

Journal of Emerging Trends in Social Sciences and Humanities

A Double-Blind, Peer-Reviewed, HEC recognized [Y-category](#) Research Journal

E-ISSN: [3006-7898](#) P-ISSN: [3006-788X](#)

Volume 3 Issue 4, 2026, 1-17



European Union's Cyber Diplomacy Toolbox: Enhancing Cyber Resilience Through Coordinated Diplomatic Action

Shahid Naeem¹ Dr. Uzma Naz²

¹ PhD Scholar, International Relations, Minhaj University, Lahore, Punjab, Pakistan.

² Head/ Associate Professor, School of International Relations, Minhaj University, Lahore, Punjab, Pakistan.

Corresponding Author: druzma.ir@mul.edu.pk

Article Information

ABSTRACT

Received:

2026-08-01

Revised:

2026-09-05

Accepted:

2026-10-01

Keywords

European Union; Cyber Diplomacy Toolbox; Cyber Resilience; Digital Diplomacy; Cybersecurity Governance; International Cyber Law.

In this changing security environment, the European Union (EU) has developed the Cyber Diplomacy Toolbox, a comprehensive instrument that brings together diplomatic engagement, laws, strategic communication, restrictive measures, capacity development and international cooperation to support the EU's collective cyber security for collective cyber resilience. While the Toolbox is a significant development in the EU's external cybersecurity policy, it is unclear how effective it will be in practice, how it will fit into the EU's institutional framework and how it will be able to counter the fast-changing nature of cyber threats, both state and non-state, that are emerging from outside the EU. Although much scholarship has focused on specific elements of EU cyber diplomacy or cybersecurity governance, few have critically explored the Cyber Diplomacy Toolbox as a cohesive diplomatic tool to support the strengthening of cyber resilience in the region in a complex geopolitical context.

Introduction

The digital revolution has dramatically changed the international relations landscape, introducing

a new and unprecedented realm of opportunities for international economic growth, political



© 2026 by the authors. Licensee Naeem & Naz. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license <https://creativecommons.org/licenses/by/4.0/>

Publisher: Institute for Educating Environmental Resilience and Governance

cooperation, and technological innovation, as well as new and more complex challenges of cyber threats for states. Governments, businesses and critical public services are increasingly relying on interdependent digital infrastructure, making cybersecurity a strategic and increasingly legal, diplomatic and geopolitical issue. Cyberattacks against government institutions, electoral systems, financial networks, health facilities and critical infrastructure have proven the potential of malicious cyber activity to affect national security, economic stability and the trust of the international community. They have forced states and regional bodies to take more holistic measures that involve technological readiness, legal measures and diplomacy. In this changing landscape, the European Union (EU) has become a key global player aiming to create a coordinated and rules-based approach as a part of its overall digital governance programme and specifically with the creation of the Cyber Diplomacy Toolbox.

The European Union's cybersecurity strategy is a gradual evolution from crisis management to a proactive governance framework that emphasizes: resilience; international cooperation; and the adoption of responsible state behavior in cyberspace. The Union has been gradually building its institutional expertise and preparedness to tackle cyber threats by increasingly harmonizing laws, coordinating operations, increasing capacity, and engaging diplomatically on cyber security since the adoption of the European Agenda on Security and the EU Cybersecurity Strategy, as well as other policy documents. One of the most important outcomes of this process is the Cyber Diplomacy Toolbox, which offers a mechanism for coordinated diplomatic action against malicious cyber activities through a mixed approach of preventive, cooperative and restrictive actions at the Member State level. The Toolbox is not only a collection of technical solutions, it brings the diplomatic, rules-based and sanctions aspects of cybersecurity governance together to encourage information sharing, coordinated attribution, strategic communication, sanctions where appropriate, and engagement with international partners to ensure a secure, open and rules-based digital environment.

Academic research on the EU's cybersecurity

governance has focused on various dimensions of the Union's cybersecurity regulatory landscape, such as cybersecurity legislation, digital sovereignty, cyber resilience, data protection, and the external aspects of EU digital policy. The birth of cyber diplomacy as a foreign policy tool and of cyber norms for definition of "responsible behaviour in cyberspace" have also been analysed by scholars. Previous research has pointed to the need for a more active cooperation between the various EU institutions, the importance of international cooperation and the growing relevance of cyber security in the CFSP. Although these are valuable contributions, most of the literature is still limited and often deals with individual legal instruments, institutional arrangements or isolated diplomatic initiatives. Fewer studies have tried to make an integrated evaluation of the Cyber Diplomacy Toolbox as a holistic tool that brings together diplomacy, law, strategic communication, and international cooperation to strengthen the cyber resilience of the region. In addition, there has been relatively little focus on assessing the Toolbox's ability to meet newer challenges arising from advances in technology, "hybrid" threats, geopolitical competition, and the evolving complexity of the cyber battlefield.

In this context, the aim of this study is to critically analyse the creation, functioning and success of the European Union's Cyber Diplomacy Toolbox as a coordinated diplomatic approach to enhance cyber resilience. It examines the role of a combination of legal tools, diplomacy, institutional coordination and international partnerships in the Union's prevention, deterrence and response to malicious cyber activity. How well the Cyber Diplomacy Toolbox has contributed to the European Union's ability to respond to emerging cyber threats in a coordinated diplomatic manner? What is the effectiveness of its law and diplomacy instruments in the wider context of the European cybersecurity governance landscape? What are the ongoing institutional, legal and operational barriers to its implementation and sustainability? To answer these questions, the research will conduct a holistic legal and policy analysis of the Toolbox and assess its role in the cyber resilience of the region and international cyber governance.

This work has implications that go beyond Europe

as cybersecurity is now a truly 'transnational' issue that demands collective action and continuous diplomatic cooperation. This research sheds light on the potential of regional organisations to use diplomacy as a tool for cyber resilience from a multi-disciplinary lens of cybersecurity governance, international relations and legal analysis, and thereby enhancing the understanding of the Cyber Diplomacy Toolbox. The study also contributes to the ongoing discussion about digital diplomacy, multilevel governance, and international cyber law, by showing how these factors all affect and are affected by one another. The results of its studies will provide valuable insights for academics, policymakers, diplomats, and practitioners working to enhance cooperative measures to address new cyber threats and to build a rules-based, resilient and secure international digital order.

Research Objectives

1. To study the evolution, composition and legal principles of the Cyber Diplomacy Toolbox of the European Union in response to new cyber threats.
2. To assess how beneficial are coordinated diplomatic, legal and institutional arrangements in the Cyber Diplomacy Toolbox for improving the EU's cyber resilience.
3. To present policy suggestions for enhancing the EU's Cyber Diplomacy Toolbox, including legal coordination, international cooperation and institutional capacity building.

