





RETHINKING EUROPEAN CYBERSECURITY INTEGRATION THROUGH LIBERAL INTERGOVERNMENTAL POLITICS IN GENERAL DATA PROTECTION REGULATION ENFORCEMENT STUDY



 I Nyoman Aji Suadhana Rai ^{(a)1}  Dudy Heryadi ^(b)  Yanyan Mochamad Yani ^(c)  Asep Kamaluddin Nashir ^(d)

^(a)Research Scholar, International Relations Department, Universitas Padjajaran, Bandung, Indonesia; E-mail: nyoman_rai13@yahoo.com

^(b)Professor, International Relations Department, Universitas Padjajaran, Bandung, Indonesia; E-mail: dudy.heryadi@unpad.ac.id

^(c)Professor, International Relations Department, Universitas Padjajaran, Bandung, Indonesia; E-mail: y.mochamad@unpad.ac.id

^(d)Assistant Professor, International Relations Department, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia; E-mail: asepkamaluddin@upnvj.ac.id

ARTICLE INFO

Article History:

Received: 30th August 2025

Reviewed & Revised: 30th August 2025
 to 8th December 2025

Accepted: 9th December 2025

Published: 11th December 2025

Keywords:

Cybersecurity, Data Protection, Liberal Intergovernmentalism, France, Germany, Supranationalism

JEL Classification Codes:

F52, F51, K24

Peer-Review Model:

External peer review was done through double-blind method.

ABSTRACT

The phenomenon of cyberattacks and data breaches in the EU has led to the implementation of the General Data Protection Regulation (GDPR) in 2018. However, this regulation could turn the supranational institution into a sovereign-based decision-making body and shift people's behavior toward enforcing data protection rules. This study investigates how the European Union implemented its strategy to enforce cybersecurity mechanisms between its member states through data protection regulations. This study employs a qualitative case study approach and collects data from 285 enforcement reports, five binding reports from the EDPB, and two unstructured interviews. We used reflexive thematic analysis to obtain the meaning of each report and each interview. The results reveal that supervisory authorities exercise power and create national and regional preferences that follow individuals and companies in the enforcement of data protection mechanisms in the EU. The study finds that Germany and France share the power to require multinational companies and public entities to comply with data protection rules across the EU. According to the thematic analysis, three themes emerge from the data collected in France and Germany: harmonization of Data Protection and cybersecurity, blending of enforcement, balancing Sovereignty and integration, and protecting national values through EU mechanisms. It shows that the EU's cybersecurity strategy aligns with the principles of Liberal Intergovernmentalism, in which each member state negotiates its preferences through the EDPB and between member states, rather than with the principles of functionalism, in which institutions cooperate voluntarily through spillover mechanisms.

© 2025 by the authors. Licensee CRIBFB, USA. This open-access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

INTRODUCTION

The evolution of cybersecurity governance in Europe reflects the broader political dynamics within the European Union (EU), particularly the balance between supranational regulation and member state sovereignty (Fuchs, 2018; Kasper & Osula, 2023; Carver, 2024; Ruohonen, 2024). As digital technologies and information flows increasingly shape global and regional security, EU member states face growing pressure to coordinate cybersecurity policies while protecting their national interests (Barrinha & Christou, 2022). This tension is especially evident in the formulation and implementation of the General Data Protection Regulation (GDPR), which stands at the intersection of security, sovereignty, and digital rights issues (Jancuete, 2020).

Rather than viewing the GDPR solely as a legal or technical framework for data protection, this study approaches it as a political outcome of intergovernmental negotiations among EU core states (Jancuete, 2020; Hilden, 2019), a phenomenon that some researchers have called data power (Karjalainen, 2022). In this context, Germany and France represent two contrasting yet influential paradigms of cyber governance: Germany, with its emphasis on institutional control and national coordination (Cymutta, 2020; Schallbruch & Skierka, 2018), and France, with its advocacy for openness, digital freedom, and inclusive governance (Bora S., 2023; Ciulla & Varma, 2021). The competition and cooperation between these

¹Corresponding author: ORCID ID: 0000-0002-2063-4276

© 2025 by the authors. Hosting by CRIBFB. Peer review under responsibility of CRIBFB, USA.
<https://doi.org/10.46281/bjmsr.v11i1.2638>

To cite this article: Rai, I. N. A. S., Heryadi, D., Yani, Y. M., & Nashir, A. K. (2025). RETHINKING EUROPEAN CYBERSECURITY INTEGRATION THROUGH LIBERAL INTERGOVERNMENTAL POLITICS IN GENERAL DATA PROTECTION REGULATION ENFORCEMENT STUDY. *Bangladesh Journal of Multidisciplinary Scientific Research*, 11(1), 23-34. <https://doi.org/10.46281/bjmsr.v11i1.2638>

states reveal how national preferences are projected onto regional cybersecurity strategies.

Cybercrime involving telecommunications and technology occurs not only in Europe but also globally in cyberspace. One example is the phenomenon of cybercrime in 2013, related to the framing of Edward Snowden (Di Salvo & Negro, 2016) or cyber-hackivism (Juned, Martin, & Pratama, 2024). Therefore, the development of telecommunications infrastructure has become the primary factor in European security. Critical Infrastructure (CI) in telecommunications is the backbone of information and technology, and it is sometimes targeted by hackers or thieves who use advanced technologies to collect personal information. These situations need to be addressed across Europe to regain the public's trust. Other examples of cybercrime include the cyberattacks in Estonia in 2007, which had a significant impact on the European cybersecurity strategy; the Cambridge Analytica scandal in 2016; the WannaCry attack in 2017, which brought ransomware globally and affected the strategic environment in cyberspace and digitalization; and the development of data protection regulation in 2018, which made the crime of using telecommunication the main target of third parties. Therefore, the European response to this phenomenon has yet to be formulated in cyberspace.

The main argument of integration theory from a neofunctionalist perspective is the "spill over" mechanism, which emphasizes the role of supranational institutions, making them self-sustaining and moving beyond the control of national governments (Bergmann, 2019). However, it only affects the European continent. At the same time, in the cross-region, neofunctionalism has a different perspective, such as security interdependence (Börzel & Risse, 2019), the euro crisis (Nicoli, 2020), or other crises (Schimmelfennig, 2024), such as Brexit, Migration, Covid, and the Russia crisis, which formed a polity of regionalization. We argue that, to some extent, technology can create a new spectrum of more profound interdependence. However, it can create a "technological dilemma" that can harm individual privacy and security in cyberspace. Private companies and public organizations that do not follow adequate levels of protection may lead to public consciousness to safeguard the cyber realms.

Following Moravcsik's view on Liberal Intergovernmental (LI) politics, we argue that understanding the situation in cybersecurity integration through data security (GDPR) can be achieved by the spillover phenomenon on integration (Lynskey, 2017); however, this approach is insufficient (Carver, 2024; Liebetrau, 2024) (Fuchs, 2018). As the limit on Sovereignty in cyberspace was questioned by Barrinha and Christou (2022), European countries faced new problems beyond cybersecurity, such as immigration policy, Brexit, the Ukraine war, and a series of cybersecurity incidents, including the Snowden revelations and the WannaCry attacks. We saw this phenomenon (EU Problems) as a tool for Europe to create a framework to support regulations binding all European countries that follow norms, helping the EU in the internationalization of digital or cyberspace, which was not regulated at the EU level between 2014 and 2018.

