The Legal Framework for Cybersecurity in Protecting E-Government Services

BAUMMAR, MAEL[*]

ABSTRACT *This paper examines the legal framework for cybersecurity in protecting e-government services, focusing on the sufficiency of European and German legislation. The analysis indicates that while German law effectively addresses a wide range of cybercrimes, it lacks specific provisions for enhanced penalties targeting attacks on e-government entities. The European Union's legislative framework has contributed significantly to harmonizing cybersecurity regulations across member states, however, additional advancements are necessary to address the unusual challenges faced by e-government services. Finally, the research reviews the crucial role of critical infrastructure operators.*

KEYWORDS: *Cybersecurity - E-government - Cybercrimes*

1. Introduction

The governments worldwide have adopted digital services to enhance public sector efficiency, improve service delivery, and streamline administrative processes, prompted by digital development. However, ensuring that this transformation upholds the integrity of public service systems and established legal frameworks remains a critical concern.

As governments transition to digital platforms, their reliance on Information and Communication Technology (ICT) exposes them to various cyber threats, such as data breaches, hacker attacks, and malware. Technological advancements in e-services are paralleled by the rise of cybercrime, making cybersecurity an urgent priority.

1. 1 General Context and Significance of the Study

The digital transformation taking place in most aspects of contemporary life presents governments with a critical challenge and requires significant efforts to keep up with this development. Public expectations are rising for governments to provide electronic services with the same efficiency and effectiveness they receive from the private sector.[1] Baummar[2] notes that technological

[*] PhD student, University of Pécs, Faculty of Law, Doctoral School of Law.

[1] Michael E.Milakovich, *Digital Governance: Applying Advanced Technologies to Improve Public Service* (New York: Routledge, 2021): 19.

[2] Mael Baummar, "Modernising Public Administration: Reimagining Public Administration for the Digital Age." *Közigazgatási és Infokommunikációs Jogi PhD Tanulmányok* no. 5.1 (2024): 6.

advancements, particularly in the fields of artificial intelligence and data analytics, hold great potential to transform the way public services are delivered. Additionally, Baummar posits that for public administration to effectively address the challenges and seize the opportunities of our increasingly digital age, digital technology must be embraced as a core component of governance. By reimagining the role of the state in the digital age, governments can foster a more efficient, responsive, and citizen-centric public administration, ensuring a sustainable, inclusive, and equitable future for all.[3]

On the other hand, Hassan, R. G. et al. indicated that access to e-government services and information must be guaranteed to individuals with the requisite legal authorisation.[4]

Kumar & Panchanatham, stated that to ensure cybersecurity in e-government-related operations, it is essential to prove the identity of all system users.[5] Milić et al., also pointed out some examples, such as the application of biometric identity verification for users of electronic government services as a unique means of authentication and permission. If citizens' identity and tax identification numbers are stolen, it can cause significant harm to the users. Biometric identity verification helps in avoiding unauthorized access in such cases.[6]

From this point of view, it can be argued, that the importance of providing public services online is as significant as the services themselves. As a result, disruptions in e-government services can have serious consequences, including the interruption of essential public services. This emphasises the critical need to ensure the stability and security of online public services, making it essential to study the cyber threats that target e-government infrastructures. Consequently, the value of cybersecurity in e-government stems directly from the vital role of public services.

Some researchers posit that the simplest means of avoiding cyber threats in online services is to refrain from utilising such services. As Schechter stated, the potential risks can be avoided by abstaining from risky activities. An example provided by Schechter of risk avoidance is the use of traditional paper ballots instead of electronic voting in general elections. This approach is inconsistent with the central objective of government, which is to serve the public effectively and efficiently. However, unlike optional risks, avoiding e-government services

[3] Baummar, “Modernising Public Administration,” 9.

[4] G. Hassan, Rasha and Othman O. Khalifa. “E-Government—an Information Security Perspective.” *International Journal of Computer Trends and Technology (IJCTT)* 36, no. 1 (2016): 2.

[5] Kumar D, and Dr. N. Panchanatham, “A Case Study on Cyber Security in E-Governance.” *International Research Journal of Engineering and Technology (IRJET)* 2, no.8 (2015): 273.

[6] Milic Petar, Dragana Kolarić, Kristijan Kuk, Stefan Kartunov, and Brankica Popovic, “The Importance of Secure Access to E-Government Services,” in *International Scientific Conference “Archibald Reiss Days”: Thematic Conference Proceedings of International Significance*, ed. Dragana Kolarić (2016), 315.

entirely is not a practical solution. It is not feasible to avoid governmental activities and services entirely.[7]

Additionally, since the public sector seems to be more vulnerable to spearphishing attacks, according to previous studies,[8] therefore, if governments do not invest in cybersecurity at the same level as the development of their services, it can lead to grave breaches.[9] This is also confirmed by Halchin stating that, without feathered cybersecurity efforts, cyberattacks could negatively affect public services and ICT infrastructure.[10]

The lack of sufficient policy measures not only affects the extent of damage caused by cyberattacks but can also lead to a slowdown in technological innovation and thus increased economic costs.[11] In some cases, countries such as Germany, the United States, China and Japan have suffered losses of 200 billion US dollars. Similarly, cybercrime in Italy resulted in $875 million in losses, with the cost of recovery and alternative opportunities rising to $8.5 billion.[12]

Accordingly, when it comes to e-government, cybersecurity represents a very important topic.

1. 2 Research Problem and Objectives

This research aims to highlight the need for effective legal frameworks that ensure the protection of cybersecurity for e-government services while maintaining a balance between security and accessibility. To achieve this, the focus will be on the research problem concerning to what extent the current cybersecurity laws provide legal support for e-government. How do the experiences of countries like Germany shape more effective legal policies? The goal is to provide a critical analysis of the legal frameworks for cybersecurity and evaluate their adequacy in ensuring e-government services.

