BRATISLAVA LAW REVIEW

PUBLISHED BY
COMENIUS UNIVERSITY BRATISLAVA
FACULTY OF LAW

p-ISSN 2585-7088
e-ISSN 2644-6359

CYBERSECURITY AND THE SLOVENIAN ELECTRICAL GRID: REGULATION AND POLICY RECOMMENDATIONS

Tal Pavel
Associate Professor
Dunarea de Jos University of Galati
Strada Domnească 47
Galați, Romania
Tal@cybureau.org
ORCID: 0000-0002-4046-0867

Luka Martin Tomažič
Associate Professor
Alma Mater Europaea University
Slovenska ulica 17, 2000
Maribor, Slovenia
luka.tomazic@almamater.si
ORCID: 0000-0002-2296-0489

Abstract: ***This article examines cybersecurity risks to the Slovenian electrical grid, a critical infrastructure asset, amid escalating global threats from state-sponsored actors, geopolitical tensions, and technological vulnerabilities, including ICT interdependencies, legacy systems, IoT devices, and supply chain weaknesses. Adopting an interdisciplinary lens from law, public policy, and cybersecurity, it addresses three research questions: identifying cyber threats, evaluating Slovenia's policy framework and legal regime, and proposing enhancements to resilience. Through normative-dogmatic, dialectical methods and a Xanthakian qualitative assessment of legislative quality, focusing on effectiveness, clarity, precision, and unambiguity, it uncovers gaps such as inconsistent strategic prioritisation, scattered provisions, and reactive approaches. Recommendations include formalising stakeholder cooperation, developing grid-specific strategies, mandating annual cyber stress tests, integrating AI-driven modelling, and refining drafting to ensure unified terminology. The study highlights Slovenia's need for proactive, EU-harmonised measures to bolster energy security amid an evolving cyber landscape.***

Key words: ***Cybersecurity; Electrical Grid; Critical Infrastructure; Slovenia; NIS2 Directive; Legislative Quality***

Suggested citation:
Tal Pavel and Luka Martin Tomažič, 'Cybersecurity and the Slovenian Electrical Grid: Regulation and Policy Recommendation' (2026) 10(1) *Bratislava Law Review* 179 https://doi.org/10.46282/blr.2026.10.1.1178

Submitted: 16 December 2025
Accepted: 19 May 2026
Published: 01 August 2026

1. INTRODUCTION

The United Nations Office for Disaster Risk Reduction (UNDRR) define the term "Critical Infrastructure" as "The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society".[1] The UK National Protective Security Authority (NPSA) define "Critical National Infrastructure (CNI)" as "those critical elements of infrastructure whose loss or compromise could severely impact the delivery of essential services or have a significant impact on national security, national defence, or the functioning of the state."

Therefore, cyberattacks targeting critical infrastructure and the electrical grid pose significant risks to national security, public health and safety, and economic stability in both cyberspace and the real world,[2] and can serve as a weapon in times of conflict, as demonstrated by incidents attributed to state actors targeting European energy infrastructure amid geopolitical tensions, including those linked to the ongoing Russia-

[1] United Nations Office for Disaster Risk Reduction (UNDRR), 'Definition: Critical Infrastructure | UNDRR' (2 February 2017) https://www.undrr.org/terminology/critical-infrastructure accessed 28 January 2026.
[2] Ewa Maria Włodyka and Krzysztof Kaczmarek, 'Cyber Security of Electrical Grids – A Contribution to Research' (2024) 2 *Cybersecurity and Law* 260 https://www.cybersecurityandlaw.com/pdf-188575-109965? accessed 28 January 2026.

Ukraine war.[3] These threats are addressed at the EU level by the NIS2, CER and NCCS triad, which Slovenia has transposed but not yet fully operationalised in the electricity sector.

With the current geopolitical circumstances, including the Russian invasion of Ukraine,[4] conflict in the Middle East,[5] and the emergence of other state-sponsored efforts to target critical infrastructure through cyber-attacks[6] the importance of adequately assessing risks and responding to threats, both preventively and curatively, can hardly be overstated. In this sense, specific circumstances, including Slovenia's NATO membership amid adversarial regimes and its geographical position, make it a potential target for malign foreign actors.