Since there is no great power in the context of cyberspace in Europe (Hansel, 2023; Barrinha & Turner, 2024), core state politics plays a crucial role in shaping policy in the European cybersecurity strategy (Genschel & Jachtenfuchs, 2013; Genschel & Jachtenfuchs, 2016; Schramm & Krotz, 2024). We contend that frameworks and standards, such as the 2001 Budapest Convention on Cybercrime, have not established a comprehensive international system for global cybersecurity. This is evident from the numerous cyberattacks that continue to occur in EU countries. Examples include the cyber-attack on Estonia, the rise in identity theft reported by CIFAS UK in 2005, the Trojan Horse breach of the German ministry, the hacking incident known as "No Name Crew" in Germany, and the 2013 NSA controversies related to the Snowden case. Additionally, during the 2017 French presidential election, approximately 10,000 emails were disseminated via an online platform in one night. The ENISA, established under the 2016/1148 NIS 1 Directive, has not succeeded in enhancing cybersecurity across European nations, particularly in core states. The preference of states to regulate data protection through Directive 95/46/EC remains unfulfilled, as evidenced by the court case *Germany v Commission* 518/07, which mandates that independent supervisory authorities operate without being influenced by political or international pressures.

Addressing these issues requires robust regulations backed by strong political and economic support (Weiss & Krieger, 2025; Dunn, Cavelti, & Wenger, 2022) or norms and cultural dimensions (Finnemore & Hollis, 2016). Some experts suggest that regulatory mercantilism (Farrand, Carrapico, & Turobov, 2024), encompassing aspects such as security, Sovereignty, and economics, can be leveraged to develop new geotechnologies and geopolitics. Conversely, some contend that cyberspace sovereignty is simply a political deterrent within EU policy (Carver, 2024; Barrinha & Christou, 2022). Simultaneously, Liebetrau (2024) conceptualizes cybersecurity regulation as a singular market function crucial for achieving success in the region. As Ursula von der Leyen (European Commission, 2020) articulated, there are three critical considerations regarding cybersecurity. First, technology should be designed to benefit individuals, with European values serving as the primary driving force behind technology that serves the population. Second, the concept of a fair and competitive economy is integral to the European value of a future of cyber technology that is reintegrated, particularly in an era characterized by hyper-competitiveness (Munkoe & Molder, 2022; Zisan, 2021) and geopolitical rivalry. The concept of fair competitiveness in data protection has been under consideration since 2013, coinciding with the European Union's recognition of the necessity to regulate the flow of information in online behavior (Mantelero, 2013). Third, an open and democratic sustainable society is a fundamental component of the European Union. In the digital age, such societies enable European countries to navigate the cyber-political landscape that divides the world into distinct sections. As Europeans, we must uphold the fair and competitive values that underpin European principles.

Given that the primary impetus for the competitive digital economy within the European Union is rooted in the labor market and digital technologies, both France and Germany have compelling reasons to transition from traditional manufacturing to a digital economy. However, Germany is less developed in the digital technology sector than France. At some point, France prioritized creating new jobs in the labor market, whereas Germany focused on training and developing its workforce. This strategic approach has been adopted by several countries within the European Union, each implementing the method deemed most appropriate for its specific context.

Germany and France are at the forefront of sector security and policy, setting precedents for other nations. Since

the post-war era, both countries have engaged in cooperative efforts, collectively accounting for approximately 50 percent of the European Union's military and industrial capabilities in security and defense (Major & Molling, 2018). Furthermore, both entities have collaborated to implement the NIS Directive and Critical Infrastructure Protection regulations across the European Union, establishing a benchmark for cybersecurity leadership.

The methods of our research to analyse data using the NVivo Application: first, we collected data from <https://www.enforcementtracker.com> and separated it by country. As already mentioned, we are looking at Germany and France's experiences in implementing data protection since the GDPR took effect. We used data from France and Germany because, according to the LI theory, core-state politics plays an important role in integration, and the two countries' political and economic players are the biggest. Second, we selected data based on the theme, checking each case by hand. From that point of view, we separate the data into categories, such as the reason for the infringement, the sector involved, the type of infringement, the total fine, whether the association is public or private, and the number of people affected by the violation. Third, we are creating a group on the theme so that we can conclude that each case appearing in Germany and France is based on three subject themes: Harmonizing Data Protection and Cyber Security, Balancing Sovereignty and Integration through the EDPB, and Protecting National Preference via EU Mechanism.

This research aims to understand how the implementation of the EU GDPR affects the integration of the EU into cybersecurity. We would like to know how the behaviors (negotiation, bargaining, and diplomacy) of the national actor, especially the EDPB, when a dispute occurs, affect the people in the EU, and which actor (in each country) dominates the national preference when it comes to data protection according to LI theory.

Each chapter in this research is a Literature Review, describing how we collected the material and the methodology that we used, followed by a discussion and conclusion. The literature review presents updated articles on the theory and practice of cybersecurity and its implementation in the region. The materials are described in terms of how we collected data and used the application for a qualitative study. The discussion describes the invention for each case selected in NVivo and identifies key players in each country. The conclusion presents a statement on whether the hypotheses are accepted or rejected, based on the LI theory used in the analysis.

LITERATURE REVIEW

Traditionally, research on European cybersecurity has been characterized by a technocratic approach. Foundational studies delineate threat categories such as cybercrime, cyberwarfare, critical infrastructure resilience, and risk management, and predominantly propose operational solutions to address these issues (Andress & Winterfield, 2011; Daras, 2019; Siegel & Sweeney, 2020). While these studies are essential for practitioners, they predominantly treat cyberspace as an engineering issue and offer limited insight into decision-making processes regarding security, the underlying reasons for these decisions, and their implications for power dynamics within the European Union (Arquilla & Ronfeldt, 1997).

Second, a more recent perspective situates cybersecurity within the domain of international relations and regional integration. Mueller (2010) reconceptualizes Internet governance as a contest over Sovereignty and legitimacy, while Kohler (2020) demonstrates how entities such as ENISA disseminate "soft" security standards throughout Europe. In this context, the scholar appropriately broadens the analytical framework; however, it remains anchored in a supranational and rule-based perspective. Consequently, this approach tends to downplay the significance of hard bargaining, veto points, and side payments, which influence policy implementation once proposals are transitioned from Brussels to the national capitals.

Consequently, government divisions have not been thoroughly examined in the literature. Despite the implementation of the Cybersecurity Act and subsequent EU strategies, effective enforcement is mainly contingent on the political commitment of member states, particularly Germany and France (Genschel & Jachtenfuchs, 2013; Genschel & Jachtenfuchs, 2016; Bora, 2023). Their differing industrial models, Paris's activist "European champion" agenda versus Berlin's ordoliberal reliance on rules, result in contrasting threat perceptions and preferred policy instruments. However, most studies only briefly mention this divergence and seldom treat it as an independent variable that elucidates why EU arrangements fluctuate between ambitious plans and hesitant implementation.

Conceptual fragmentation further compounds this gap. The classic fourfold taxonomies of cyberspace activity cooperation (Bjola & Zaiotti, 2020), conflict (Yannakogeorgos & Lowther, 2013), warfare (Arquilla & Ronfeldt, 1997; Andress & Winterfield, 2011; Geers, 2011), and governance (Mueller, 2010; Kohler, 2020) illuminate breadth but blur key analytical questions: who benefits from cross-border digital markets? How do national security establishments reconcile military doctrine with EU law, and what role do data protection norms, such as the GDPR, hailed as a "gold standard," play in power projection (Siegel & Sweeney, 2020; Daras, 2019)? How does the political economy of data as "the new oil" (Yanwardhana, 2023) reshape these calculations? Without connecting these pieces, for instance, linking cyber resilience frameworks (Carrapico & Barrinha, 2018; Dunn Cavelti, 2008) to the material leverage they create, the proliferation of categories risks masquerading as theoretical progress.