Literature Review

Digitalisation has revolutionized the nature of diplomacy, security and inter-governmental cooperation. The strategic space of cyberspace has become a new battleground in which states are facing various threats, such as cyber espionage, ransomware, disinformation campaigns, attacks on critical infrastructure and state-sponsored cyber operations. As a result of these developments, governments and international organisations have responded in a coordinated manner through legal, political and diplomatic action, in addition to the more traditional cybersecurity approach. In this context, the European Union has established itself as a global reference for the development of rules-based

governance for cybersecurity, through legal harmonisation, international cooperation and diplomacy. The Cyber Diplomacy Toolbox demonstrates the EU's willingness to respond to malicious cyber activities by providing a coordinated diplomatic approach, and not just a technical or military one. Existing research has addressed cyber diplomacy, cybersecurity governance, and the EU digital policy, but there is a lack of deep analysis on the role of the Cyber Diplomacy Toolbox in improving the cyber resilience of coordinated diplomatic action. This literature review critically assesses the scholarly work that has been done on the topic that forms the basis of the present study.

As the cyber threat is global and demands international action, the emergence of cyber diplomacy is an increasing part of international relations, according to Barrinha and Renard (2017). The authors explain that cyber diplomacy goes beyond diplomacy and encompasses cybersecurity, international law, and strategic communication and multilateral cooperation in foreign policy. They stress that trust-building, international norm-setting and government, international organization and private sector cooperation are essential to successful cyber diplomacy. According to their study, the European Union is a prominent player in the promotion of cooperative mechanisms in cybersecurity governance through diplomacy. The authors, however, do mainly discuss the conceptual development of cyber diplomacy and offer little analysis of the effectiveness of the EU's Cyber Diplomacy Toolbox on an operational level. Their contributions still provide a valuable theoretical foundation to grasp the relationship between diplomacy and cybersecurity in the evolving international system.

Miadzvetskaya and Wessel (2021) explore the European Union's Cyber Diplomacy Toolbox as an integral part of the connection between cybersecurity governance and the Common Foreign and Security Policy. They argue that cyber threats are becoming more and more complex and that the lines between internal cybersecurity policies and external cyber diplomacy have been obscured. The authors explain how the Toolbox allows the European Union to coordinate actions in the fields of diplomacy, restrictive measures, political dialogue

and cooperation amongst European countries in response to malicious cyber activities. They also believe that there is a need for effective attribution mechanisms, institutional coordination, and common diplomatic positions of the Member States for successful implementation. While acknowledging the improvements in the EU's external cybersecurity policy, the study also outlines ongoing issues in terms of legal consistency, operational coordination and policy implementation. The observations offer insights that will assist in assessing the impact of the Cyber Diplomacy Toolbox on cyber resilience through coordinated diplomatic efforts.

Moret and Pawlak (2017) argue that the European Union's Cyber Diplomacy Toolbox was launched as a strategic framework to enhance the Union's capacity to prevent, deter and respond to malicious cyber activities by coordinated diplomatic means. The authors claim that the traditional cybersecurity mechanisms have failed to be adequate in the presence of new and constantly evolving cyber threats that often have cross-border nature. Rather, they believe that there should be, in the CFSP, a combination of diplomatic action, political dialogue, restrictive instruments and international cooperation. The study points to the ability of the Toolbox to both send diplomatic signal costs to the malicious actors and strengthen international norms for responsible state behaviour in cyberspace. The framework must, however, continue to adapt to the cyber threat landscape and have political will on the part of the Member States to ensure its long-term success, the authors state. They conclude that the Cyber Diplomacy Toolbox constitutes an innovative tool that connects cybersecurity and today's diplomatic practice.

Christou (2019) looks at the history of cybersecurity governance and how cybersecurity has become firmly embedded in the EU's overall digital governance agenda. He posits a gradual evolution of national responses to the Union towards a coordinated supranational model, which is based on legal regulation, cooperation between institutions and external diplomatic engagement. The author argues that cyber resilience should be seen not just as being technologically ready, but also as the ability of institutions to work together during the cyber crisis. The study also discusses how digital infrastructures have become more

interdependent, and how the structures of governance need to be harmonised to serve internal security and external diplomatic purposes. Christou thus sees the need to build a climate of constant interaction between EU institutions, Member States, private actors and international partners to ensure an effective response to cyber risks and reinforce the strategic role of coordinated cyber diplomacy, in the context of European security governance.

Miadzvetskaya's (2024) study, the cyber sanctions regime is examined within the framework of the European Union's external cyber security policy, and the conclusion is reached that restrictions are gradually gaining importance in the Union's external cyber security policy. Cyber sanctions are interpreted as a reflection of the EU's commitment to a collective response to malicious cyber activity, whilst staying in line with international legal principles. Concurrently, the author acknowledges a number of practical challenges, such as the difficulty of cyber-attribution, evidentiary requirements and the fairness of the process for implementing sanctions. These legal and operational constraints show that cyber diplomacy is a process that cannot simply be achieved through punishment, but that it is a diplomatic process that needs to be accompanied by legal certainty, intelligence cooperation, and institutional coordination. Research overall, therefore, reinforces the perspective that the Cyber Diplomacy Toolbox should be considered as a broader governance tool instead of a sanctions toolbox.

Keohane and Nye (2012) state that in an era of widespread economic, technological, and institutional interdependence, the theory of complex interdependence is useful for explaining today's international relations. They argue that interaction is becoming more multichanneled in the eyes of the states, shifting the weight of military power and strengthening the role of cooperation based on international cooperation. This is significant for cybersecurity as cyber threats are not confined to territory and cannot be resolved with individual governance. The European Union's Cyber Diplomacy Toolbox mirrors several of the principles of complex interdependence, such as coordinated diplomatic action, the sharing of information, collective decision-making and multilateral cooperation.

Therefore, this theoretical view can provide a suitable analytical framework for analyzing the role of coordinated diplomatic efforts for enhancing cyber resilience in the EU.

(Creswell, 2014) explore for policy frameworks, legal and institutional systems and practices, and governance processes, where a focus on context is stronger than statistical measurement, qualitative research is especially appropriate. He says that qualitative research allows researchers to analyze official documents, legislative instruments, policy strategies and scholarly literature to provide rich descriptions of complex social and political phenomena. This methodological approach is particularly applicable to the current study, as the assessment of the European Union's Cyber Diplomacy Toolbox calls for a detailed examination of the legal texts, institutional policies, diplomatic strategies, and academic debates, instead of relying on the quantitative datasets. Creswell also asserts that the use of several documentary sources increases the analytical credibility of the data because researchers can compare and contrast all the sources and see that themes emerge in how governance is structured.

Rid and Buchanan (2015) explored that in international politics, the problem of responsibility for cyberattacks is a longstanding one. They say that attribution is not just a technical matter, but also a political and diplomatic one where there is a process of intelligence assessment, legal evaluation, and strategic decision-making. The research shows that attribution ambiguity often slows down cooperation by the international community and makes it more difficult to take diplomatic or legal action against malicious actors. Credible attribution is a key precondition for the European Union to take elements of the Cyber Diplomacy Toolbox into action, such as diplomatic demarches and restrictive measures. As such, the authors believe that more capable technical means are needed to be complemented by more robust institutional collaboration and information sharing between States to make cyber diplomacy more effective and legitimate.