[7] Stuart Edward Schechter, Computer Security Strength and Risk: a Quantitative Approach (PhD diss. Harvard University, 2004), 28.

[8] Symantec (2014), "*Symantec Internet Security Threat Report*," https://docs.broadcom.com/doc/istr-14-april-volume-19-en: 36.

[9] Global Cybersecurity Index (GCI) (2018), https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Publications.aspx.

[10] L. Elaine Halchin, "Electronic Government: Government Capability and Terrorist Resource," *Government Information Quarterly* 21, no.4 (2004): 407.

[11] David Burt, Aaron Kleiner, J. Paul Nicholas and Kevin Sullivan, "Cyberspace 2025 Today's Decisions, Tomorrow's Terrain. Navigating the Future of Cybersecurity Policy," *Microsoft Corporation* (2014): 31.

[12] Center for Strategic and International Studies. 2014. "Net Losses: Estimating the Global Cost of Cybercrime." Report, June 2014: 18. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

1. 3 Definition of *e-government*

Hu et al.[13] state that the term "e-government" is globally used, with variations in interpretations among individuals. This suggests that there is no unified definition of the term.

In the context of this article, the term refers to the use of information technology in the administration sector. Its main goal is to provide services to citizens while improving the efficiency and effectiveness of administrative tasks in terms of cost, quality and time.[14]

The definition of e-government as outlined by the United Nations also encompasses the provision of government services to citizens via the Internet. It is defined as "utilizing the Internet and the World Wide Web for delivering government information and services to citizens".[15] Moreover, Jaeger introduced additional terms that expand upon this definition, including database, networks, discussion support, multimedia, automation, tracking and tracing, and personal identification technologies.[16]

Similarly, Yildiz highlighted that the definition of e-government should not be limited to specific technologies, service providers, or associated entities. Instead, it is a concept defined by the overarching goal of enhancing government information and providing services to citizens and businesses.[17]

From another perspective, the e-government scientific community does not necessarily need a unified model but relies on a shared identity. This representation embodies how members of the field perceive it, rather than prescribing how they should think about it.[18]

Some researchers incorporate the concept of security into the definition of e-government. According to the analysis conducted by Hu et al., the commonly accepted definition of e-government includes several elements that comprise the concept of e-government. These elements include, among other things, initiatives aiming to enhance service quality and security, communication processes, policy-making, security, and overall service quality.[19]

[13] Guangwei Hu, Wenwen Pan, Mingxin Lu, Jie Wang, "The Widely Shared Definition of e-Government: An Exploratory Study," *The Electronic Library* 27, no.6 (2009): 6.

[14] Mete Yildiz, "E-government Research: Reviewing the Literature, Limitations, and Ways Forward," *Government Information Quarterly* 24, no.3 (2007): 650.

[15] United Nations (UN). 2002. "Benchmarking E-government: A Global Perspective," 16. Available at: https://desapublications.un.org/file/790/download

[16] Paul T Jaeger, "The Endless Wire: E-government as Global Phenomenon," *Government Information Quarterly* 20, no.4 (2003): 323–331.

[17] Yildiz, "E-government Research," 654.

[18] Rajiv Nag, Donald C. Hambrick, and Ming-Jer Chen, "What is Strategic Management, Really? Inductive Derivation of a Consensus Definition of the Field," *Strategic Management Journal* 28, no.9 (2007): 950.

[19] Hu, et al, "The Widely Shared Definition of e-Government," 9.

2. The Legal Relationship Between E-Government and Cybersecurity

Krishna and Sebastian assert that the growing cybersecurity challenges, driven by the rapid development of e-government services, are pushing governments to establish and implement cybersecurity guidelines and standards. This, in turn, enhances the efficiency of e-government services. Thus, cybersecurity must keep pace with digital advancements to ensure resilience in cyberspace. Furthermore, Hassan and Khalifa highlight that e-government services require integrity to prevent any form of tampering with information and data, ensuring they remain in their original, valid state.[20]

2. 1 Understanding E-Government Services

To stay within the research scope, cybersecurity can be categorized into two types: the first pertains to measures that users of electronic services must follow to protect their data. These include safety and cybersecurity practices imposed on users of electronic services, including government services. This category encompasses cybersecurity laws and cybercrime regulations that users can rely on when facing threats or cybercrimes, covering reporting, prosecution, litigation, as well as the right to privacy and data protection. The second type concerns cybersecurity measures adopted by governments to protect their electronic services. While these two types overlap significantly, this research focuses on cybersecurity laws related to e-government services.

To understand the nature of e-government services, it is essential to distinguish between four types of government interactions: Through Government-to-Citizen (G2C), as Alshehri and Drew explain, citizens can conveniently and instantly access government information and services from anywhere, anytime.[21] The Government-to-Business (G2B) system, similar to G2C, is beneficial, as Moon (2002) notes, in enhancing the efficiency and quality of services and transactions within the business sector, promoting equity and transparency in government contracts and projects.[22] Government-to-Government (G2G), as mentioned by Alshehri and Drew, has the primary objective of improving the organizational processes between authorities by improving cooperation and coordination.[23] The last type is the Government-to-Employee (G2E) system: as for the relationship

[20] Hassan and Khalifa. "E-Government—an Information Security Perspective," 3.

[21] Mohammed Alshehri, and Steve Drew. "E-Government Fundamentals." *IADIS International Conference ICT, Society and Human Beings*. 2010: 36.