In Europe, traditional approaches to cybersecurity have been predominantly examined from technological, legal, and operational perspectives. The extant literature primarily focuses on frameworks that classify cyber threats into technical domains, such as cybercrime, cyberwarfare, infrastructure resilience, and digital risk management (Andress & Winterfield, 2011; Daras, 2019; Siegel & Sweeney, 2020). While these studies provide crucial insights into the functional and security aspects of cyberspace, they often lack political analysis concerning the integration of cybersecurity strategies within the dynamics of power, state interests, and regional governance.

The development of cybersecurity strategies within the European Union should not be confined to technical or institutional frameworks. As cybersecurity plays a pivotal role in national security, economic competitiveness, and social trust, it has emerged as a politically contested domain. To comprehend the dynamics underpinning the EU's cybersecurity architecture, particularly the General Data Protection Regulation (GDPR) enforcement.

The purpose of this study is to understand regional integration in terms of cybersecurity and data protection. In particular, the political effect of implementing data protection regulations for regional integration is examined. The hypotheses of this research are "regional integration will increase the national security (preference) of each country instead of voluntary integration by the actors (spill over) when it comes to cybersecurity and data protection."

MATERIALS AND METHODS

Research Design

This study aims to investigate how core state systems regulating data protection affect regional enforcement through a case study. When contemporary phenomena in real life reveal unclear boundaries between the phenomenon and its context, the case-based method is the most appropriate approach for gaining detailed insights and understanding the phenomenon (Yin, 2009). This research employed qualitative data collection through systematic case study analysis to understand the actors involved in GDPR enforcement between Germany and France and their roles in regional enforcement within the EDPB (Lamont, 2021). The topics were collected between 2020 and 2023. This research encompasses binding decisions by the European Data Protection Board (EDPB) concerning companies such as Twitter, Facebook Ireland, WhatsApp Ireland, Meta Platforms, TikTok, and Google. In our study, we will employ a reflexive thematic analysis, which is a qualitative method (Braun & Clarke, 2021). A reflexive thematic analysis (RTA) of Liberal Intergovernmentalism has been provided in articles by Ewane (2025) and Lubis, Setiyono, Kushandajani, and Sardini (2025). The Ewane approach enables researchers to identify and analyze patterns and themes within a dataset. In line with this approach, we investigate the EDPB's binding decision to understand the German Supervisory Authority (DE SA) and French Supervisory Authority (France SA) policy positions within the EU GDPR.

Data Collection and Sources

Primary data were obtained through archival and document-based research with an intense investigation of each case (Gagnon, 2010). We also conducted two interviews with representatives from the two countries and five binding decisions of the EDPB. The material data collected from <https://www.enforcementtracker.com/>, an interview, and the EDPB's Binding decision were analysed to interpret the phenomenon. The total number of cases from both countries collected from 2018 to 2025 included 285 case studies from enforcement trackers, five binding decisions from the EDPB, and two interviews with experts.

Reflective Thematic Analysis

We analyzed data with tools from NVivo, which were separated into three reflexive themes (Braun & Clarke, 2021) harmonization of data protection and Cybersecurity, Balancing Sovereignty and integration through EDPB, protecting national preference via EU Mechanism, and associated codes of data such as type of infringement, the articles that have been violated, sector involved, total fine produced, and reason of infringement (individual or organized attack).

Six Phases of RTA

Phase 1. The RTA was a data familiarization phase in this study. In this section, we begin the analysis of the 26 selected materials. During this phase, we highlighted France and Germany's views on data protection regulation at the national level, separating them into two categories: cybersecurity and data protection; Sovereignty and integration; and protection of national preferences via the EU Mechanism. We then analyzed them alongside related cases that could serve as inputs for other themes. This engagement allowed us to identify linguistic patterns, recurring justifications, and narratives of the national interest in the EU as a supranational institution.

Phase 2. Initiated the generation of codes, which are the primary foundation of the analysis. After identifying the relevant data, we developed initial codes in the text with critical semantics and meaning (Braun & Clarke, 2021). The codes were generated using digital coding tools. For example, in relations with harmonizing data protection and cybersecurity, we coded Credential-stuffing attacks, Data Breach, inadequately protected its system, Ransomware attacks, SQL Injection, Adequate safeguard, Advertising message, Analyzed data without consent, Unlawful use of dashcam, Email address visible, Video game, Video surveillance camera, Use WhatsApp for private concern.

Phase 3. This is where the code data is reviewed after code generation. We began collecting data by identifying the shared meanings of the themes. The codes addressed concepts similar to the theme categories. Each theme was shaped by a cluster of related codes that consistently appeared across the documents.

Phase 4. In this phase, we reviewed the themes and revisited the datasets to ensure that each theme captured the data extract. This phase involved checking internal homogeneity and external heterogeneity to ensure that the content was cohesive and free of contradictions. This step was crucial for refining the thematic structure to ensure analytical clarity.

Phase 5. This is the process of defining and naming the themes. Each theme was clearly defined and named to reflect its unique contribution to the research question. The theme begins by harmonizing cybersecurity and data protection, setting the initial backdrop for the selected cases in France and Germany. This was followed by balancing Sovereignty and integration through the EDPB, which was selected to understand the evidence from each national supervisory authority in France and Germany. The last theme aligned with the LI theory, which combines national preferences and rational institutionalization to ensure that negotiations occur within the EU mechanism.

Phase 6. The final phase of the selected theme contributed to the final report of the analysis document *using digital tools*. This is the final phase, which is conducted after deciding on the themes for further analysis.

RESULTS

This study found that France and Germany's supervisory authorities (SA) exercise power through the EDPB mechanism, influencing decisions in each selective case involving Twitter, Facebook, Meta Platforms, WhatsApp, TikTok, and other case studies, by distributing their national preferences into binding enforcement decisions at a regional level.

Table 1. Document Demographic Information

Coding	Reports, Documents, and Supervisory Authority
P1	Thuringen
P2	Schleswig-Hosstein
P3	Saxony
P4	Sachsen-Anhalt
P5	Saarland
P6	Rhineland-Palatinate
P7	Rhineland-Pfalz
P8	Nordhein-Westfalen
P9	Niedersachsen
P10	Mecklenburg-Vorpommern
P11	Hessen
P12	Hamburg
P13	Federal Commission
P14	Bremen
P15	Brandenburg
P16	Berlin
P17	Bavaria
P18	Baden-Wuerttemberg
P19	French Data Protection Authority (CNIL)
P20	Binding Decision EDPB 1 Twitter
P21	Binding Decision EDPB 2 Facebook
P22	Binding Decision EDPB 3 WhatsApp
P23	Binding Decision EDPB 4 Meta Platform Ireland
P24	Binding Decision EDPB 5 TikTok
P25	Interview with a French academic
P26	Interview with a German ambassador expert

Table 1 presents the total of 26 documents analyzed and the resulting Reflexive Thematic Analysis (RTA) for each supervisory authority (SA) in each state. This table reflects the documents that followed Braun and Clarke's (2021) instructions for formulating themes, using the six phases identified in each case study.