The electrical grid is a crucial component of critical infrastructure, given its importance for economic activity and for ensuring the population's access to adequate living conditions.[7] The proliferation of distributed energy resources, combined with the development of novel AI-driven cyber capabilities, has created additional cyber and physical vulnerabilities across distribution and transmission networks, as well as in production capabilities.[8]

This article focuses on the Slovenian electrical grid from the perspective of optimising legal and policy frameworks to effectively prevent and counter cyber threats. Such an analysis needs to be comprehensive, focusing not only on the narrower legal acts and policies governing the electrical grid but also on broader information and communication-related legislation. The quality of legislation, global best practices, and specific domestic circumstances must be considered when proposing appropriate public policy improvements.[9]

2. LITERATURE REVIEW

The literature review aims to map the existing work on cybersecurity threats to the electrical grid globally and in Slovenia, as well as the local policy and legal measures to mitigate them. It examines how various studies contribute to a broader understanding of cybersecurity in the electrical grid, as well as Slovenia's regulations and policies aimed

[3] Andrew Cottey, 'NATO and the Russia–Ukraine War: Geopolitics, Ideology, and the New Politics of the Alliance' (2025) 25(4) *Defence Studies* 1 https://doi.org/10.1080/14702436.2025.2562982 accessed 27 November 2025.

[4] Ibid.

[5] Seevan Saeed, 'The Crises in the Middle East: Reshaping the Region's Geopolitical Landscape and Altering the Global Order' (2025) 4(1) *Asian Review of Political Economy* 1 https://doi.org/10.1007/s44216-024-00043-3 accessed 27 November 2025.

[6] Ashish Saraswat and Garima Tiwari, 'United Nations and Beyond: Legal Strategies for Defending Critical Energy Infrastructure Against Cyber Attacks' in Mohamed Chawki and Ajith Abraham (eds), *Cybercrime Unveiled: Technologies for Analysing Legal Complexity* (Springer Nature Switzerland 2025) https://doi.org/10.1007/978-3-031-80557-8_13 accessed 27 November 2025.

[7] TA Rajaperumal and C Christopher Columbus, 'Transforming the Electrical Grid: The Role of AI in Advancing Smart, Sustainable, and Secure Energy Systems' (2025) 8(1) *Energy Informatics* 51 https://doi.org/10.1186/s42162-024-00461-w accessed 27 November 2025.

[8] Phylicia Cicilio and others, 'Resilience in an Evolving Electrical Grid' (29 January 2021) https://www.mdpi.com/1996-1073/14/3/694 accessed 27 November 2025.

[9] At this point, we would also like to acknowledge that some of the ideas presented here have been developed in our previous individual publications. This contribution therefore builds upon our earlier research, in particular: Luka Martin Tomažič and Borut Bratina, 'Pravni okvir odzivanja na krizna stanja v slovenskem elektroenergetskem sistemu' [Legal Framework for Responding to Crisis States in the Slovenian Electrical Energy System] (2024) 50(8) *Podjetje in delo* 1417 https://www.podjetjeindelo.si/literatura/PID101D202412V8PS1417PE1417N1/ accessed 08 July 2026.

at mitigating cyber threats to the grid. The scientific literature examined both the cyberattacks on the electrical system and their mitigation.

Mazhar et al. analysed the risks and flaws that can affect the safety of critical, innovative grid network components using modern technologies such as Machine Learning and Blockchain.[10] Maurya et al. analysed cybersecurity attacks on power system networks and their protection schemes, focusing on the vulnerabilities of digital substation relays and their impact on power grid dynamics, particularly communication protocol flaws.[11] Bouramdane examines various types of cyber-attacks and their implications for smart grids.[12]