[22] Jae Moon, "The Evolution of E-Government Among Municipalities: Rhetoric or Reality." *Public Administration Review* 62, no. 4 (July 2002): 424–433. https://doi.org/10.1111/0033-3352.00196

[23] Alshehri and Drew, "E-Government Fundamentals," 36.

between government and employees, some researchers view it as an internal component of government operations, distinct from e-government.[24] According to W Seifert, the purpose of this relationship is to serve employees by providing online services such as applying for annual leave, checking leave balances, and reviewing payroll records, among others.[25]

According to Millard, the most significant operational challenge facing e-government is undoubtedly cybersecurity, encompassing threats to identity, privacy, and data systems[26]. Specifically, e-government must address security challenges, such as information interception, manipulation, denial of services, theft of system resources, faking of information, tampering and forgery.[27] These threats impose substantial financial burdens on governments, with their impact likely to escalate as cybercrime risks and sophistication grow.[28] Moreover, e-government services must store citizens' data, inherently vulnerable to cyberattacks that could result in illegal theft or alteration of this information.[29]

2. 2 Challenges of E-Government: Cybersecurity

Cybersecurity law, as stated by Kumar and Panchanatham (2015), is a law that addresses issues within the virtual world, such as data and information privacy. It also includes rules defining cybersecurity crimes and compensating for damage that may result from them. From the perspective of e-government, the mentioned challenges related to e-government security, the threat of cybersecurity can come from government employees, clients, or users of electronic governance programs. Threat sources can also be external, originating from hackers or organized criminal entities.[30] According to Fuster et al. the term "cybersecurity" has various

[24] B.T Riley, "Electronic Governance and Electronic Democracy: Living and Working in The Connected World," *Commonwealth Centre For Electronic Governance, Brisbane Australia* no. 2 (2011) Cited in Alshehri and Drew, "E-Government Fundamentals," 36.

[25] W Seifert, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance. Congressional Research Service: The Library of Congress* (2013), Cited in Alshehri and Drew, "E-Government Fundamentals," 36.

[26] Jeremy Millard, "The Global Rise of E-Government and Its Security Implications," in *Cybersecurity: Public Sector Threats and Responses*, ed. Kim J. Andreasson (Boca Raton, FL: Taylor & Francis, 2011): 5.

[27] Zhitian Zhou, and Congyang Hu, "Study on the E-Government Security Risk Management," *International Journal of Computer Science and Network Security* 8, no.5 (2008): 208–213.

[28] David Maimon and Eric R. Louderback, "Cyber-Dependent Crimes: An Interdisciplinary Review," *Annual Review of Criminology* no. 2 (2019): 191–216.

[29] Singh, Shailendra, and D. Singh Karaulia, "E-governance: Information security issues," in *International Conference on Computer Science and Information Technology (ICCSIT'2011) Pattaya* (2011): 121.

[30] Kumar D and Dr. N. Panchanatham, "A Case Study on Cyber Security in E-Governance," 272.

dimensions from the European Union's perspective. It includes cyber resilience, cybercrime concerns, cyber defence, and global cybersecurity.[31]

The Cybersecurity Act of the European Union, Article 2(1) introduces the following legal definition: "*The term 'cybersecurity' means the measures necessary to protect network and information systems, the users of those systems, and other persons affected by cyber threats.*"[32]

The Term is defined in the International Standard ISO/IEC 27002:2005 as the confidentiality, integrity and availability of information.[33] Other researchers defined information security as "the protection of information and its critical elements, including the systems and devices that use, store, and transmit that information."[34]

3. Legal Framework of Cybersecurity

The government should be committed to implementing comprehensive technical measures and closing security loopholes to protect personal data. However, some researchers contend that merely providing technical protection and eliminating digital vulnerabilities is insufficient for ensuring the security of the digital environment. Consequently, they propose an additional framework for addressing this issue. In their 2016 study, Hassan and Khalifa introduce the concept of "binding force," which posits that legal obligations can serve to bolster cybersecurity protection. According to the principle of legally binding force, cybersecurity can be ensured and improved by establishing rules, conditions and regulations that have legal force, as well as coherent terms of use, for example, by establishing legal requirements that must be complied with when using electronic services, and also by establishing strict requirements for user identity documentation by requiring valid legal proof of the user's identity.[35] Milic et al. come to a similar conclusion and agree that suitable legal procedures and regulation of the digital environment can help prevent cyberattacks.[36]

Cybersecurity encompasses a set of legislations aimed at protecting digital infrastructure, sensitive data, and electronic systems in both public and private sectors. These legislations are comprehensive, addressing the needs of various industries and domains. This paper focuses on examining these legislations in the context of e-government services, allowing for an in-depth exploration of their effectiveness in safeguarding such platforms. The research will centre on

[31] Gloria González Fuster and Lina Jasmontaite, "Cybersecurity Regulation in the European Union: the Digital, the Critical and Fundamental Rights," *The Ethics of Cybersecurity* (2020): 97–115. https://doi.org/10.1007/978-3-030-29053-5_5.

[32] Regulation (EU) 2019/881 (Cybersecurity Act, Article 2, paragraph 1).

[33] International Standard ISO/IEC 27002 (2005). ISO/IEC 27002: Information technology — Security techniques — Code of practice for information security management 2005, 2.5.

[34] Michael E Whitman, and Herbert J. Mattord. Principles of Information Security. 6th *ed. Boston, MA: Cengage Learning,* 2018: 11.

[35] Hassan and Khalifa. "E-Government—an Information Security Perspective," 2.

[36] Milić, et al. "The Importance of Secure Access to E-Government Services," 315.

challenges such as information interception, manipulation, denial of services, theft of system resources, faking of information and tampering and forgery.

3. 1 The European Legal Framework for Cybersecurity

In the 1990s, the EU directives related to cybersecurity were not binding. Rather, they were merely recommendations aimed at encouraging countries to adopt their national legal procedures on cybersecurity and to make legislative proposals in support of cyber protection. In 2005, the Council of the European Union adopted Council Framework Decision No. 2005/222/JHA of 24 February 2005, which is considered to be one of the first legally binding acts of the European Union on attacks on information systems. This decision obliges Member States to investigate cases of unauthorised access to data and information systems and classify them as criminal offences. The decision emphasises the need to establish 24/7 contact points to issue warnings at the EU level in the event of cyber-attacks.[37]

A review of the decision reveals that it aims to standardise legislation across EU member states concerning attacks on information systems. This will facilitate the ability of e-governments to address cross-border cyber threats and ensure the safety of sensitive data and systems used in the provision of electronic public services.