Word Cloud Enforcement of GDPR from France and Germany

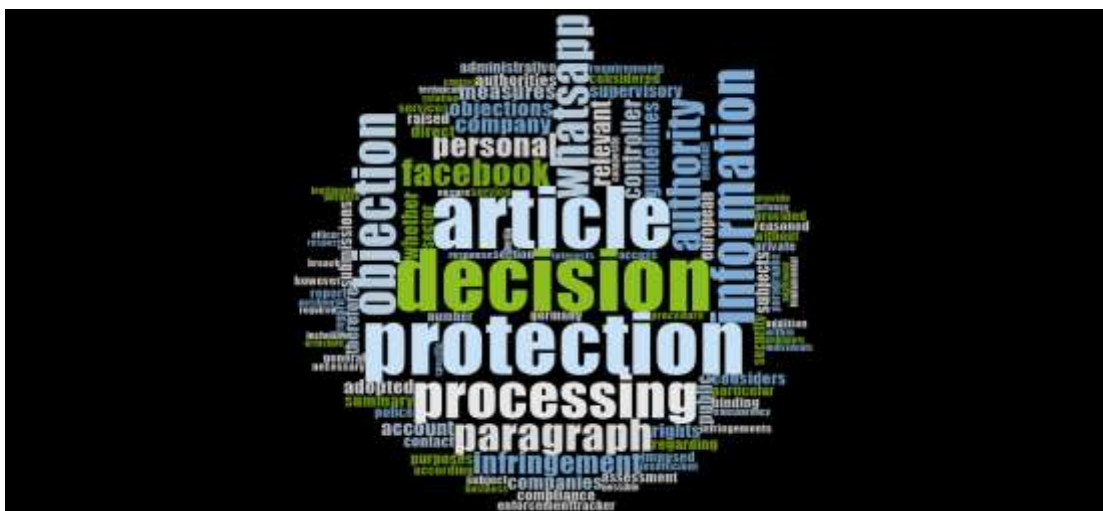


Figure 1. Word cloud enforcement of GDPR from France and Germany. Show the level of core state power plays in the EU GDPR Mechanism.

The word cloud analysis (Figure 1) visually captures the thematic dominance of terms such as “decision,” “protection,” “article,” “processing,” and “Facebook.” These terms indicate that the role of the core state actor in the enforcement of GDPR still predominates over the neo-functionalism or supranational agent perspective. At the same time, “objection” and “authorities” align with the other debate on the enforcement process. Terms such as “Infringement,” “companies,” and “controller” suggest dynamics at the national preference level, where companies, including multinational companies, are relevant actors. Words like “WhatsApp” and “breach” point to the cybersecurity and data protection aspects of Sovereignty for Europeans.

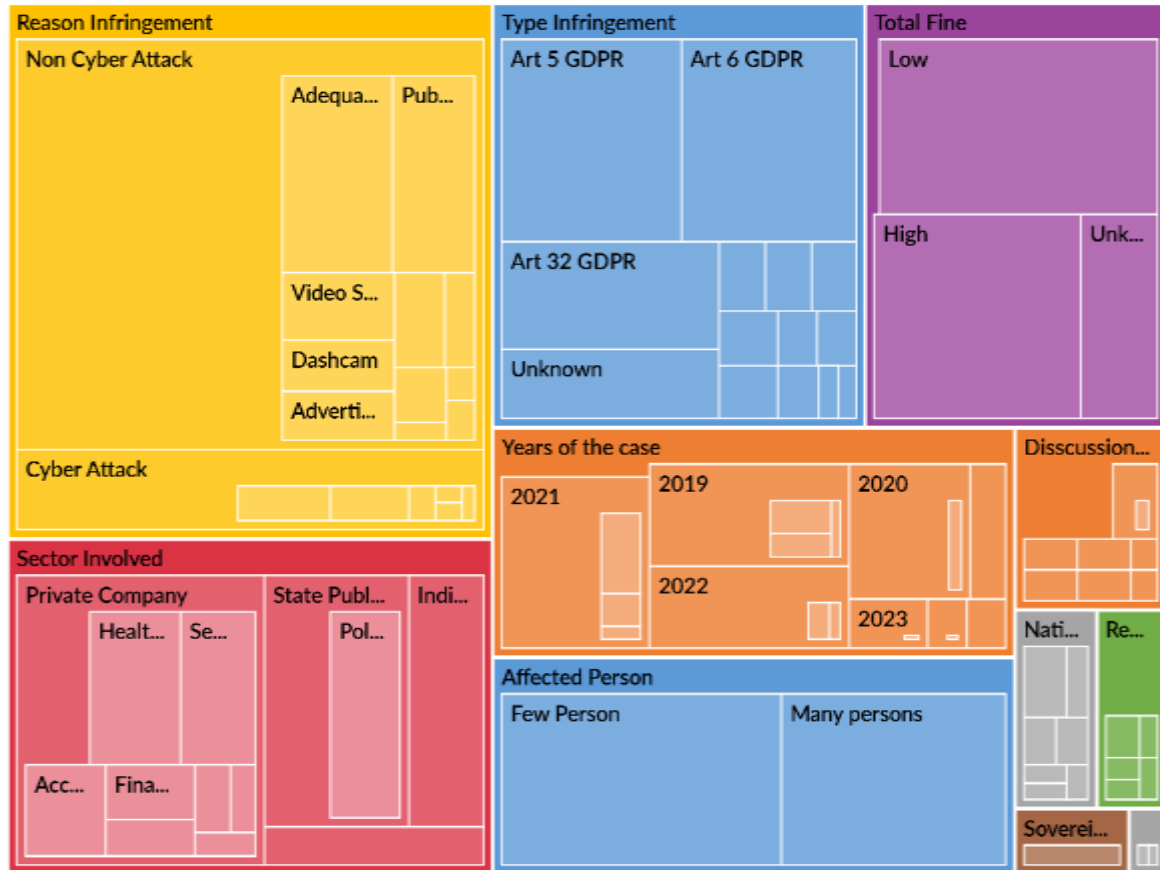


Figure 2. Hierarchy chart illustrating the relationship between cybersecurity and data protection for each supervisory authority in France and Germany.

As illustrated in the Hierarchy Chart (Figure 2), the core state power of the Supervisory Authority (SA) in France and Germany is exercised in a vertically expansive manner, allowing influence over each sector involved, whether by public or private organizations. The process of liberal intergovernmentalism (LI) can be seen in discussions with other states, as shown in the purple chart. The dominance of national preferences is evident in regulations formulated by core state actors, such as cookie regulations, as well as in regional-level determinations of preference. Sovereignty and integration can be observed in companies' authority problems. Whether appropriate technical and organizational measures are used, or whether there is a lack of competent authority. The consensus-building mechanism indicates that regional integration is acceptable.

Table 2. Synthesis of Data: Thema, Sub Thema, and Coding

Theme	Sub-theme	Coding
Harmonising of Data Protection and Cybersecurity	Data protection regulation and cybersecurity regulation	Credential-stuffing attacks, Data Breach, inadequately protected its system, Ransomware attacks, SQL Injection, Adequate safeguard, Advertising message, Analyzed data without consent, Unlawful use of dashcam, Email address visible, Video game, Video surveillance camera, Use WhatsApp for private concern
Balancing Sovereignty and Integration through EDPB	Sovereignty, European Integration, Coordinated Enforcement	E-Privacy regulation, European Academy for Freedom of Information and Data Protection, European Data Governance ACT, Transatlantic Data Privacy Framework
Protecting national preference via the EU Mechanism	National preference, EU Mechanism	Conference of Independent Federal State data protection (DSK), Cookies regulation, Digitalization Act, Petersberg Declaration on data Protection, Role of the BKA (Police Department) in the international Context, Telecommunication and Telemedia Data Protection Act(TTDSG), The Transparency Act,

Table 2 indicates that the LI was constructed from three themes identified in the collected documents. Harmonizing of Data Protection and Cybersecurity contributed to coding credential stuffing attacks, Data Breach, inadequately protected IT systems, ransomware attacks, SQL Injection, inadequate safeguard, advertising messages, analyzing data without consent, unlawful use of dashcam, email address visible, video game, video surveillance camera, and use of WhatsApp for private concerns. Sovereignty and integration are balanced through the E-Privacy Regulation, the European Academy for Freedom of Information and Data Protection, the European Data Governance Act, and the Transatlantic Data Privacy Framework. National protection preferences can be seen in the coding, especially in the police department, and cookie regulations proposed to the EU and later adopted by other EU states. This study finds a correlation with the core state exercising power at the regional level through the EU mechanism. In regards with theme 1, balancing Sovereignty and integration through EDBP, after we analyze From document of Binding EDPB 1 (Twitter) that has been analyzed found that Germany DE SA was using his power to influence decision on potential infringement of Art 5(1) (f) about possibility organizational not following integrity and confidentiality and Art 24 DE SA view that there will be a potential of failure of organizational measure to follow security, in Art 32 also related to pseudonymisation and encryption of personal data that might violate the security of processing, however, through consensus building in EDPB this objection is not seem follow the procedure of objection mechanism. Germany and France, through their SA, follow Moravcsik's idea of national preference, which occurs in each national core state.