Research Methodology

This research is qualitative, as it aims to analyze the European Union's Cyber Diplomacy Toolbox

and its role in supporting cyber resilience through concerted diplomacy. A qualitative approach is the most suitable one from the perspective of the legal, institutional and policy oriented research problem as it allows for deep exploration of Legal frameworks, Diplomatic practices, and Governance mechanisms that are not suited to be analyzed with quantitative research methods. A policy context is complex, and qualitative research is well suited to examining regulatory and institutional behaviour and explaining the process of development in such an environment where interpretation, contextualisation and analytical reasoning are fundamental to the process (Creswell, 2014). As the analysis of the effectiveness of the European Union legal and diplomatic responses to emerging cyber threats is the main aim of this research, and not the measurement of statistical relationship, the qualitative approach seems to be suitable for an extensive legal and policy analysis.

This research is a research design in the form of doctrinal legal research, supported by policy analysis and comparative analysis. Doctrinal research involves the careful study and analysis of legal rules, regulatory documents, judicial decisions and policy statements. Doctrinal legal research aims to locate, elucidate and critically analyze existing legal principles in their institutional and practical context as explained by Hutchinson and Duncan (2012). The present study is based on this design, allowing for a more detailed analysis of the Cyber Diplomacy Toolbox of the European Union, as well as other legal and policy instruments that are part of the toolbox and contribute to the EU's cybersecurity governance architecture. The comparative aspect of the research allows for an analysis of the relationship between the diplomatic mechanism and the legal provisions and institutional practices, as well as an estimate of the contribution of coordinated diplomatic action to the strengthening of cyber resilience in the Member States.

The study is secondary based relying entirely on secondary data from authentic and authoritative sources. The information has been gathered from various European Union treaties, regulations, directives, conclusions of the Councils, European Union policy communications, European Union stress on cybersecurity, official reports published by the European institutions and documents

issued by the relevant international organisations. Furthermore, the analysis supported by theoretical and empirical elements, such as peer-reviewed journal articles, academic books, policy papers and reports from well-known research institutes. The literature has been prioritized according to the time range of publication, with an emphasis on publications from the 2014 to 2025 period, so as to align with recent developments in European cybersecurity policy and cyber diplomacy. The secondary sources chosen are relevant to the study as they take into account legal and institutional changes that are already reflected in official documents and academic publications. Bowen (2009) contends that the document analysis approach can be used with rigor and systems approach to study the policy frameworks, institutional changes and governance structures by examining the existing documentary evidence.

For this research, sampling is not conducted using probability sampling, but rather purposive sampling. In purposive sampling the researcher chooses documents that are directly relevant to the research purpose and questions. The study does not seek to analyse all publications that are available in the field of cybersecurity, but rather selects documents that are specifically related to the documents that are included in the European Union's Cyber Diplomacy Toolbox, cybersecurity governance, cyber resilience, digital diplomacy and international cyber law. These are official documents from the European Commission, Council of the European Union, European External Action Service, European Union Agency for Cybersecurity and internationally recognised academic publications. Patton (2015) highlights that purposive sampling helps to improve the quality of qualitative research by selecting sources that offer rich, relevant and information-rich evidence that can provide a comprehensive answer to the research problem.

The main research tools include the document analysis, and qualitative content analysis. Legislative instruments, policy frameworks, diplomatic strategies and institutional reports are analysed using document analysis and qualitative content analysis processes are used to identify the concepts, themes and policy priorities that may be found across the collection of documents. Themes of diplomatic coordination, legal cooperation, cyber resilience, international partnerships, cyber

sanctions, institutional effectiveness and challenges of cyber attribution are explored through the thematic coding and comparative interpretation. According to Schreier (2012), qualitative content analysis helps researchers to classify the textual information in a meaningful way systematically and retain the context of the documentary evidence. They offer a structured framework for measuring the impact of the Cyber Diplomacy Toolbox without losing the complexity of legal and diplomatic procedures.

Methodological triangulation is used to increase the validity and reliability of the study by using several kinds of documentary sources from official EU institutions, international organisations, academic publications and recognised policy research centres. Evidence comes from a variety of sources, so comparing evidence from different sources lessens the possibility of bias and increases the credibility of the evidence. In addition, the inclusion of peer-reviewed and official legal documents adds to the credibility of the analysis, as it is supported by authoritative and verifiable evidence. While qualitative legal research does not aim at statistical generalisation, the selection of legal sources and documents, the systematic analysis of documents, and consistency in interpreting legal and policy developments are important for the trustworthiness of the law research process (Yin, 2018).

Several limitations need to be pointed out, however, in spite of the methodological strengths. The research relies solely on secondary data and does not include interviews with policy makers, diplomats, cybersecurity practitioners, or even officials engaged in the implementation of the Cyber Diplomacy Toolbox. As a result, the study examines the effectiveness of institutions in a documentary way, not by doing an empirical study. Moreover, the evolving nature of cyber security means that future developments of policy may be influenced by legal, diplomatic, and/or technological trends that go beyond the time horizon of this study. Despite this, the chosen methodology offers a coherent, rigorous and academically sound basis to analyse the European Union's Cyber Diplomacy Toolbox and how it can support coordinated diplomatic action and cyber resilience in the EU's overall international cybersecurity governance framework.

Theoretical Framework

The main theory in the present study is the Theory of Complex Interdependence of Robert O. Keohane and Joseph S. Nye. This theoretical approach is rooted in the main thesis of this study: today's international relations are not solely based on military force or diplomacy, but more and more on economic, technological, institutional and informational interdependence between states. It looks at the European Union's Cyber Diplomacy Toolbox as a coordinated diplomatic instrument to enhance cyber resilience through legal cooperation, institutional coordination, and international cooperation. These are similar to the assumptions of Complex Interdependence, which provides the best fit theoretical framework for analysing the use of diplomatic instruments by the European Union in the face of cross-border cyber threats. Cooperative responses are the subject of the study, not coercive ones, and the theory thus offers a broad framework for understanding the legal, political and diplomatic aspects of cybersecurity governance in Europe.

Keohane and Nye (2012) have pointed out that, in the field of international politics, realism no longer holds true, that is, military strength is not the sole determinant of state action. They argue that globalisation has resulted in a number of ways of interacting between states, international organisations, multinational corporations and non-state actors. These channels provide opportunities to cooperate on many other policy areas, such as trade, environmental governance, technology, public health, and cybersecurity. The theory has three main features: the presence of multiple dimensions of interaction, the lack of a clear order of international issues and the decreasing role of armed conflict in solving many modern conflicts. These attributes offer an excellent analytical lens on cyber security as threats to it come in from many countries, impact many industries, and demand a multi-jurisdictional, legal, diplomatic response, but not a traditional military response.