This decision is highly significant as it strengthens the protection of digital infrastructure that governments use to deliver services to citizens. This includes safeguarding government information systems from cyberattacks such as hacking, viruses, and malware, which could disrupt the continuity of public services and national security.

Additionally, as mentioned earlier, e-government is not limited to the online delivery of public services (government to citizen); it also encompasses the management and regulation of digital infrastructure and the interaction between various governmental entities (government-to-government). Accordingly, the coordination between authorities to address cybercrimes can be considered part of e-government activities.

To provide a framework for the categorisation of EU regulations relevant to the field of cybersecurity, we can draw upon the report by Niethammer et al.:

3. 1. 1 The Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive): This directive entered into force in early 2023 and stipulates that EU member states are required to incorporate its rules into their national laws by 18 October 2024.

The NIS 2 Directive also does not explicitly address e-government, nevertheless, it indirectly impacts it by focusing on the protection of essential digital infrastructures, including those used by governments to deliver services. While the directive targets sectors such as energy, transport, healthcare, and water,

[37] Filip Radoniewicz, "Cybersecurity in the European Union Law," *Cybersecurity in Poland: Legal Aspects* (2022): 67.

which are deemed vital, it also encompasses digital services, of which e-government services are a key component. While e-government is not explicitly referenced, the safeguarding of government-operated digital systems and sensitive data represents a pivotal element of the directive. A comprehensive examination of the text thus demonstrates that the NIS 2 Directive plays a pivotal role in reinforcing the cybersecurity framework that underpins the continuity and security of e-government services across the EU.[38]

3. 1. 2 The Digital Operational Resilience Act (DORA): This regulation entered into force at the beginning of 2023, and will be applicable as of January 17, 2025. The regulation includes specific resiliency requirements for financial entities and ICT service providers.

The Digital Operational Resilience Act (DORA) is aimed at enhancing the stability of the financial system within the European Union by ensuring that financial institutions can withstand and manage digital risks and technological crises. It includes provisions focused on protecting digital infrastructure, securing data, and ensuring business continuity in the face of cyberattacks and technological disruptions.

From an overview of the provisions of the regulation, it can be inferred that the legislation is primarily targeted at financial institutions. However, it also establishes requirements pertaining to the resilience of digital systems, as well as the adoption of cybersecurity best practices across a number of sectors, including, for instance, those involving government systems that process financial transactions or that rely heavily on digital infrastructure.[39]

3. 1. 3 The Cyber Resilience Act (CRA): The European regulation, known as the Cyber Resilience Act (CRA), has been designed to enhance the cybersecurity of digital products. It places a particular emphasis on the protection of both hardware and software against cyber risks, with a specific focus on those that could potentially impact critical infrastructures. As the CRA is primarily concerned with the security of digital products across a range of industrial and commercial sectors, its relevance to e-government is indirect. The act does not address the specific challenges or frameworks associated with e-government services in a dedicated manner. Nevertheless, the provisions of the CRA related to the cybersecurity of digital infrastructure and the resilience of products used within these sectors may have a secondary impact on the protection of e-government services. The CRA contributes to the enhancement of the cybersecurity posture of e-government systems by ensuring the security and resilience of the hardware and software utilised by government agencies, despite

[38] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[39] The Digital Operational Resilience Act (DORA).

not being explicitly designed for this purpose. Consequently, while not targeting e-government directly, the CRA may influence the security of digital public services by strengthening the broader digital ecosystem in which they operate.

In addition to the above, the Cybersecurity Act strengthens the European Union's cybersecurity capabilities by establishing the European Union Agency for Cybersecurity (ENISA) and creating a framework for the certification of digital services. While these laws do not specifically target e-government, they provide a fundamental legal and regulatory framework that indirectly impacts the protection of e-government services by enhancing security standards for digital systems, critical infrastructure, and data protection across both the public and private sectors. Therefore, their provisions are crucial for improving the security of e-government infrastructures within the European Union.

The objective of this section is not to provide an exhaustive analysis of the details of European Union cybersecurity legislation and regulations. Instead, it aims to present an overview of the EU’s cybersecurity laws from the perspective of their relevance to e-government. The adequacy of this legislation is dependent on the manner in which the EU’s legislative acts are formulated, their binding nature, and the extent to which they encompass legal aspects in comparison to local laws. Consequently, the following section will analyse the cybersecurity legislation in Germany to assess the appropriateness of the current legislative framework.

3. 2 The Legal Framework for Cybersecurity in Germany: An Example of National Implementation

Criminal law is the main legal framework for addressing cybercrime. However, legal responses to more specific matters also fall under other laws, such as civil and administrative law. Each legal system has defined objectives and guarantees for cybersecurity.[40]

3. 2. 1 Cybersecurity under German law

This section offers an overview of the main provisions related to cybersecurity in German laws and the strengths and weaknesses of the German approach.

3. 2. 1. 1 Cybercrimes

The principal matters addressed in this research are encompassed within the scope of cybercrimes as delineated by German legislation, outlined as follows:[41]

The act of gaining unauthorised access to a computer system, including the use of hacking and illegally gaining unauthorized access to data, falls within the

[40] Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko, “Comprehensive Study on Cybercrime.” *United Nations Office on Drugs and Crime, Tech. Rep* (2013): 51–52.