Theme 2, Harmonization of Data protection and cybersecurity, can be seen in the relations between each SA in Germany and France, in each case where non-cyber attacks dominated, with associated coding such as adequate safeguards and access to the public.

Databases subject to unauthorized access from public and private organizations account for the most data protection violations, which is not the main topic: cybersecurity.

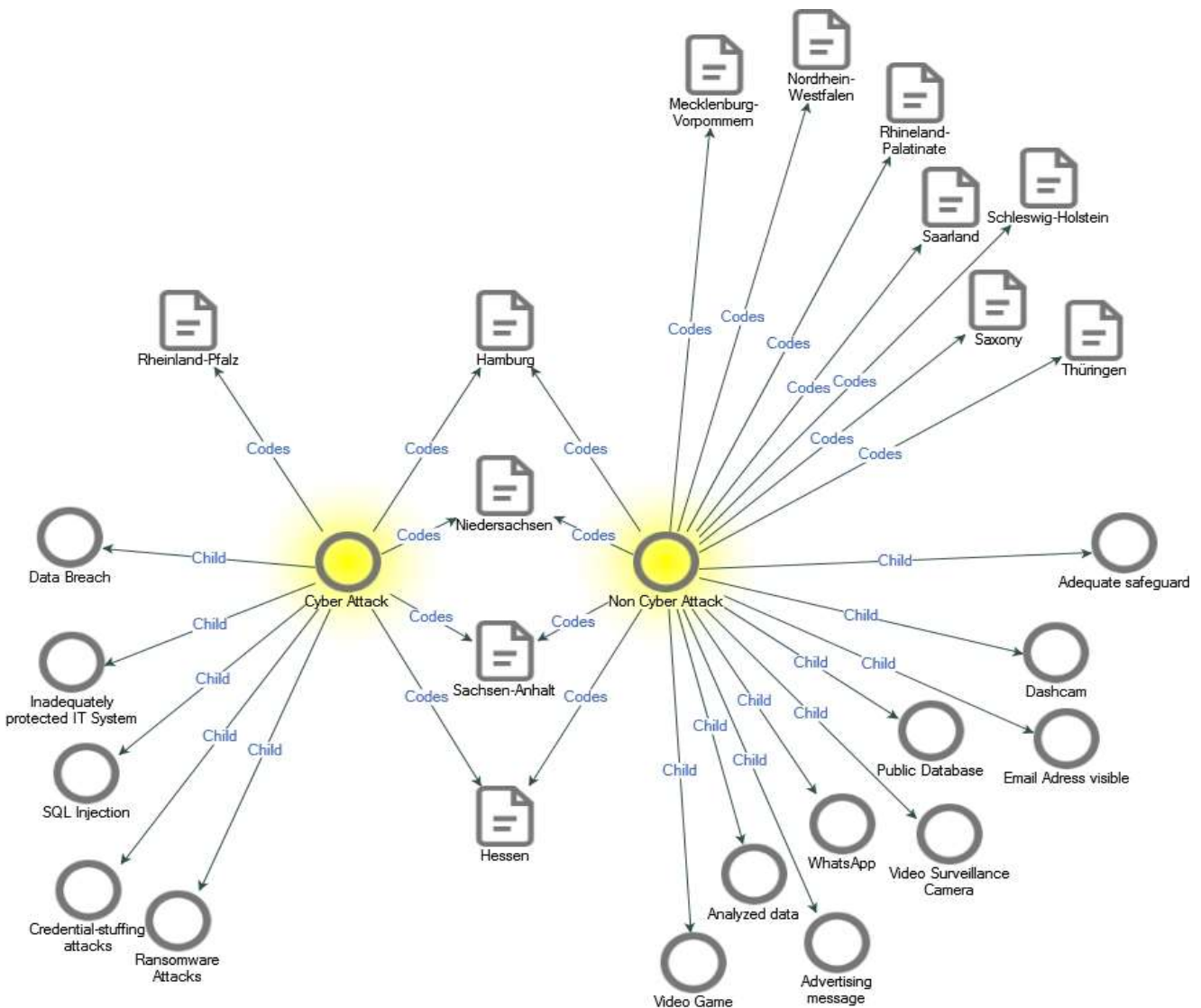


Figure 3. The relation of Cyber Attacks and Non-Cyber Attacks in the enforcement of GDPR

Theme 3, protecting national preference via EU mechanism, can be viewed in document EDPB Binding 2,3,4,5, where each SA, whether from France or Germany, follows national preference related to the situation in its local environment, for example, the cookies regulation that lies in Germany also gets attention from the French SA.

DISCUSSIONS

From the perspective of liberal intergovernmentalism (LI), Germany's involvement in cybersecurity negotiations under the General Data Protection Regulation (GDPR) can be interpreted as an endeavor to align its preference for data sovereignty with the broader objectives of European Union integration. By advocating for robust cybersecurity and privacy frameworks, Germany positions itself as both a protector of national interests and a normative leader within the EU, while avoiding the complete transfer of authority to Brussels.

The German police force operates within the framework of a federal system of government, in which the police are subject to the Sovereignty of the *Länder*. The police are subject to criminal investigations by the *Landeskriminalamt* (LKA) and form an integral component of the *Bundeskriminalamt* (BKA), the federal criminal police. Both the LKA and the BKA have departments specializing in cybercrime. In addition to collaborating with police forces from other countries, Germany's most significant partners include Interpol and Europol, which have specialized units such as the European Cybercrime Center (EC3) and the Joint Cybercrime Action Task Force (J-Cat).

As a central state power, Germany prioritizes public values (Genschel & Jachtenfuchs, 2016), particularly those related to regional interests (Freudlsperger & Jachtenfuchs, 2021). Berlin SA maintained its leadership by developing administrative regulatory institutions that contributed to a stable, rule-based order characterized by intergovernmental cooperation and decentralization rather than supranational integration.

Germany is trying to contribute to the foreign policy framework known as European Political Cooperation. The idea of a Political Union brings the value of intergovernmentalism within the CFSP framework (Haroche, 2023). Germany's national companies and organizations have created a situation in the EU that has driven deeper integration and stabilization since 2018 (Wiliarty, 2011; Mushaben, 2022). This establishes a robust and decentralized cybersecurity policy framework (Farrand, Carrapico, & Turobov, 2024).