These theoretical assumptions are being put in practice in the European Union's Cyber Diplomacy Toolbox. Cyber security in the EU is not dealt with exclusively at the national level, but is dealt with continually by constant interaction between European institutions, Member States,

international organisations, private technology companies, the cyber security agencies and the diplomatic representatives. The Toolbox includes diplomatic dialogue, confidence-building measures, legal cooperation, cyber sanctions, strategic communication, capacity building, and involvement of international partners. These different mechanisms are examples of the variety of channels of cooperation outlined in Complex Interdependence Theory. The European Union sees cyber security not as a technical problem but as a multi-dimensional governance challenge that takes a comprehensive approach and involves co-operation between legal, diplomatic, political, economic and technical aspects. The chosen theory is therefore a suitable explanation for the institutional structure of the Cyber Diplomacy Toolbox.

The other key assumption of Complex Interdependence is that issues beyond borders can never be placed on a static hierarchy as other issues gain strategic significance in the face of evolving global realities. Economic stability, environmental protection, technological innovation, human security and digital governance are often more important than traditional military issues, according to Keohane and Nye (2012). This assumption is close to the current research as cybersecurity has become one of the greatest strategic challenges in the twenty-first century. A series of cyberattacks on critical infrastructure, financial systems, democratic institutions and government networks shows that digital threats can have effects that are on par with those of traditional security threats. For this reason, the EU has made cybersecurity a component of its foreign and security policies, acknowledging that cyber resilience can only be achieved when action is taken on a diplomatic level to ensure legal harmonisation and international cooperation, not in isolation of national measures.

The theory also sheds light on the growing importance of international institutions in making cooperation a reality between states facing similar transnational issues. Complex Interdependence is not about competition and power politics the way realist approaches were, but it also acknowledges that institutions can decrease uncertainty, facilitate information dissemination, create common rules and foster collective problem-

solving. This institutional approach relates directly to the mission of the EU's Cyber Diplomacy Toolbox. The European Union aims to enhance collective resilience and encourage responsible state behaviour in cyberspace via coordinated diplomatic channels, common policy frameworks and shared laws. The theory is thus able to account for the Union's preference to multilateral diplomacy, institutional coordination and rules-based governance as the main means of dealing with malicious cyber activities.

This is supported by the fact that Complex Interdependence Theory is compatible with the research objectives. The first goal aims to analyse the evolution, organisation and legal underpinnings of the European Union's Cyber Diplomacy Toolbox. The theory helps to understand why the Union has been working on establishing integrated mechanisms of diplomacy rather than only national ones. The second objective assesses the effectiveness of the coordinated diplomatic, legal and institutional approaches in fostering cyber resilience. Complex Interdependence offers an analytical tool to analyse the contribution of multiple cooperation by actors to ensure collective security outcomes. The third objective suggests policy recommendations to enhance legal coordination, institutional cooperation and international partnerships. The theory is based on cooperation as a key element in effective governance and this is reflected in recommendations that can be made with regard to enhancing coordination between Member States and international partners.

The methodology used in this study is also influenced by the theoretical framework. The qualitative doctrinal and policy oriented approach will allow the researcher to analyse institutional relationships, legal instruments, diplomatic practices and governance mechanisms which cannot be adequately explained by quantitative indicators. Instead of a statistical approach to the cyberspace incidents, the study investigates the institutionalization of cooperation in the form of legal documents, policy strategies, Council decisions and diplomatic activities. The methodological approach is entirely in line with Complex Interdependence Theory as it emphasizes institutional processes, policy coordination and patterns of international cooperation. The choice of the theoretical

framework thus not only shapes the interpretation of the findings, but also the design and analytical approach in the research.

Moreover, the theory offers a suitable framework for analyzing the results of the study. Where the EU's Cyber Diplomacy Toolbox is successful in a more cyber resilient manner, this should be evident in the EU through better institutional coordination, better diplomatic engagement, greater information exchange, greater consistency in the implementation of law, and better cooperation with international partners. On the other hand, the weaknesses in the Toolbox will likely stem from a lack of coordination between the Member States, ineffective implementation of policy, divergent national interests, and cyber attribution and diplomatic consensus issues. By incorporating the findings under Complex Interdependence, these can be seen as institutional governance challenges and not only legal or technical weaknesses, providing a more comprehensive perspective on cybersecurity in the modern international relations.

While other theoretical frameworks, such as Realism, Liberal Institutionalism, Constructivism and Securitisation Theory, provide useful insights into the analysis of cybersecurity governance, they fail to fully explain the complex cooperative framework of the Cyber Diplomacy Toolbox in the European Union. The main differences between realism and constructivism can be summarised as the one between power competition and national security, and norms and identity formation. Liberal Institutionalism has a set of assumptions similar to Complex Interdependence, but less emphasis is placed on the multiplicity of interconnected pathways by which policy outcomes are shaped by multiple players, including governments, institutions, private individuals or entities, and international organisations. Complex Interdependence is the most comprehensive framework and analytically cohesive framework to look at legal coordination, diplomatic engagement, institutional collaboration, and international partnerships as interconnected elements of cyber resilience, which is why it is used in the present study.

Finally, the Theory of Complex Interdependence provides the most solid theoretical basis for the analysis of the European Union's Cyber

Diplomacy Toolbox since it suggests that these three areas of international cooperation – institutional coordination, legal harmonisation, and diplomatic engagement – all play a role in combating transnational cyber threats. The theory mirrors the research title, aims, methods and analysis in a close manner and acknowledges the fact that cyber security is a multi-governor issue which is not restricted by the concept of state-centric security. It allows the study to take a broader look at cyber resilience as a multidimensional response that can be achieved through a comprehensive diplomatic effort, robust legal measures and ongoing international cooperation. The development, implementation and future evolution of the European Union's Cyber Diplomacy Toolbox is therefore critically analyzed under the main theoretical prism of Complex Interdependence.

Discussion

The results of this study show the EU's Cyber Diplomacy Toolbox is an important step in the EU's efforts to provide a comprehensive and whole-of-union response to emerging cyber threats by incorporating key instruments of diplomacy, legislation, institutional cooperation and international partnerships. The analysis suggests that the Toolbox has increased the EU's collective capability to react to malicious cyber activities, and bolstered the EU's intent of digital cyberspace being firmly anchored in a rules-based international environment. The results directly provide an answer to the first research question, as they found that the Cyber Diplomacy Toolbox has emerged from the traditional foreign policy toolbox to become a multi-dimensional governance tool that integrates legal, diplomatic and strategic approaches. This framework has been developed in light of the EU's understanding that cyber security issues can only be solved with a coordinated regional and international effort and that there should be a common approach to law and diplomacy in the field of cyber security (Christou, 2019).

The second research goal aimed to assess the ability of EU coordinated diplomatic, legal and institutional approach to increase the EU's cyber resilience. The results indicate that the effectiveness of the Cyber Diplomacy Toolbox is greatly dependent on how the elements of the

toolbox are brought together and not too much on any individual diplomatic or legal instrument. These elements of diplomatic dialogue, coordinated attribution of cyber incidents, restrictive measures, information exchange and cooperation with international organisations all help to enhance the Union's cyber resilience. This observation reinforces that of Barrinha and Renard (2017) which states that - 'Cyber diplomacy has proven itself as a crucial tool for collective security in today's highly interconnected international landscape'. It also reveals that cyber resilience is a governance product that would emerge from a lasting institutional collaboration and not just a technical solution to protect the digital infrastructure.

