (ENISA) has emerged as one of the principal institutional actors in European cybersecurity governance.

4.The effectiveness of European cybersecurity policy continues to be affected by disparities in national capabilities among Member States.

5.The NIS2 Directive and the Cyber Resilience Act have substantially strengthened the European Union's cybersecurity governance framework.

6. Achieving higher levels of policy effectiveness requires stronger institutional coordination, deeper integration, and sustained investment in technological and human capacities.

Recommendations

1.Strengthen institutional cooperation between European Union institutions and Member States in the field of cybersecurity.

2.Develop harmonized mechanisms for information sharing, early warning, and coordinated responses to cyber incidents.

3.Support Member States with less developed cybersecurity capacities through targeted capacity-building initiatives and the transfer of technical expertise.

4.Increase investment in scientific research, technological innovation, and advanced digital technologies.

5. Expand specialized education, professional training, and workforce development programs in cybersecurity.

Promote European digital sovereignty by reducing strategic dependence on external technologies and suppliers while strengthening indigenous technological capabilities.

References

First: Official Documents and Reports

1. European Commission. The EU's Cybersecurity Strategy for the Digital Decade. Brussels: European Commission, 2020.

2. European Commission. 2030 Digital Compass: The European Way for the Digital Decade. Brussels: European Commission, 2021.

3. European Commission. Cybersecurity Policies. Brussels: European Commission, 2024.

4. European Commission. Cyber Resilience Act: Protecting Consumers and Businesses from Cyber Threats. Brussels: European Commission, 2024.

5. European Commission. NIS2 Directive: Strengthening Cybersecurity across the EU. Brussels: European Commission, 2023.

6. European Parliament and Council of the European Union. Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act). Official Journal of the European Union, 2019.

7. European Parliament and Council of the European Union. Directive (EU) 2022/2555 on Measures for a High Common Level of Cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, 2022.

8. European Parliament and Council of the European Union. Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act). Official Journal of the European Union, 2024.

9. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023. Athens: ENISA, 2023.

10. European Union Agency for Cybersecurity (ENISA). Cybersecurity Cooperation: Information Sharing and Situational Awareness. Athens: ENISA, 2023.

11. European Union Agency for Cybersecurity (ENISA). National Coordination Centres and Cybersecurity Governance in the EU. Athens: ENISA, 2023.

12. European Union Agency for Cybersecurity (ENISA). National Cybersecurity Strategies in the EU. Athens: ENISA, 2023

13. European Union Agency for Cybersecurity (ENISA). About ENISA – The EU Agency for Cybersecurity. Athens: ENISA, 2024.

14. European Union Agency for Cybersecurity (ENISA). ENISA Annual Report 2023. Athens: ENISA, 2024.

15. European Union Agency for Cybersecurity (ENISA). ENISA Work Programme 2024. Athens: ENISA, 2024.

Second: Books and Academic Studies

16. Cavelty, Myriam Dunn. Cybersecurity: Politics, Governance and Cooperation. London: Routledge, 2018.

17. Hix, Simon, and Bjørn Høyland. The Political System of the European Union. London: Palgrave Macmillan, 2022.

18. Hooghe, Liesbet, and Gary Marks. Multi-Level Governance and European Integration. Lanham: Rowman & Littlefield, 2001.

19. Singer, P. W., and Allan Friedman. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014.