When national actors question Sovereignty over data processing, it is input to the national bargain core state actor (Bellanova, Carrapico, & Duez, 2022). Since 2013, following the Snowden revelations, Germany (Pohle, 2020; Steiger, Schunemann, & Dimmroth, 2017) has actively disseminated information on the securitization of data processing and privacy. All media, including television and news channels, provided information supporting Sovereignty in cyberspace and raised privacy concerns. This also applies to France, where the French Minister of Culture, Catherine Morin-Desailly, feels that if countries do not respond to the development of the digital realm soon, it will become a colony. After a few years, the GDPR became a key element in European discussions.

From the perspective of fundamental state power theory, state elites function like intergovernmental economic interest groups. These elites are proponents of enhanced competency at the European Union level, thereby facilitating institutional integration within the core state authority. From a realist perspective, Germany has the potential to meet realist expectations, particularly regarding state power and public administration in the Union's cybersecurity sector. Germany has demonstrated its capability as a nation-state to control and regulate activities in cyberspace effectively. This is evidenced by the enforcement of the General Data Protection Regulation (GDPR) in the EU. Since 2018, the most significant violations by the private sector have originated from German digital industries, including Vodafone and H&M. The total fines imposed on the private sector amounted to approximately 10 million. In contrast, police departments and other public bodies have committed the most frequent violations in the public sector.

Against this background, France has articulated a more inclusive and outward-oriented vision of European Union cybersecurity, rooted in the liberal principles of transparency, pluralism, and multistakeholderism. Since the commencement of President Macron's administration in 2017, France has positioned digital policy as a strategic diplomatic instrument, leveraging initiatives such as the Paris Call for Trust and Security in Cyberspace to assert its leadership in shaping the global digital landscape.

France's cyber strategy is rooted not only in national security considerations but also in its self-conception as a normative power dedicated to promoting its republican values within the digital realm. From the French perspective, the General Data Protection Regulation (GDPR) is perceived not merely as a regulatory framework but as a mechanism for protecting human rights, electoral integrity, and media pluralism. France's strong advocacy for legal instruments, such as Convention 108+, and its emphasis on disinformation regulation exemplify this commitment.

In 2017, during the French elections, a cyberattack (Willsher & Henley, 2017) targeted one of the presidential candidates, Emmanuel Macron. According to the winning team's report, a 'massive and coordinated' attack was carried out by a hacker group. Approximately 10,000 emails and other documents were shared online after the incident. Disinformation in emails and documents can cause political and social instability in France; therefore, electoral authorities prohibit the publication of such information to the public because it may violate the law.

France invited all cyber practitioners and cybersecurity companies to attend the Paris Call. The Paris Call is an international event that focuses on information technology and cyberspace issues. The Paris Call sets out nine principles and norms to maintain security and trust in cyberspace. State representatives, including dozens of private sector participants, attended the prestigious event. Dozens of civil society representatives are spread across the world. This confirms that France is a cyber center with a strong foundation of freedom and inclusiveness in its cybersecurity framework. Representatives from various countries and local governments participated in this event.

French foreign policy is fundamentally characterized by the promotion of peace values that foster interdependence within the context of economic liberalization (Ciulla & Varma, 2021). In France, the process of political integration in Europe has invariably influenced the trajectory of economic liberalization. Staunton's (2025) research provides evidence for assessing European civilization in relation to the International Liberal Order, an integral component of French civilization's pursuit of equality and freedom in shaping international attitudes.

Under Emmanuel Macron's leadership, France's approach to cyberspace governance has been notably influential. Within the European cybersecurity framework, France demonstrates pronounced openness towards the private sector and actively engages with the broader community. This approach aligns with France's longstanding cultural values of openness, freedom, and democracy, which it seeks to extend to the digital domain. Through the Paris Call, France advocates for an Internet governance framework that is open, secure, stable, accessible, and peaceful. This initiative exemplifies President Macron's commitment to establishing global leadership in promoting economic and social stability, particularly in response to the rising tide of nationalism in cyberspace. The Paris Call advocates collaboration between public and private entities to establish new cybersecurity standards to enhance future cyber protection. This emphasizes the importance of utilizing existing international agreements, such as the Budapest Convention on Cybercrime, to combat cybercrime effectively.

The principle of openness is also evident in the CNIL Strategic Plan 2022–2024, which is structured around three primary themes: (1) promoting the control and respect of individual rights in practice, (2) establishing the GDPR as a trusted framework, and (3) prioritizing regulation concerning significant privacy issues. Macron encouraged all sectors of society to protect personal data through stringent cybersecurity measures.

The successful implementation of the Paris Call in 2018 instilled confidence in France to enforce the Personal Data Protection regulations enacted that year. Following a protracted two-year period of anticipation of the enforcement of these regulations, the CNIL was well-positioned to implement the regulatory framework effectively.

Convention 108 offers individuals the opportunity to safeguard their personal data through agreements aligned with international principles. Within this framework, various aspects of data collection are subject to regulation, similar to the European Personal Data Protection Directive. This convention demonstrates France's commitment to addressing international concerns, particularly the protection of fundamental rights amid rapid technological advancements. France consistently prioritizes dialogue in its policymaking processes, necessitating engagement in the digital realm. While adhering to regulations to safeguard personal data, France also seeks to align the digital environment in Europe with its cultural ethos of being open.

France's digital sector policies represent a consensus that encompasses differences, particularly within the private sector. The nation seeks to extend its historical success into the digital space. Consequently, France is recognized for its commitment to openness and an inclusive digital environment that allows the private sector to operate freely. However, this approach has implications for law enforcement in the public sphere. The fines imposed by the CNIL on the public sector in France indicate that external actors must enforce digital regulations. Such actors may include personal data protection communities in countries such as Germany and the UK (Davies, 2022). The need for regional stabilization and integration requires strong leadership from these two countries (Schramm & Krotz, 2024).

CONCLUSIONS

The primary focus of this study is to investigate how data protection regulations affect relations in the region, specifically Germany and France. Although both France and Germany endorse the fundamental objectives of the General Data Protection Regulation (GDPR) and cybersecurity collaboration, they embody distinct strategic cultures. Using a qualitative case study approach, this study collected data from enforcement reports of the GDPR. Germany advocates for controlled institutionalization and intergovernmental regulation, whereas France emphasizes inclusive norm-setting and democratic legitimacy. These differences are not merely stylistic; they are deeply rooted in political ideologies and domestic pressure. Their interaction exemplifies the core of Moravcsik's argument: European integration is driven by the aggregation of national preferences and rational bargaining. Moreover, the GDPR emerged not as a top-down legal imposition but as a negotiated outcome of member-state diplomacy, facilitated by the EU's institutional frameworks.

In light of the preceding discussion, Europe is endeavoring to implement its cybersecurity strategy through intergovernmental collaboration. The principal nations responsible for formulating cybersecurity policies aim to establish standards that align with their national interests. Germany, as a key economic and political force in Europe, seeks to develop a cybersecurity strategy that reflects its intergovernmental approach to regional interests.

Examining the GDPR within the expansive framework of the European cybersecurity strategy indicates that regional digital governance transcends mere technocratic or regulatory efforts. Instead, it constitutes a politically contested domain influenced by the interplay of national preferences, institutional authority, and strategic interests. The European Union, frequently perceived as a normative entity in global digital policy, serves as a platform where principal state powers, notably Germany and France, compete and collaborate to influence policy outcomes in alignment with their domestic agendas and international objectives.

This study finds that the European cybersecurity framework is the product of an intergovernmental compromise that reflects a balance among Sovereignty and integration, state control, and regional coordination. This dynamic interplay between politics, power, and policy will continue to shape the future of cybersecurity in Europe through three themes: harmonizing data protection and cybersecurity, balancing Sovereignty and integration through the EDPB, and protecting national preferences via the EU mechanism.