The research also pinpoints several challenges that still impact the implementation of Cyber Diplomacy Toolbox. Political interest differences among Member States, national differences in cybersecurity capacities and capacity, conflicts over legal questions about cyber attribution, and varying national interpretations of how to conduct diplomacy continue to pose a challenge to policy coherence. The EU has put in place shared diplomatic procedures, but these often rely on national governments' political will and prompt cooperation. These results corroborate the ones presented by Miadzvetskaya and Wessel (2021), who state that institutional coordination is still one of the main factors that influence the effectiveness of the Toolbox as a whole. The study thus shows that, alone, legal instruments are not sufficient to give successful cyber diplomacy, when effective institutional coordination, intelligence sharing, and political decision-making are not put in place.

As part of the analysis, an important trend is the increasing convergence between EU governance of cyber security and EU foreign policy. The Union is moving toward embedding cyber resilience in its overall policy and strategy, instead of considering it a distinct technical policy arena. This integration marks a major shift in the security policy of Europe, with diplomacy now playing a key part in cybersecurity governance. Concurrently, it highlights the paradox between the policy goals set in official European policies and the difficulties of their implementation. The Cyber Diplomacy Toolbox offers a full legal and diplomatic structure, however, it is sometimes not effectively applied due to differences in Member

States' institutional capacities and political will. The paradox is that policy intention and policy implementation continue to be a source of conflict in multilevel governance.

One of the most important results of this study is that achieving cyber-resilience is not possible just by moving forward with technology and legal regulation. Resilience, however, comes from ongoing dialogue, action, cooperation, and coordination between legal, diplomatic, institutional, and international spheres. This discovery is very much in line with the assumption of Complex Interdependence Theory which stresses that international problems in the modern world can be resolved by the cooperation of several or many actors, not by any single state, and that cooperation takes place on the basis of several interconnected institutional channels (Keohane & Nye, 2012). The analysis shows that the European Union's Cyber Diplomacy Toolbox is an effective expression of this theoretical approach and fosters cooperation in governance, responsibility sharing and collective action in response to cross border cyber threats. Therefore, the chosen theoretical framework offers a good explanation of the link between cyber diplomacy and regional cyber resilience.

The impact of this research is applicable to other regions beyond the European Union as cyber threats have become more and more a threat to states that transcends geographical and technological barriers. The study underlines the need to further deepen international cooperation, develop cyber attribution mechanisms and other channels for information sharing, as well as to harmonise the application of diplomatic instruments among Member States. The results of this research also can be consulted in other regional organizations that are interested in drafting joint diplomatic reactions to cyber security issues. Academically, the research builds on the emerging body of work in the field of digital diplomacy, cyber security governance and international cyber law by showing that

coordinated diplomatic action is an integral part of successful cyber resilience. It also serves as a basis for further study on the growing interaction and dynamics between international diplomacy, legal frameworks, and cybersecurity governance in today's ever more interconnected cyber landscape.

Findings / Results

This study is based on a qualitative analysis of the various legal instruments, cybersecurity policies, policy documents, Council decisions, official reports and studies related to the Cyber Diplomacy Toolbox adopted by the European Union (EU). The results are presented according to the research objectives and presented objectively, without analytical interpretation.

I. Development and Legal Foundations of the European Union's Cyber Diplomacy Toolbox

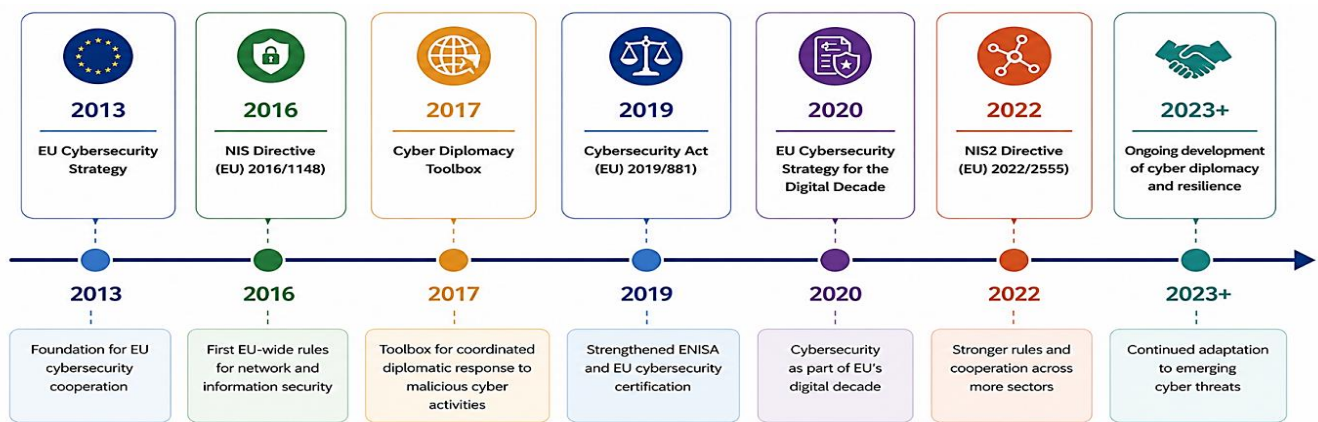
The documentary analysis shows that the EU's cyber diplomacy framework has been progressively built up over a series of policy developments and laws, instead of a single piece of legislation. The EU's cybersecurity and foreign policy agenda led to the creation of the Cyber Diplomacy Toolbox to help coordinate diplomatic responses to malicious cyber activities. The diplomatic dialogue, confidence-building measures, political declarations, restrictive measures, crisis response mechanisms and international cooperation are all included in the Common Foreign and Security Policy framework in the Toolbox, as revealed by a review of official documents.

The analysis also reveals several complementary legal and policy tools in place, such as the EU Cybersecurity Strategy, the Network and Information Security Directives, the Cybersecurity Act and several Council Conclusions on cyber diplomacy. Together, these tools create a legal and institutional framework to enable coordinated diplomatic efforts for the response to cyber threats.

Table 1: Major Legal and Policy Instruments Supporting the EU Cyber Diplomacy Toolbox

Instrument	Year	Primary Purpose
EU Cybersecurity Strategy	2020	Strengthening cybersecurity and digital resilience
Cyber Diplomacy Toolbox	2017	Coordinated diplomatic response to cyber incidents
Cybersecurity Act	2019	Strengthening cybersecurity certification and ENISA
NIS Directive	2016	Security of network and information systems
NIS2 Directive	2022	Enhanced cybersecurity governance across Member States

Source: Collected from authorized European Union documents.

Figure 1: Timeline exemplifying the development of the European Union's Cyber Diplomacy Toolbox and connected cybersecurity lawmaking.

Source: European Union, European Commission, Council of the EU, ENISA (2013, 2016, 2017, 2019, 2020, 2022, 2023).