[41] ICLG. 2024. “Cybersecurity Laws and Regulations – Germany.” In *Cybersecurity Laws and Regulations 2025*, ed. Edward R. McNicholas (London: Global Legal Group) https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany.

scope of criminal law and is punishable. Furthermore, the individuals attempting to delete or render data unusable may face imprisonment, particularly when the target is a public authority. Also, phishing for unauthorized access to data is prohibited. Additionally, falsifying technical records is a criminal offence. The creation or distribution of tools for cybercrimes is prohibited. This encompasses the sale of software or devices designed for such purposes, as well as incitement to commit cybercrimes and intentional and unlawful assistance in committing cybercrimes. Identity theft, contingent on the methodology employed, may constitute fraud, computer fraud, or document forgery. In addition, the use of another individual's identity may be considered forgery of documents or data. Additionally, breaches related to employees, such as the exploitation of trust by current or former employees, can result in prosecution. Other cybercrimes include unauthorised handling, interception, violation of confidentiality of communications, computer sabotage, breaches of the GDPR, and falsification of digital evidence.

It can further be concluded that German criminal law does not differentiate between cybercrimes targeting e-government entities and those targeting private sector entities. Nevertheless, an examination of these crimes from the perspective of e-government reveals that they inherently affect e-government practices as a matter of course.

For example, unauthorised access to a computer system, including hacking and the illicit acquisition of data, can directly impact users of e-government services. It may be more appropriate to impose more severe penalties when such crimes target e-government systems, given the harm they cause, not only to users but also to trust, the quality and infrastructure of governmental services. In accordance with the extant legal provisions, those who perpetrate such crimes are liable to punishment under Sections 202a and 202b of the German Criminal Code, which may entail a term of imprisonment of up to three years or a fine.

This viewpoint is corroborated by the observation that numerous countries' legislation imposes more stringent sanctions when the affected party is a governmental entity. Research undertaken in 2013 by the United Nations Office on Drugs and Crime (UNODC) revealed that in excess of 50% of the national laws examined provided for special protection by increasing penalties for unauthorised access to computers managed by governmental authorities or connected to the operation of critical infrastructure.[42]

Conversely, in the case of a denial-of-service (DoS) attack, the German Criminal Code, under Section 303b, prescribes a penalty of up to three years' imprisonment. The penalty can be extended to five years if the target is a government authority.

3. 2. 1. 2 Cybersecurity legislation

Cybersecurity legislation is not limited to criminal law; it also includes several other regulations such as the Federal Office for Information Security Act (BSI

[42] Malby et al. "Comprehensive Study on Cybercrime," 85.

Act - BSIG), the Federal Data Protection Act (Bundesdatenschutzgesetz BDSG), as well as sector-specific regulations like the Telecommunications and Telemedia Data Protection Act (TTDSG), the Telecommunications Act (Telekommunikationsgesetz), and other laws applicable to banking (Kreditwesengesetz), energy industry (Energiewirtschaftsgesetz), securities trading (Wertpapierhandelsgesetz), and the Federal Trade Secrets Protection Act (Gesetz zum Schutz von Geschäftsgeheimnissen).

Additionally, informal guidelines are provided through documents such as the BSI Guide for Information Technology Security. Compliance with international standards, such as ISO/IEC 15408, the ISO/IEC 27000 series, and the Information Technology Control Objectives and Related Technologies (COBIT), is considered crucial. Furthermore, the European Cybersecurity Act grants the European Union Agency for Cybersecurity (ENISA) the authority to issue cybersecurity certifications, which companies may voluntarily obtain to demonstrate compliance with cybersecurity regulations.

3. 2. 1. 2 The strengths and weaknesses of the German approach

One of the prominent strengths of the German legal approach is its coverage and inclusiveness of a wide range of potential cybercrimes, allowing for the handling of a broad spectrum of cybersecurity threats. This demonstrates that German law is aligned with technological developments and highly adaptable to the evolving nature of these crimes, keeping pace with the various forms of cyber threats, such as hacking, data theft, system manipulation, and cyber sabotage. The legal framework enables the handling of different methods that may be used by perpetrators of cyberattacks, thereby reinforcing the ability to confront the growing issue of cybersecurity.

However, there are some gaps in this approach, especially when it comes to cybercrimes targeting the public sector. Since cybercrimes can also target government entities, these attacks pose a significant threat to public institutions, and the impact of such attacks may be more pronounced on government infrastructure. An attack could disrupt essential services relied upon by citizens or steal sensitive data, which could undermine public trust in services, along with increasing costs for the public sector. The provision of eGovernment services is characterized by a high degree of confidence that transactions are adequately protected without compromising their security. This is achieved by securing both the technical and non-technical infrastructure to ensure the stability of transactions and strengthen citizens’ trust. The aspect of trust, as mentioned by Milić et al., helps the government enhance its electronic services and leads it to success.[43]

In this context, it may make sense to impose more stringent penalties for such cases, given the potential widespread impact of these attacks. This would justify stricter penalties to deter such crimes and protect the state’s critical infrastructure. Moreover, tightening penalties in this context would ensure consistency across

[43] Milić et al., “The Importance of Secure Access to E-Government Services,” 315.

all types of cybercrimes and their corresponding punishments within this framework.

4. Regulation of Basic Infrastructure Operators

Following a review of cybercrimes and associated legislation, this section seeks to elucidate the measures, regulations, obligations and sanctions that govern the conduct of operators of basic infrastructure. Despite there being no exclusive government operators of such infrastructure in the European Union, and despite infrastructure operators not providing their services solely to the public sector, these measures and regulations are considered in this research from the perspective of e-government.

4. 1 The regulations that govern operators of basic infrastructure facilities

Infrastructures include facilities, like energy, communication network, public roads, public health, safe water supply, food security, and sanitation. They are of great significance to the functioning of society, as their failure or weakness may lead to material shortages or risks to public safety.[44]

Regardless, the list of essential infrastructures was extended to cover retail outlets, hospitals, data centres, banking and financial services and derivatives transactions, among others, with the second amendment to the ordinance (BSI-KritisV, Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz).[45]

Niethammer et al. stated that infrastructure operators are obliged to undertake all reasonable regulatory and technical efforts by implementing the latest security measures, which have recently been tightened under Article 8a (1) and (1a) of the BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik), to avoid service interruptions and to ensure the integrity, security and confidentiality of their information technology systems. Moreover, operators of critical infrastructures are required:

- to prove compliance with BSI requirements to the BSI at least every two years through security audits, inspections or certifications;
- to register with the BSI, give notice to the authorities and provide a contact point to the BSI within the first working day after the designation as critical infrastructure, and this contact point has to be available around the clock seven days a week; and
- to report incidents to BSI through the designated contact point.