The first theme, which involves harmonizing data protection and cybersecurity policy, reveals that both states have established a paradoxical framework. This framework necessitates that international companies operating within the EU require broader regulations, such as the European Data Act, to ensure business sector certainty. The second theme, balancing Sovereignty and integration, provides evidence that both states share a cyber preference that aligns national interests with those of individuals and the business sector, thereby addressing regional gaps. An example of this is how multinational digital companies respond to European concerns about privacy and security. Thirdly, national interests have mechanisms for representation within supranational bodies.

Personal data protection and cybersecurity are intrinsically linked and cannot be separated. On the one hand, personal data protection necessitates comprehensive control over the four layers of the digital world. Conversely, effective law enforcement requires entities capable of overseeing the enforcement process, particularly through robust public administration governance. The concept of personal data protection in Europe is inextricably linked to the roles of two key actors in fostering a clean, secure, and open cyber environment. However, it also requires decisiveness from public officials to enforce regulations. The GDPR facilitates intergovernmental cooperation, enabling the enforcement of rules and fostering a cyber climate in Europe that avoids authoritarianism and promotes freedom of expression.

The limits of this study are based only on reports, binding documents from the EDPB, and two unstructured interviews with experts from both countries. This analysis is based on only two countries and does not represent all interests within the EU framework. The absence of data from all countries could lead to different results in other studies. Future research should conduct data triangulation across multiple sources, methods, and theories to address gaps that may arise during the research process.

Author Contribution: Conceptualization, I.N.A.S.R. and D.H.; Methodology, I.N.A.S.R., D.H. and Y.M.Y.; Software, I.N.A.S.R.; Validation, I.N.A.S.R. and A.K.N.; Formal Analysis, I.N.A.S.R. and D.H.; Investigation, I.N.A.S.R. and Y.M.Y.; Resources, I.N.A.S.R. and A.K.N.; Data curation, I.N.A.S.R.; Writing Original Draft Preparation, I.N.A.S.R., D.H., Y.M.Y. and A.K.N.; Writing Review & Editing Preparation, I.N.A.S.R., D.H., Y.M.Y. and A.K.N.; Visualization, I.N.A.S.R.; Supervision, I.N.A.S.R.; Project Administration, I.N.A.S.R.; Funding acquisition, I.N.A.S.R., D.H., Y.M.Y. and A.K.N. The authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Funding: The authors received no direct funding for this research.

Acknowledgments: The author would like to thank the Indonesian education scholarship “afirmasi” for the educational scholarship from semesters 1 to 6.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

- Andress, J., & Winterfield, S. (2011). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier. <https://doi.org/10.1016/C2010-0-66971-9>
- Arquilla, J., & Ronfeldt, D. (1997). In *Athena’s Camp: Preparing for Conflict in the Information Age* (1st ed.). RAND Corporation.
- Barrinha, A., & Christou, G. (2022). Speaking Sovereignty: The EU in the cyber domain. *European Security*, 31(3), 356–376. <https://doi.org/10.1080/09662839.2022.2102895>
- Barrinha, A., & Turner, R. (2024). Strategic narratives and the multilateral governance of cyberspace: The cases of European Union, Russia, and India. *Contemporary Security Policy*, 45(1), 72–109. <https://doi.org/10.1080/13523260.2023.2266906>
- Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, 31(3), 337–355. <https://doi.org/10.1080/09662839.2022.2101887>
- Bjola, C., & Zaiotti, R. (2020). *Digital Diplomacy and International Organisations: Autonomy, Legitimacy and Contestation* (C. Bjola & R. Zaiotti, Eds.; 1st ed.). Routledge. <https://doi.org/10.4324/9781003032724>
- Bora, S. I. (2023). ‘A Sovereign Europe’? Strategic Use of Discourse at the Service of French Economic Interests in EU Politics (2017–2022). *JCMS: Journal of Common Market Studies*, 61(5), 1281–1297. <https://doi.org/10.1111/jcms.13463>
- Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide* (1st edition). Sage Publication.
- Bergmann, J. (2019). Neofunctionalism and EU external policy integration: the case of capacity building in support of security and development (CBSD). *Journal of European Public Policy*, 26(9), 1253–1272. <https://doi.org/10.1080/13501763.2018.1526204>
- Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, 19(3), 299–303. <https://doi.org/10.1080/23745118.2018.1430712>
- Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union’s external relations policy. *Journal of European Public Policy*, 31(8), 2250–2286. <https://doi.org/10.1080/13501763.2023.2295523>
- Dunn Cavelty, M. D. (2008). *Cyber-security and Threat Politics: US Effort to secure the information age*. Routledge. Retrieved from https://www.routledge.com/Cyber-Security-and-Threat-Politics-US-Efforts-to-Secure-the-Information-Age/Dunn/p/book/9780415569880?srsltid=AfmBOoqb7nRK_otjjknintzPjtFr-P35idfkBd8mkgLhJuXBc9sDDEI
- Dunn Cavelty, M. D., & Wenger, A. (2022). *Cyber Security, Politics, Socio-Technological Transformations, and Political Fragmentation*. Routledge.
- Ciulla, M., & Varma, T. (2021). The lonely leader: The origins of France’s strategy for EU foreign policy. European Council on Foreign Relations. Retrieved from <https://ecfr.eu/article/the-lonely-leader-the-origins-of-frances-strategy-for-eu-foreign-policy/>
- European Commission. (2020). *SHAPING EUROPE’S DIGITAL FUTURE*. Retrieved from <https://share.google/TEP6oGmv7J7mplb9Q>