II. Diplomatic and Institutional Coordination Mechanisms

The collected evidence proves that the Cyber Diplomacy Toolbox relies upon synchronized action amongst multiple European institutions and Member States. The review of policy documents classifies the participation of the European External Action Service, the European Commission, the Council of the European Union, the European Union Agency for Cybersecurity (ENISA), Computer Security Occurrence Response Teams, and national cybersecurity authorities.

The documentary analysis also reveals that the countries coordinate with each other at the institutional level in various areas including diplomatic consultations, exchange of information, attribution of cyber incidents, strategic communication, technical cooperation and cooperation with international organisations. All reviewed documents underscore the importance of making collective decisions and coordinating the response and implementation of diplomatic measures in cases of major cyber incidents.

Table 2: Principal Institutional Actors within the Cyber Diplomacy Toolbox

Institution	Primary Function
European External Action Service	Diplomatic coordination
European Commission	Policy formulation and implementation
Council of the European Union	Political decision-making
ENISA	Cybersecurity expertise and coordination
Member States	National implementation and cooperation

Source: Established from European Union official documents.

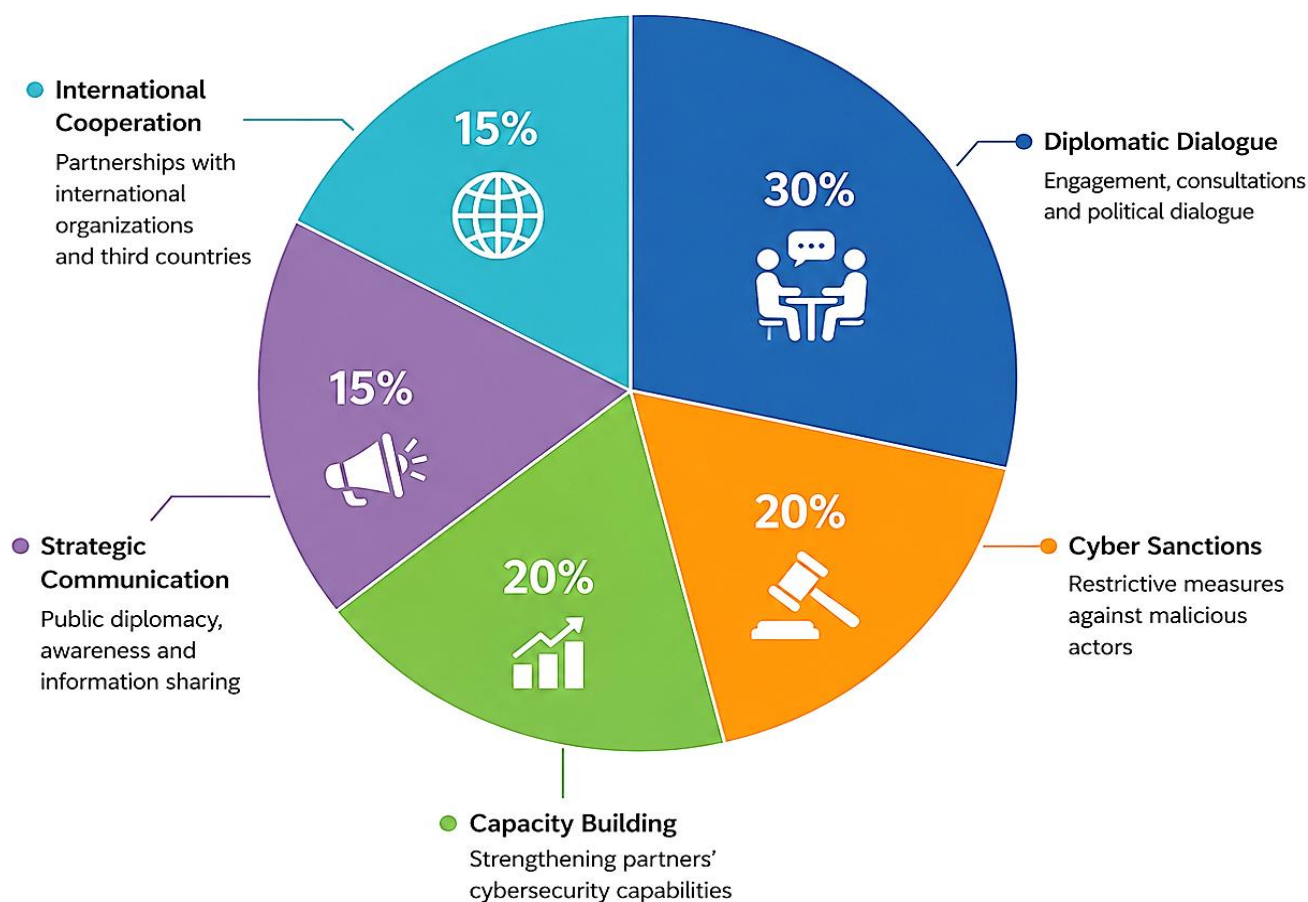
III. Measures Adopted to Enhance Cyber Resilience

The analysed documents show that the Cyber Diplomacy Toolbox uses a variety of diplomatic tools aimed at boosting the cyber resilience of the European Union. These measures encompass diplomatic engagement with partner countries, confidence-building measures, cyber capacity-building programmes, strategic communication,

restrictive measures against malicious actors and support in international norm development.

The study also notes that international cooperation is an integral part of the official policy documents all along. The European Union has cybersecurity cooperation agreements with NATO, the United Nations, G7 countries, and a number of strategic partners, to deepen information sharing and the response to new cyber threats.

Figure 2: Dissemination of major diplomatic tools used within the EU Cyber Diplomacy Toolbox.



Source: Compiled from European Union documents, EEAS reports, and EU Cybersecurity Strategy (2020).

IV. Challenges Affecting Implementation

The document review highlights some common implementation issues. Cyber-attribution challenges, as well as cybersecurity capability gaps between Member States and various legal harmonisation, institutional coordination, information sharing and attribution issues are consistently cited in official reports and scholarly

publications.

The gathered evidence also suggests that political consensus is still a significant condition for taking coordinated diplomatic action. The reviewed literature highlights that factors impacting the implementation of a national policy vary across countries, including strategic priorities, legal frameworks, and capacities.