Beyond this, critical infrastructures are subject to the requirements of NIS 2, whereby they are considered essential facilities. The new Directive on the Resilience of Critical Entities (RCE), presented at the same time as the NIS 2 Directive, updates the conditions for critical entities, for example, concerning risk

[44] ICLG, “Cybersecurity Laws and Regulations – Germany.”

[45] Ibid.

assessments and obligations to report. Member states must implement the RCE Directive into national law by October 18, 2024.[46]

4. 2 Reporting to authorities

Under German and European law, there are special reporting obligations for incidents:[47]

4. 2. 1 The essential facility subject to NIS 2 must, in the event of significant incidents, notify the competent authority appointed by the national law. The responsible authority in Germany is the BSI.[48]

This reporting requirement contains a set of measures, including the early warning to the CSIRT (computer security incident response teams) within 24 hours, notifying the incident within 72 hours, and the final and interim report upon request within one month of the date of the report of the incident.

4. 2. 2 According to Section 8b of the Federal Office for Information Security Act (BSIG), operators of critical infrastructures must immediately report certain disruptions to the availability, integrity, authenticity, and confidentiality of the IT systems, components, or processes to the BSI. The report must contain information about the disruption, possible cross-border consequences, and the technical conditions, specifically, the suspected or actual cause, the affected IT systems, and the type of system affected.

4. 2. 3 Under the provisions outlined in the Digital Operational Resilience Act (DORA), financial entities are obligated to categorise incidents and notify competent authorities about significant ICT-related incidents, as per Article 17 and subsequent articles. The reporting of noteworthy cyber threats may also be voluntary. The initial notification and subsequent reports must furnish the competent authority with comprehensive information to facilitate the assessment of the significance and potential cross-border ramifications of the major ICT-related incident. The specified timeframe for reporting, initially perceived as: without undue delay or within the business day, is slated to be established by the Joint Committee of European Supervisory Authorities by July 17, 2024.

4. 2. 4 Controllers are obligated to inform the relevant Data Protection Authority about personal data breaches under Article 33 of the GDPR, unless the security breach is deemed unlikely to pose a significant risk to the rights and freedoms of the data subject. This notification must be submitted promptly and no later than 72 hours after discovering the breach. The report should include a comprehensive account of the incident, specifying the category of the affected data, identifying the concerned data subjects, and providing a detailed overview of the measures implemented to rectify or alleviate any adverse consequences. Additionally, the notification to the competent Data Protection Authority should outline the anticipated repercussions of the personal data breach and detail the actions taken

[46] Ibid.

[47] Ibid.

[48] Federal Office for Information Security (BSI).

by the controller to mitigate the impact. Furthermore, the data protection officer's name and contact information must be included in the notification.

4. 2. 5 Public telecommunications networks or service providers are obligated, as per Section 168 of the Telecommunications Act, to promptly inform the Federal Network Agency and the BSI of any disruptions to telecommunications networks and services that result in or have the potential to result in significant security breaches. The notification must encompass details regarding the disruption, including the technical aspects, specifically the suspected or actual cause and the information technology affected.

4. 2. 6 Reporting to Affected Individuals or Third Parties:

In the event of an incident involving a breach of personal data that poses a significant threat to the rights and freedoms of individuals, controllers must notify the data subject of the breach without undue delay under Article 34 of the General Data Protection Regulation.

Furthermore, financial entities subject to DORA law are required to promptly notify their clients of any information technology and communication incidents that affect their financial interests (Article 19). This includes reporting the measures taken to mitigate the negative impacts of such incidents. In the case of a significant cyber threat, financial entities must, as necessary, notify their potential clients of the appropriate preventive measures they can take.[49]

4. 3 Sanctions

The NIS 2 Directive establishes the authority for Member States to impose fines on essential entities, amounting to a maximum of €10 million or 2% of the total annual worldwide turnover, as outlined in Article 34. For important entities, fines may reach up to €7 million or 1.4% of the total annual worldwide turnover, with the higher of the two being applicable. These figures are subject to potential increases under national legislation. Moreover, the German law on administrative offences (OwiG) permits the doubling of fines under specific circumstances.

A notable change introduced by the NIS 2 Directive, detailed in Articles 32(6) and 33(5) of NIS 2, emphasizes management responsibility. The directive provides the option of temporarily removing management, as specified in Article 32(5)(b) of NIS 2.

Fines under the Digital Operational Resilience Act (DORA) are determined by the competent authority and national legal framework, under Article 50 and related provisions. The specific sequence of proceedings depends on the contextual circumstances.

Concerning fines under the German Information Technology Law (BSIG), Article 30(2) of BSIG outlines fines ranging from €100,000 to €20 million. These fines can be levied if a critical infrastructure subsidiary fails to adhere to requirements or submit the necessary documents. The Federal Office for Information Security (BSI) has established typical thresholds for fines, such as up to €20 million for the violation of security flaw processing, up to €10 million

[49] ICLG, "Cybersecurity Laws and Regulations: Germany."

for failure to submit evidence, up to €10 million for non-implementation of technical and organizational measures, up to €500,000 for non-registration with BSI, up to €500,000 for failure to report incidents, and up to €100,000 for the absence of a dedicated contact point.