Various sources emphasise the need for a comprehensive policy to mitigate cyber threats to the electrical grid. Kazancı indicates the inadequacy of cyber personnel in the electricity sector.[13] Abraham et al. advocated integrating cybersecurity frameworks to enhance resilience.[14] Kirvan examines the risks and mitigation strategies in U.S. energy infrastructure,[15] while Sanger outlines the immediate steps needed to address cyber risk.[16] Nguyen et al. emphasise the need for holistic defence strategies to safeguard power grids, focusing on detection techniques, protection plans, and mitigation practices across generation, transmission, and distribution sectors.[17] The article advocates for enhancing grid resilience against cyber adversaries, as even modest improvements can yield significant economic benefits and improve societal welfare. Farooq et al. emphasise the detection and mitigation of cyber-attacks to enhance the stability and security of the electrical grid. Numerous cyber reports analyse the cyber threats to the electrical grid.[18] IronNet analyses past cyber-attacks on the various stages of the energy supply chain, specifically generation, transmission, and distribution.[19] Dragos explores various

[10] Tehseen Mazhar and others, 'Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods' (2023) 15(2) *Future Internet* https://doi.org/10.3390/FI15020083 accessed 28 January 2026.

[11] Arun Kumar Maurya, Pranav Singhaal and Harsh Kumar Pathak, 'Analysis of Cyber Security Attacks on Power System Networks and Its Protection Schemes' [2024] 2024 4th International Conference on Advances in *Electrical, Computing, Communication and Sustainable Technologies, ICAECT 2024* https://doi.org/10.1109/ICAECT60202.2024.10469140 accessed 28 January 2026.

[12] Ayat Allah Bouramdane, 'Cyberattacks in Smart Grids: Challenges and Solving the Multi-Criteria Decision-Making for Cybersecurity Options, Including Ones That Incorporate Artificial Intelligence, Using an Analytical Hierarchy Process' (2023) 3(4) *Journal of Cybersecurity and Privacy* 662 https://doi.org/10.3390/JCP3040031 accessed 28 January 2026.

[13] Baybarshan Ali Kazancı, 'The Strategic Importance of Cyber Security in Electric Energy Policies' (2024) 14(4) *International Journal of Energy Economics and Policy* 599 https://doi.org/10.32479/IJEEP.16244 accessed 28 January 2026.

[14] Doney Abraham and others, 'Consequence Simulation of Cyber Attacks on Key Smart Grid Business Cases' (2024) 12 *Frontiers in Energy Research* 1395954 https://doi.org/10.3389/FENRG.2024.1395954/BIBTEX accessed 28 January 2026.

[15] Paul Kirvan, 'What Resilience Professionals Need to Know: Protecting Critical Infrastructure – the Power Grid' [2023] *Risk and Resilience Hub* https://www.riskandresiliencehub.com/what-resilience-professionals-need-to-know-protecting-critical-infrastructure-the-power-grid/ accessed 28 January 2026.

[16] David E Sanger, 'Russian Hackers Appear to Shift Focus to U.S. Power Grid' [2018] *The New York Times* https://www.nytimes.com/2018/07/27/us/politics/russian-hackers-electric-grid-elections-.html accessed 28 January 2026.

[17] Tien Nguyen and others, 'Electric Power Grid Resilience to Cyber Adversaries: State of the Art' (2020) 8 *IEEE Access* 87592 https://doi.org/10.1109/ACCESS.2020.2993233 accessed 28 January 2026.

[18] Asma Farooq and others, 'Impact of Cyber-Attack on Coordinated Voltage Control in Low Voltage Grids' (2023) 17(11) *IET Renewable Power Generation* 2887 https://doi.org/10.1049/RPG2.12571 accessed 28 January 2026.

[19] IronNet, 'Cyber Attacks on the Power Grid' https://www.ironnet.com/blog/cyber-attacks-on-the-power-grid accessed 28 January 2026.

DOI: 10.46282/blr.2026.10.1.1178

malware and their capabilities, mainly CRASHOVERRIDE, known as "the first-ever malware framework designed and deployed to attack electric grids."[20]

Despite the growing body of work on cyberattacks on the electrical grid worldwide, several gaps remain, including analyses of cyber threats to Slovenia's electrical grid and a lack of emphasis on regulation and policy. The topic of this paper is to examine different angles of the question, namely, (RQ1) What are the cyber threats to the electrical grid? (RQ2) What are Slovenia's policy and legal framework to mitigate cyber attacks on the local electric grid? (RQ3) What are the policy and legal measures Slovenia should implement to improve its resilience to cyber threats to the local electrical grid?