- Cymutta, S. (2020). National Cybersecurity Organisation: Germany.
- Daras, N. (2019). Cyber-Security and Information Warfare.
- Davies, P. (2022). France election: How Macron and Le Pen's pledges for tech, cybersecurity, and social media compare. Euro News. Retrieved from <https://www.euronews.com/next/2022/04/20/french-election-how-macron-and-le-pen-s-pledges-for-tech-cybersecurity-and-social-media-co>
- Di Salvo, P., & Negro, G. (2016). Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States. *Journalism*, 17(7), 805–822. <https://doi.org/10.1177/1464884915595472>
- Ewane, G. (2025). Norway's Immigration Policies and the Influence of Europeanisation.
- Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and Sovereignty. *International Affairs*, 100(6), 2379–2397. <https://doi.org/10.1093/ia/iaae231>
- Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*, 110(3), 425–479. <https://doi.org/10.1017/S0002930000016894>
- Schimmelfennig, F. (2024). Crisis and polity formation in the European Union. *Journal of European Public Policy*, 31(10), 3396–3420. <https://doi.org/10.1080/13501763.2024.2313107>
- Freudlsperger, C., & Jachtenfuchs, M. (2021). A member state like any other? Germany and the European integration of core state powers. *Journal of European Integration*, 43(2), 117–135. <https://doi.org/10.1080/07036337.2021.1877695>
- Fuchs, T. A. E. (2018). The Limits of European Integration Theories: Cyber-Development and the Future of the European Union. In: Carayannis, E., Campbell, D., Efthymiopoulos, M. (eds) *Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense*. Springer, Cham. https://doi.org/10.1007/978-3-319-09069-6_62
- Gagnon, Y.-C. (2010). *The Case Study as Research Method: A Practical Handbook*. Presses de Université du Québec.
- Geers, K. (2011). *STRATEGIC CYBER SECURITY*. CCD OOE Publication.
- Genschel, P., & Jachtenfuchs, M. (Eds.). (2013). *Beyond the Regulatory Polity?: The European Integration of Core State Powers*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199662821.001.0001>
- Genschel, P., & Jachtenfuchs, M. (2016). More integration, less federation: The European integration of core state powers. *Journal of European Public Policy*, 23(1), 42–59. <https://doi.org/10.1080/13501763.2015.1055782>
- Hansel, M. (2023). Great power narratives on the challenges of cyber norm building. *Policy Design and Practice*, 6(2), 182–197. <https://doi.org/10.1080/25741292.2023.2175995>
- Haroche, P. (2023). A 'Geopolitical Commission': Supranationalism Meets Global Power Competition. *JCMS: Journal of Common Market Studies*, 61(4), 970–987. <https://doi.org/10.1111/jcms.13440>
- Hilden, J. (2019). *The Politics of Datafication: The Influence of Lobbyist on the EU's Data Protection Reform and its Consequences for Legitimacy of the GDPR*. Doctoral Dissertation. Retrieved from https://helka.helsinki.fi/discovery/fulldisplay/alma9932988073506253/358UOH_INST:VU1
- Jancuite, L. (2020). European Data Protection Board: A nascent EU agency or an 'intergovernmental club'? *International Data Privacy Law*, 10(1), 57–75. <https://doi.org/10.1093/idpl/ipz021>
- Juned, M., Martin, A., & Pratama, N. (2024). Bjorka's Hacktivism in Indonesia: The Intercourse Paradox of Cyberdemocracy, Cyberactivism, and Cybersecurity. *Academic Journal of Interdisciplinary Studies*, 13(5), 369. <https://doi.org/10.36941/ajis-2024-0171>
- Karjalainen, T. (2022). The battle of power: Enforcing data protection law against companies holding data power. *Computer Law & Security Review*, 47, 105742. <https://doi.org/10.1016/j.clsr.2022.105742>
- Kasper, A., & Osula, A.-M. (2023). 'Spill Over' and 'Fail Forward' in the EU's Cybersecurity Regulations. In D. Ramiro Troitiño, T. Kerikmäe, & O. Hamulák (Eds.), *Digital Development of the European Union: An Interdisciplinary Perspective* (pp. 21–44). Springer International Publishing. https://doi.org/10.1007/978-3-031-27312-4_3
- Kohler, C. (2020). The EU Cybersecurity Act and European standards: An introduction to the role of European standardization. *International Cybersecurity Law Review*, 1(1–2), 7–12. <https://doi.org/10.1365/s43439-020-00008-1>
- Lamont, C. (2021). *Research Methods in International Relations* (Second Edition). Sage Publication.
- Liebetrau, T. (2024). Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice. *JCMS: Journal of Common Market Studies*, 62(3), 705–724. <https://doi.org/10.1111/jcms.13523>
- Lubis, Setiyono, B., Kushandajani, & Sardini, N. H. (2025). THE STRUCTURE AND STRATEGY OF LOCAL STRONGMEN IN THE DEFEAT OF INDEPENDENT CANDIDATES: A QUALITATIVE STUDY. *Bangladesh Journal of Multidisciplinary Scientific Research*, 10(5), 12–19. <https://doi.org/10.46281/4kz2g758>
- Lynskey, O. (2017). The 'Europeanisation' of Data Protection Law. *Cambridge Yearbook of European Legal Studies*, 19, 252–286. <https://doi.org/10.1017/cel.2016.15>
- Major, C., & Molling, C. (2018). Franco-German Differences Over Defense Make Europe Vulnerable.
- Mantelero, A. (2013). Competitive value of data protection: The impact of data protection regulation on online behaviour. *International Data Privacy Law*, 3(4), 229–238. <https://doi.org/10.1093/idpl/ipt016>
- Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. The MIT Press. <https://doi.org/10.7551/mitpress/9780262014595.001.0001>
- Mushaben, J. M. (2022). Against All Odds: Angela Merkel, Ursula von der Leyen, Annegret Kramp-Karrenbauer and the German Paradox of Female CDU Leadership. *German Politics*, 31(1), 20–39. <https://doi.org/10.1080/09644008.2021.2000599>
- Munkoe, M., & Molder, H. (2022). Cybersecurity in the era of hypercompetitiveness: can the EU meet the new challenges?. *Revista CIDOB d'Afers Internacionals*, 131, 69–92. Retrieved from <https://www.jstor.org/stable/27186235>

- Nicoli, F. (2020). Neofunctionalism revisited: integration theory and varieties of outcomes in the Eurocrisis. *Journal of European Integration*, 42(7), 897–916. <https://doi.org/10.1080/07036337.2019.1670658>
- Pohle, J. (2020). Digital Sovereignty. A new key concept of digital policy in Germany and Europe.
- Ruohonen, J. (2024). The Incoherency Risk in the EU's New Cyber Security Policies. <https://doi.org/10.48550/ARXIV.2405.12043>
- Schallbruch, M., & Skierka, I. (2018). The Organisation of Cybersecurity in Germany. In *Cybersecurity in Germany* (pp. 31-47). Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-90014-8>
- Schramm, L., & Krotz, U. (2024). Leadership in European crisis politics: France, Germany, and the difficult quest for regional stabilization and integration. *Journal of European Public Policy*, 31(5), 1153–1178. <https://doi.org/10.1080/13501763.2023.2169742>
- Siegel, C. A., & Sweeney, M. (2020). *Cyber strategy: risk-driven security and resiliency*. Auerbach Publications.
- Steiger, S., Schunemann, W. J., & Dimmroth, K. (2017). Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany. *Media and Communication*, 5(1), 7–16. <https://doi.org/10.17645/mac.v5i1.814>
- Staunton, T. (2025). An exploration of tensions amongst career guidance practitioners when it comes to the conceptualisation of digital technology. *International Journal for Educational and Vocational Guidance*, 1–17. <https://doi.org/10.1007/s10775-024-09722-2>
- Börzel, T. A., & Risse, T. (2019). Grand theories of integration and the challenges of comparative regionalism. *Journal of European Public Policy*, 26(8), 1231-1252. <https://doi.org/10.1080/13501763.2019.1622589>
- Weiss, M., & Krieger, N. (2025). The political economy of cybersecurity: Governments, firms and opportunity structures for business power. *Contemporary Security Policy*, 46(3), 403–428. <https://doi.org/10.1080/13523260.2025.2474867>
- Wiliarty, S. E. (2011). Gender and energy policy making under the first Merkel government. *German Politics*, 20(3), 449–463. <https://doi.org/10.1080/09644008.2011.614841>
- Willsher, K., & Henley, J. (2017). Emmanuel Macron's campaign hacked on eve of French election. Retrieved from <https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>
- Yannakogeorgos, P. A., & Lowther, A. B. (Eds.). (2013). *Conflict and Cooperation in Cyberspace: The Challenge to National Security* (0 ed.). CRC Press. <https://doi.org/10.1201/b15253>
- Yanwardhana, E. (2023). Jokowi: Data Adalah “New Oil” yang Berharga & Tidak Terhingga. CNBC Indonesia.
- Yin, R. K. (2009). *Case Study Research: Design and Methods* (3rd ed.). Sage Publication.
- Zisan, T. H. (2021). ANALYZING THE STATUS OF WOMEN IN E-GOVERNANCE ERA OF BANGLADESH: CHALLENGES AND POTENTIALS. *Bangladesh Journal of Multidisciplinary Scientific Research*, 3(2), 1-10. <https://doi.org/10.46281/bjmsr.v3i2.1169>

Publisher's Note: CRIBFB stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



© 2025 by the authors. Licensee CRIBFB, USA. This open-access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

Bangladesh Journal of Multidisciplinary Scientific Research (P-ISSN 2687-850X E-ISSN 2687-8518) by CRIBFB is licensed under a Creative Commons Attribution 4.0 International License.