Article 83 of the General Data Protection Regulation outlines fines for non-compliance with specified requirements, reaching up to €10 million or 2% of the total annual worldwide sales, depending on the type of data protection violation. In terms of implementation, examples of actions taken in cases of non-compliance with the aforementioned requirements are not provided in the recent precise regulation issued by the BSIG group, as of the preparation date of this report. Nevertheless, German data protection authorities have continued to impose administrative fines on companies that do not comply with Articles 32 and 30 of the General Data Protection Regulation. For instance, in 2022, an automotive manufacturing company in Lower Saxony was fined €1.1 million for the failure to document technical and organizational security measures during the testing of the driver assistance system.

A review of the regulatory framework for critical infrastructure in the context of cybersecurity in the European Union and Germany reveals an increasing focus on enhancing cybersecurity. Organisations responsible for critical infrastructure are obliged to implement robust security measures in order to comply with regulations such as NIS 2, DORA, and BSIG. These rules are in place to protect the confidentiality, integrity, and reliability of the services that these infrastructures provide. Furthermore, penalties and fines are imposed on those who fail to comply with these regulations, which demonstrates the seriousness with which the authorities regard the protection of cybersecurity and encourages businesses to improve their technological infrastructure in order to meet these standards.

5. An Analysis and Discussion of the Challenges in Cybersecurity

In light of the increasing reliance on digital infrastructure to provide public services, cybersecurity for e-government systems has become a significant concern. Governments face serious challenges in ensuring cybersecurity, particularly because cybersecurity issues transcend national borders, necessitating coordination and collaboration among nations. This requires unified mechanisms, joint bodies, and appropriate authorities to address cyber threats effectively. Consequently, the inconsistency between local and international regulations directly impacts cybersecurity measures.

Obiso and Fowlie assert that discrepancies and incongruities in national and regional legislation substantially compromise the efficacy and efficiency of cybersecurity measures, thereby intensifying the threats posed by cyberattacks and online criminal activities. The absence of international harmonisation in cybercrime legislation engenders complications in investigations and prosecutions, as criminal activities are categorised in divergent ways across different countries. In light of the global nature of the Internet, a unified approach is imperative to ensure its security.[50]

For the European Union, cybersecurity directives and decisions aim to tackle these challenges by harmonizing cybersecurity laws. These directives provide member states with guidelines on unifying their legislation and coordinating their efforts. Additionally, they establish coordinating and supervisory bodies to enhance cooperation and consistency among member states in the realm of cybersecurity.

One of the primary challenges facing nations in the field of cybersecurity is the ability of legislation to keep pace with technological advancements and to effectively address cyber threats. Germany has demonstrated notable progress in aligning its cybersecurity laws with these developments. Its legislation covers cybercrimes and threats comprehensively and ensures that EU directives are enforceable at the national level. Similarly, EU legislation addresses cybersecurity challenges, including initiatives such as the Artificial Intelligence Act. However, these laws require continuous review and revision, leading to lengthy and complex legislative processes. This may result in delays that risk the delivery of secure public services.

For instance, despite the significance of the subject of artificial intelligence and the associated risks posed by its misuse in various fields, as outlined in the draft law, the debate surrounding the European Artificial Intelligence Act, which commenced in April 2021 with the presentation of the European Commission's initial proposal, has since undergone numerous phases of evolution. This process included discussions in the European Parliament and the Council of the European Union, as well as contributions from the private sector, academic experts, and civil society. Most of the rules of the AI Act will come into force on 2 August 2026. Exceptions are made for prohibitions of AI systems deemed to present an unacceptable risk, which will already apply after six months, and the rules for so-called general-purpose AI models, which will apply after 12 months.[51]

It is essential to reconsider existing legislative mechanisms and develop faster processes that align with the rapid pace of technological innovation. This includes revisiting traditional legislative procedures, integrating technology-based approaches, and conducting ongoing research and discussions to refine legislative mechanisms and enact laws effectively. By doing so, public services can remain secure and efficient in the digital era. Furthermore, in the event that neither novel measures are devised nor the ongoing advanced threats still need to be addressed, and a successful attack occurs, there will inevitably be political pressure to enact reactive legislation aimed at addressing the perceived cause of the attack as

[50] Marco Obiso and Gary Fowlie, “Toward a Global Approach to Cybersecurity,” in *Cybersecurity: Public Sector Threats and Responses*, ed. Kim J. Andreasson (Boca Raton, FL: Taylor & Francis, 2011): 84.

[51] European Commission. (n.d.). European Artificial Intelligence Act comes into force. ec.europa.eu. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4123.

argued by Teplinsky.[52] Such legislation may be expedited, resulting in ineffectual policies prioritising mere compliance over the actual protection of interests.[53]

On the other hand, the novelty of e-government services, the seriousness of cyber threats, and the delay in issuing legislation related to e-governance make the progress of electronic services cautious and slow, which is not in line with the rapid pace of technological development. This highlights the necessity and importance of adopting a legislative framework for cybersecurity that is suitable to address any threats accompanying technological advancement and provides governments and legislators with the confidence to develop e-government services.

An opposing perspective warns against the introduction of burdensome regulations that fail to consider economic implications. Burt et al. argue that striking a balance in drafting technology-related regulations is essential to harness the benefits offered by modern states, such as cost reduction, enhanced e-government, and improved well-being. Failure to achieve this balance, while neglecting economic considerations, may lead to the imposition of overly restrictive compliance measures that hinder technological innovation and diminish economic growth.[54]

However, cyber threats and electronic crimes have become a source of concern among users of electronic services. This concern makes users hesitant and cautious when utilizing e-government services, which often require the submission of highly sensitive and private personal data. This hesitation impacts the quality of services provided by e-governments and highlights the growing importance of cybersecurity. As Millard asserted, the establishment of adequate privacy and data protection, along with the trust they facilitate, is paramount to the full realisation of the advantages offered by e-government.[55] Likewise, Seifert observes, that the realm of information security, often termed cyber security or computer security, represents a significant challenge within the context of e-government. This is due to its role as a crucial element in the establishment of trust between citizens and the government.[56]

It is not only the lack of trust among users that affects e-government services. The lack of clarity in legislation, users' unfamiliarity with how to apply laws or report electronic crimes, and the ambiguity surrounding jurisdiction further complicate the matter. This understanding aligns with what Sutherland

[52] Melanie J Teplinsky, “Fiddling on the Roof: Recent Developments in Cybersecurity.” *American University Business Law Review* 2, no. 2 (2013): 315–392. Cited in Chris Laughlin, Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective (2016). *Colorado Technology Law Journal* 14, no. 2 (2016). SSRN: https://ssrn.com/abstract=2871452: 262.