3. METHODOLOGY

This article employs an interdisciplinary methodological approach that integrates perspectives from cybersecurity, law, and public policy to comprehensively analyse the regulatory framework governing the Slovenian electrical grid. The primary data sources include Slovenian legislative acts, legislation, and strategic policy documents, such as the Slovenian policy and Strategy documents, published from 1994 to 2025, as they appear on the Cyber Policy Portal[21] and the Policy Portal of the Government of Slovenia.[22] Academic literature was systematically reviewed to examine global cybersecurity threats to electrical grids, international regulatory approaches, and legislative drafting quality standards. The scope of this research is limited to the Slovenian legal and policy framework as it relates specifically to electrical grid cybersecurity, excluding broader critical infrastructure sectors and detailed technical implementation analysis. The study's limitations include the absence of empirical data on incident response effectiveness, limited access to classified security assessments, and the rapidly evolving nature of cyber threats.

Specifically, with respect to legal science and regulatory aspects, a combination of analytical, logical, dialectical, and normative-dogmatic approaches will be utilised. An analytical approach will be used to identify the relevant aspects of law and policy that are adequate and those that require amendment. In doing so, the logical approach will ensure appropriate reasoning and rigorous argumentation, especially in informal contexts.[23] The authors will employ the dialectical method to consider arguments and counterarguments to individual standpoints, aiming to reach rational conclusions.[24] With a normative-dogmatic approach, they will treat law as a social phenomenon that enables the government to influence the behaviour of legal subjects through legislation and the state's coercive apparatus.[25]

---

[20] DRAGOS, 'CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations' https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf accessed 28 January 2026.

[21] United Nations Institute for Disarmament Research (UNIDIR), 'Slovenia - Cyber Policy Portal' (November 2023) https://cyberpolicyportal.org/states/slovenia accessed 11 November 2025.

[22] Government of the Republic of Slovenia, 'Policies' https://www.gov.si/en/policies/ accessed 12 November 2025.

[23] Jan Woleński, 'Formal and Informal in Legal Logic' in Dov M Gabbay, Patrick Canivez, Shahid Rahman and Alexandre Thiercelin (eds), *Approaches to Legal Rationality* (Logic, Epistemology, and the Unity of Science vol 20, Springer 2010) 73 https://doi.org/10.1007/978-90-481-9588-6_4 accessed 27 November 2025.

[24] Bart Verheij, 'Dialectical Argumentation with Argumentation Schemes: An Approach to Legal Logic' (2003) 11(2-3) *Artificial Intelligence and Law* 167 https://doi.org/10.1023/B:ARTI.0000046008.49443.36 accessed 27 November 2025.

[25] Aleksei Dolzhikov, 'THE CONSTITUTIONAL PRINCIPLE OF PROPORTIONALITY: A LEGAL-DOGMATIC METHOD' [2021] *Вестник Пермского университета. Юридические науки* 540 https://doi.org/10.17072/1995-4190-2021-53-540-561 accessed 28 January 2026.

4. CYBER RISKS TO THE ELECTRICAL GRID

The electrical grid is critical infrastructure and a basic human resource on which most human activities, including the most critical ones, depend, either directly or indirectly. Its increasing reliance on digital control systems and networked technologies exposes it to a range of cyber threats, which could disrupt electricity supply, damage equipment, and compromise the safety and security of millions. Among those risks are:

High reliance on information and communication technologies means that electrical and smart grids employ advanced communication systems that are vulnerable to cyberattacks, potentially resulting in privacy breaches and system failures.[26] For example:

The electrical grid comprises interconnected ICT elements that operate independently, thereby increasing its vulnerability to cyberattacks. Hence, IT security for electricity grids is increasingly crucial.[27] In addition, the growth of networks and communication protocols within Industrial Control Systems (ICS) introduces persistent vulnerabilities that threat actors will exploit. Adopting interoperable technologies for smart grid development further broadens the cyber-attack landscape.[28]