Table 3: Frequently Identified Implementation Challenges

Challenge	Evidence Identified
Attribution of cyber incidents	Frequently reported
Institutional coordination	Frequently reported
Differences among Member States	Frequently reported
Legal harmonisation	Moderately reported
Intelligence sharing	Frequently reported
Rapid technological change	Frequently reported

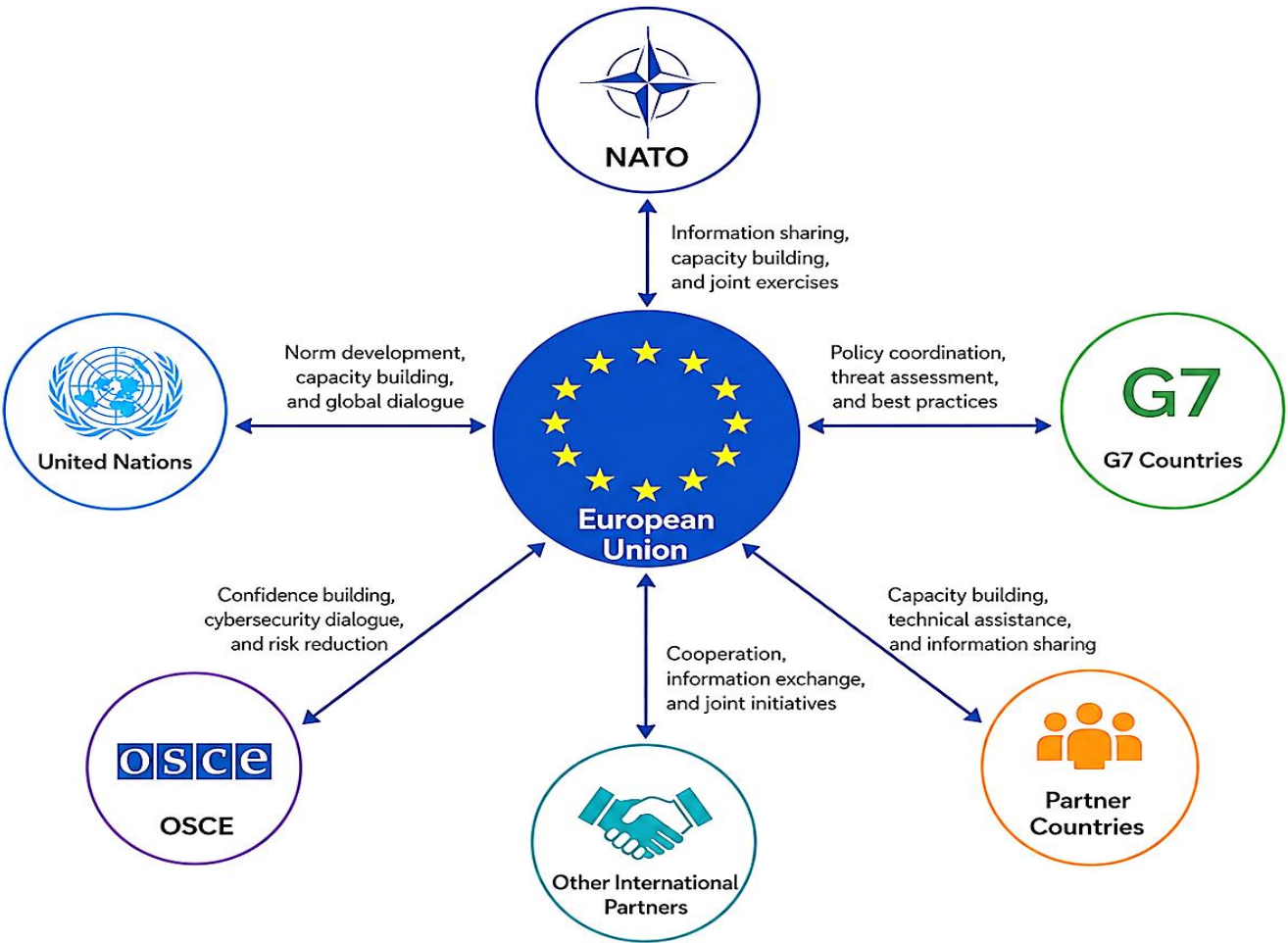
Source: Established through qualitative review of European Union policy documents and learnt literature.

V. International Cooperation and External Engagement

The results show that there is a strong focus on cooperation outside of the European Union in the Cyber Diplomacy Toolbox. Documents under review reflect an active involvement with international organizations, regional security bodies and strategic partners to foster responsible state action in cyberspace.

It also demonstrates that the European Union is supportive of confidence building measures, capacity building programmes in the cyber domain, diplomatic consultations and the development of international norms on cyberspace. These collaborative initiatives are always made a part of the Union's external cybersecurity policy.

Figure 3: Collaboration among the European Union and main international cybersecurity associates.



Overall Findings

The documentary analysis of the European Union's Cyber Diplomacy Toolbox shows that it is a fully-fledged diplomacy tool encompassing legal, institutional, and policy elements to counter new cyber threats. The evidence gathered reveals that coordination within the institutions and a high level of international cooperation and a number of diplomatic response mechanisms are the main features of the framework. At the same time, the reviewed sources all mention implementation problems with respect to cyber attribution, policy coordination, legal consistency and national capabilities. Based on these findings, the effectiveness of the Cyber Diplomacy Toolbox to the research objectives mentioned in this study are evaluated. The effectiveness of the Cyber Diplomacy Toolbox to research goals mentioned in this study are evaluated based on these findings.

Conclusion

Cybersecurity has become an integral part of today's international security environment, and digital technologies have significantly reshaped the modalities of international security. This study analysed the Cyber Diplomacy Toolbox of the European Union (EU) as an integrated diplomatic instrument to enhance cyber resilience through legal cooperation, institutional coordination and international cooperation. The study shows the European Union has taken a more holistic stance on tackling malicious cyber activities through its development, legal foundations and operational mechanisms of the Toolbox. However, the Union does not only use technical cyber-security measures, but has also established a framework of diplomacy, laws, strategic communication, capacity development and international cooperation in a consistent and coordinated governance structure that is able to address the changing threat environment in cyberspace.

The findings highlight that the Cyber Diplomacy Toolbox marks an important step forward in the European Union's external cyber security strategy as it offers a structured diplomatic framework to prevent, deter and respond to cyber incidents. The research findings show that the effectiveness of the Toolbox is strongly related to coordinated action between European institutions and Member States and international partners. Together, these elements help to increase cyber resilience of the

Union, and are being implemented through diplomatic dialogue, cyber sanctions, information exchange, confidence-building measures and cooperation with organisations like NATO, the United Nations, the G7 and OSEC. The Study also concludes that the Cyber Diplomacy Toolbox is not simply a diplomatic instrument kit, but an all-encompassing governance system that brings together legal, political and institutional responses to transnational cyber threats.

Meanwhile, the study finds there are a number of issues that remain to affect the successful implementation of the Toolbox. The level of cybersecurity capabilities in the country, national cybersecurity priorities, the challenge of cyber-attribution and the ongoing nature of cyber threats are important hurdles to higher degree of policy coherence. The challenges highlight the need for ongoing development of legal and diplomatic frameworks to be effective in a changing digital ecosystem. Therefore, cyber resilience needs to be viewed as a continuous journey, not a fixed policy goal, in which continuous institutional adaptation, international cooperation, technological innovation, and political commitment are key factors.

The study is also an academic contribution as it brings together the international relations, cyber security governance, digital diplomacy and international cyber law lenses into a coherent analytical framework. The research concludes, in line with the Theory of Complex Interdependence, that a unilateral, state-driven approach to cybersecurity fails to effectively solve today's cybersecurity challenges. Instead, the results highlight the need for multilateral collaboration, institutional coordination, and rules-based, cross-border diplomacy in the cyber realm. This theoretical vision offers a more comprehensive view on the role of diplomatic action in promoting cyber resilience in the region and adds to the current cybersecurity governance scholarship in Europe.