[53] Laughlin, “Cybersecurity in Critical Infrastructure Sectors,” 362.

[54] Burt et al., “Cyberspace 2025 Today’s Decisions, Tomorrow’s Terrain,” 47.

[55] Millard, “The Global Rise of E-Government and Its Security Implications,” 6.

[56] Jeffrey W Seifert, “A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance,” *Washington DC, USA* 16 (2003). cited in Alshehri, Mohammed, and Steve Drew. “E-Government Fundamentals,” *IADIS International Conference ICT, Society and Human Beings* (2010): 38.

highlighted in his study “Governance of Cybersecurity – The Case of South Africa”, where he noted that the ability to address and investigate cybersecurity breaches, as well as to prosecute individuals, seems a distant prospect. This is due to the necessity of providing training for police officers, prosecutors, and judges.[57] Therefore, it is crucial to consider this issue along with the traditional procedures that are more familiar to the public. This will assist in developing more transparent and accessible processes, while also ensuring the effectiveness of these procedures.

Similarly, Norris et al. reached the conclusion in their study, entitled “Cyberattacks at the Grassroots Level: American Local Governments and the Need for High Levels of Cybersecurity,” that the lack of awareness regarding cybersecurity issues represents a significant challenge that must be addressed. In order to address this challenge, the authors proposed some general recommendations: the establishment and maintenance of a culture of cybersecurity; end-user training; the implementation of cybersecurity best practices; and the elimination of the “lack of knowledge.”[58]

To address these challenges, countries are establishing specialized centers responsible for handling complaints, clarifying jurisdiction, and enhancing tools to respond to cyber threats and crimes. For instance, in the United States, Castro states that to assist victims of cybercrimes, the FBI, the Office for Victim Assistance, and the National White Collar Crime Center collaborated to create the Internet Crime Complaint Center (IC3). This center serves as a single hub for collecting data on internet-related crimes and referring cases to the appropriate authorities.[59]

Likewise, the European Cybercrime Centre (EC3), part of Europol, coordinates efforts to combat cross-border cybercrimes among EU member states and acts as a technical expertise hub in this field. Additionally, Europol provides an online platform for reporting cybercrimes, allowing individuals to submit their reports through designated national websites in their respective countries.[60]

At the national level, there are national cybersecurity agencies. In Germany, the responsibility for cybersecurity issues primarily falls on the German Cybersecurity Agency (BSI), which is part of the Ministry of the Interior. The BSI serves as the central body coordinating national cybersecurity policies and works to protect critical infrastructure and government information systems.

[57] Ewan Sutherland, “Governance of Cybersecurity – The Case of South Africa,” *The African Journal of Information and Communication* no. 20 (2017): 89.

[58] Donald F. Norris et al. “Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity,” *Public Administration Review* 6, no. 79. (2019): 7.

[59] Daniel Castro, “U.S. Federal Cybersecurity Policy” in *Cybersecurity: Public Sector Threats and Responses*, ed. Kim J. Andreasson (Boca Raton, FL: Taylor & Francis, 2011): 134.

[60] Europol. “European Cybercrime Centre (EC3).” Accessed December 20, 2024. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Germany also strives to ensure compliance with European regulations related to cybersecurity, such as the European Cybersecurity Directive (NIS Directive).[61]

6. Conclusion

This paper examined the cybersecurity framework with a focus on the sufficiency of European and German legislation from the perspective of e-government. The European Union's legislation has been instrumental in harmonizing cybersecurity regulations across member states and promoting cooperation among them. However, continued efforts are necessary to address the challenges faced by e-government services. While significant progress has been made, legislative measures remain slow and often fail to keep pace with the rapid technological advancements. The traditional multi-stage legislative processes further hinder timely adaptation, necessitating a comprehensive review of these procedures to ensure they are more agile and responsive to emerging cybersecurity threats.

On the other hand, the German legal framework demonstrated reasonable alignment with evolving cybersecurity threats, covering a wide range of cybercrimes. Nonetheless, a gap was identified due to the absence of specific provisions that increase the consequences for cyberattacks targeting e-government entities. Addressing these shortcomings requires not only the introduction of specific measures but also a shift toward more proactive and flexible legislative mechanisms capable of responding effectively to the dynamic nature of cybersecurity risks.

The research highlighted the crucial role of operators of critical infrastructures in ensuring the resilience of e-government systems. Moreover, the research underlined the complexities arising from the intersection of national and international cybersecurity frameworks. The challenges associated with achieving a unified approach to cybersecurity, particularly in light of the rapid pace of technological advancements, were discussed.

In conclusion, this research contributes to the ongoing discourse on cybersecurity for e-government services. By identifying the strengths and weaknesses of existing legal frameworks, this study offers valuable insights for policymakers and practitioners seeking to enhance the security and resilience of e-government systems. Although this paper represents a contribution to the reduction of the gap in the scholarly literature on e-government cybersecurity, it is evident that further work is required. It would be beneficial to conduct follow-up surveys to gain a deeper understanding of cybersecurity practices and outcomes at the practical level.

[61] Federal Office for Information Security (BSI). “Cybernation,” *Bundesamt für Sicherheit in der Informationstechnik (BSI)*. Accessed December 20, 2024. https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation_node.html.