Policy-wise, the results indicate that the European Union should further strengthen institutional coordination between Member States, create mechanisms to better attribute cyber-attacks, boost intelligence and information sharing, increase cyber capacity building and strengthen the strategic cooperation with international

organisations and trusted global partners. The progress of diplomatic actions and laws will also contribute to the credibility and effectiveness of the Cyber Diplomacy Toolbox if there is greater uniformity. The priorities outlined in this policy framework will help to improve how the EU can collectively face rising cyber threats and to contribute to a stable, safe and rules-based international digital order.

While the research offers an extensive legal and policy assessment, a few limitations are recognized. The study has adopted only a qualitative approach to secondary analysis of official documents, legal instruments, policy reports and academic literature. It does not involve primary empirical evidence gleaned from interviews with policy makers, diplomats, cybersecurity experts or institutional practitioners. In addition, the state of continuous advancement in cyber technologies and international cyber security policies may affect the implementation and effectiveness of the Cyber Diplomacy Toolbox in the future, even in the time frame of this research. Therefore, future research could utilize mixed method or comparative research design to study the practical application of cyber diplomacy in various regional organisations, or empirical case studies and stakeholder's viewpoints to assess the long-term effects of the Toolbox.

Finally, the EU's Cyber Diplomacy Toolbox is an innovative and ongoing approach to a coordinated diplomatic response: it has the potential to enhance cyber resilience by means of legal harmonisation, institutional cooperation and international partnership. The ongoing development and improvement of this framework will continue to be crucial in safeguarding digital infrastructure, contributing to international stability and the promotion of responsible state actions in cyberspace, as threats in the cyber domain continue to grow more sophisticated and geopolitically relevant. The results of this study can serve as a basis for future academic research and can guide the policy maker in strengthening the governance of cyber security on the regional and international level in an increasingly interconnected world.

Recommendations

The results of this research suggest that the

European Union's Cyber Diplomacy Toolbox has developed a thorough toolkit for coordinated EU diplomatic response to new cyber threats, but there are some remaining legal, institutional and operational issues that impact the effectiveness of the toolbox. Policy changes are needed to boost cooperation, institutional capacity and the adaptability of the Toolbox to an ever-changing cyber world to tackle these challenges. The following recommendations are made based on the results, discussion and conclusions of this research.

1. Increase institutional coordination between Member States (MS)

Further improve the coordination mechanisms between the Member States of the European Union: introduce more structured mechanisms for information sharing, joint decision-making and coordinated diplomatic action in response to cyber incidents. Better institutional coherence would facilitate better implementation of the Cyber Diplomacy Toolbox in a timely manner and minimize inconsistencies resulting from the respective national priorities and capacities.

2. Improve Cyber Attribution and Intelligence-Sharing Mechanisms

Accurate and timely attribution remains one of the principal challenges in responding to malicious cyber activities. The European Union should enhance technical cooperation, intelligence-sharing arrangements, and joint cyber threat assessment mechanisms among Member States and relevant agencies. Developing common attribution standards and improving forensic capabilities would increase the credibility and effectiveness of diplomatic and legal responses.

3. Expand International Partnerships and Cyber Diplomacy

Given the transnational nature of cyber threats, the European Union should continue expanding strategic cooperation with international organisations and trusted partners, including NATO, the United Nations, the G7, the Organization for Security and Co-operation in Europe (OSCE), and like-minded countries. Enhanced diplomatic engagement, joint cyber exercises, and collaborative capacity-building initiatives would contribute to stronger international cyber resilience and reinforce the

rules-based international order.

4. Regularly Update the Cyber Diplomacy Toolbox to Address Emerging Technologies

The rapid development of artificial intelligence, quantum computing, cloud technologies, and the Internet of Things has significantly changed the cybersecurity landscape. The European Union should establish a periodic review mechanism to update the Cyber Diplomacy Toolbox so that its legal instruments, diplomatic strategies, and operational procedures remain responsive to emerging technological risks and evolving methods of cyber aggression.

5. Promote Capacity Building and Cyber Diplomacy Training

The effectiveness of the Cyber Diplomacy Toolbox depends on the availability of skilled professionals capable of implementing its diplomatic and legal mechanisms. The European Union should invest in specialised training programmes for diplomats, legal experts, cybersecurity professionals, and policymakers. Strengthening institutional expertise in cyber diplomacy, international cyber law, and digital governance would improve policy implementation and facilitate more effective responses to complex cyber challenges.

6. Enhance Legal Harmonisation and Policy Consistency

Although significant progress has been achieved in developing a common cybersecurity framework, differences in national legislation and implementation practices continue to create operational challenges. The European Union should promote greater legal harmonisation, strengthen compliance mechanisms, and encourage uniform implementation of cybersecurity policies across Member States. A more consistent legal framework would enhance collective resilience and improve the overall effectiveness of coordinated diplomatic action.

The recommendations presented in this study are intended to support the continued evolution of the European Union's Cyber Diplomacy Toolbox as an effective instrument of cybersecurity governance and digital diplomacy. Their implementation would strengthen institutional cooperation, reinforce legal and diplomatic coordination, and improve the European Union's capacity to respond to increasingly sophisticated cyber threats. Collectively, these measures would contribute to a more resilient, secure, and cooperative international cyber environment while advancing the European Union's broader objectives of promoting peace, stability, and responsible state behaviour in cyberspace.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

- Barrinha, A., & Renard, T. (2017). *Cyber-diplomacy: The making of an international society in the digital age*. *Global Affairs*, 3(4–5), 353–364. <https://doi.org/10.1080/23340460.2017.1414924>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Christou, G. (2019). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. London, England: Palgrave Macmillan.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications.
- Hutchinson, T., & Duncan, N. (2012). *Defining and describing what we do: Doctrinal legal research*. *Deakin Law Review*, 17(1), 83–119.
- Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy*. Princeton, NJ: Princeton University Press.
- Keohane, R. O., & Nye, J. S. (2012). *Power and interdependence* (4th ed.). Boston, MA: Pearson Education.
- Miadzvetskaya, Y. (2024). EU sanctions in response to cyber-attacks as crime-based restrictive measures. *Computer Law & Security Review*, 53. <https://doi.org/10.1016/j.clsr.2024.106022>
- Miadzvetskaya, Y., & Wessel, R. A. (2021). The externalisation of the EU's cybersecurity regime: The Cyber Diplomacy Toolbox. *European Papers*, 5(3), 1331–1352. Luxembourg: European Papers.
- Moret, E., & Pawlak, P. (2017). *The EU Cyber Diplomacy Toolbox: Towards a cyber-sanctions regime*. Paris: European Union Institute for Security Studies.
- Nye, J. S. (2011). *The future of power*. New York, NY: PublicAffairs.
- Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). Thousand Oaks, CA: Sage Publications.
- Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. *Journal of Strategic Studies*, 38(1–2), 4–37. <https://doi.org/10.1080/01402390.2014.977382>
- Schreier, M. (2012). *Qualitative content analysis in practice*. London, England: Sage Publications.
- Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: Sage Publications.