Legacy systems in the energy sector, often outdated due to organisational constraints, pose significant security risks due to limited monitoring capabilities.[29] Grid systems are usually managed and monitored remotely. However, attackers may exploit vulnerabilities in these connections to gain access and rely on a complex supply chain of outsourced hardware and software components. Weak security practices by third-party vendors or compromised software updates can expose these systems to attacks. Furthermore, the Internet of Things (IoT) poses novel security challenges, including the potential to manipulate power demand via IoT devices, which may cause blackouts and fluctuations in power flow.[30]

A cyber-attack on the electrical grid can disrupt essential services, leading to system instability and blackouts. Such attacks can induce significant disturbances, including voltage fluctuations and inverter failures, thereby threatening overall grid stability and potentially causing extensive blackouts. These events could jeopardise hospitals, emergency services, and communication networks. The compromise of critical infrastructure may afford adversaries a substantial strategic advantage in diplomatic or military negotiations. As a result, State-sponsored Advanced Persistent Threats (APTs) frequently target critical infrastructure to achieve strategic objectives during conflicts.

Disruptions in telecommunications infrastructure may hinder national defence activities and emergency response coordination. Interference with communication

[26] Bishowjit Paul and others, 'Potential Smart Grid Vulnerabilities to Cyber Attacks: Current Threats and Existing Mitigation Strategies' (2024) 10(19) *Heliyon* e37980 https://doi.org/10.1016/J.HELIYON.2024.E37980 accessed 28 January 2026.

[27] Abasse Kpegouni, Eyouleki Tcheyi Gnadi Palanga and Adekunle Akim Salami, 'Electricity Grids Facing Cyber Threats: What Approaches for Electricity Companies?' [2022] *International Conference on High Technology for Sustainable Development, HiTech 2022 - Proceedings* https://doi.org/10.1109/HITECH56937.2022.10145560 accessed 28 January 2026; Włodyka and Kaczmarek (n 2).

[28] Idaho National Laboratory Mission Support Center, 'Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector' (2016) https://www.energy.gov/policy/articles/cyber-threat-and-vulnerability-analysis-us-electric-sector accessed 28 January 2026.

[29] Kehinde Ayano, 'Cybersecurity In Critical Infrastructure: Protecting Power Grids and Smart Grids' [2024] *Cyber Defense Magazine* https://www.cyberdefensemagazine.com/cybersecurity-in-critical-infrastructure-protecting-power-grids-and-smart-grids/ accessed 28 January 2026.

[30] Suman Maiti and Soumyajit Dey, 'Smart Grid Security: A Verified Deep Reinforcement Learning Framework to Counter Cyber-Physical Attacks' https://arxiv.org/abs/2409.15757v1 accessed 28 January 2026.

DOI: 10.46282/blr.2026.10.1.1178

networks or transportation systems can obstruct military mobilisation and operational coordination during periods of conflict.[31]

Cyber-attacks can lead to economic instability by causing significant financial damage to critical infrastructure. These damages may include expenses for repairs, data recovery, enhanced security measures, and theft prevention. Over time, such attacks can shake investor confidence, disrupt supply chains, and lower productivity. This can result in higher insurance costs, job losses, and, in extreme cases, loss of life.

Furthermore, cyberattacks that interrupt essential services may exert a considerable psychological influence on the populace. Extended service disruptions or data breaches can diminish public trust in governmental institutions. Moreover, social unrest could emerge if vital services, such as water or healthcare, remain inaccessible for extended durations.

Utilities frequently lack a comprehensive understanding of their cybersecurity posture due to limited staffing and resources. This deficiency impairs their ability to identify cyber assets, understand system architectures, and perform critical cybersecurity assessments, monitoring, and upgrades. Such limitations may, for instance, contribute to inappropriate regulation within the United States. The multitude of regulatory standards and guidelines governing cybersecurity in utilities results in inconsistent adoption practices. Consequently, this leads to overlap and confusion between federal and state jurisdictions, prompting utilities to adopt diverse compliance approaches and complicating the evaluation of industry-wide best practices.[32]

Across the years, cyber-attacks have hit the electrical grids, causing blackouts and damage worldwide:

A cyberattack on Ukrainian power companies caused outages at three regional electric distribution companies on 23 December 2015, affecting approximately 225,000 customers. The U.S. Government indicated that the attack was synchronised and coordinated, likely following extensive network reconnaissance. It attributed the attack to Russian nation-state cyber actors and assessed it as part of a broader cyber campaign against Ukraine's critical infrastructure.[33] A year later, the CRASHOVERRIDE malware targeted a single transmission-level substation in Ukraine, impacting electric grid operations. While the attack demonstrated proof-of-concept capabilities rather than the malware's full potential, its significance lies in the evolution of attack methods.[34]

Phishing emails, sent by known cyber threat actors likely affiliated with the North Korean government, targeted U.S. electric companies on 22 September 2017. The activity was early-stage reconnaissance, not an immediate indication of a disruptive cyber-attack; such attacks can take months to develop if undetected.[35] In July 2018, state-sponsored

[31] Vetrivel Subramaniam Rajkumar and others, 'Cyber Attacks on Power System Automation and Protection and Impact Analysis' (2020) *2020-October IEEE PES Innovative Smart Grid Technologies Conference Europe* 247 https://doi.org/10.1109/ISGT-EUROPE47291.2020.9248840 accessed 28 January 2026.

[32] Government Information Security Office of the Republic of Slovenia, 'Protecting Critical Infrastructure against Cyber Threats' (2022) https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Dogodki/Protecting-critical-infrastructure-against-cyber-threats.pdf#page=8.06 accessed 28 January 2026; Mission Support Center (n 28).

[33] Cybersecurity & Infrastructure Security Agency (CISA), 'Cyber-Attack Against Ukrainian Critical Infrastructure' https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 accessed 28 January 2026.

[34] Dragos, 'CHRYSENE Threat Group' https://www.dragos.com/threat/chrysene/ accessed 28 January 2026; Luis Salazar and others, 'A Tale of Two Industroyers: It Was the Season of Darkness' [2024] *2024 IEEE Symposium on Security and Privacy* (SP) 312 https://doi.org/10.1109/SP54263.2024.00162 accessed 28 January 2026.

[35] FireEye, 'North Korean Actors Spear Phish U.S. Electric Companies' https://web.archive.org/web/20171012004812/https://www.fireeye.com/blog/threat-research/2017/10/north-korean-actors-spear-phish-us-electric-companies.html accessed 28 January 2026.

Russian hackers infiltrated the control rooms of U.S. power utilities through their corporate networks using conventional tactics, such as spear-phishing emails.[36]

Venezuela suffered from several cyberattacks on the local energy sector in March[37] and July 2019,[38] and again in August 2024,[39] plunging the country into darkness.

The RedEcho group, linked to China, conducted a targeted cyber campaign against India's critical infrastructure in mid-2020, specifically the power sector and seaports, targeting 10 Indian power organisations. This activity increased amid heightened tensions along the India-China border.[40]

5. SLOVENIAN POLICY AND LEGAL MITIGATION TO CYBER THREATS TO THE ELECTRICAL GRID

5.1 Slovenian Civilian, Cyber and Military National Strategy

To evaluate the official Slovenian strategy for mitigating cyber threats to the local electrical grid, the study analyses eight civilian, military, and cyber policy papers published by the government of Slovenia between 1994 and 2025 to identify references to the term "Electrical Grid".

Name	Publisher	"Electrical Grid"
Defense Act (ZObr)	Government of the Republic of Slovenia[41]	-
Act on the Slovenian Intelligence and Security Agency (ZSOVA)	Government of the Republic of Slovenia[42]	-

[36] Don C Smith, 'Enhancing Cybersecurity in the Energy Sector: A Critical Priority' (2018) 36(4) *Journal of Energy & Natural Resources Law* 373 https://doi.org/10.1080/02646811.2018.1516362 accessed 28 January 2026.
[37] Sasha Ingber, 'Blackout In Venezuela Leaves Its Leaders Casting Blame In The Dark' [2019] *NPR* https://www.npr.org/2019/03/08/701448955/blackout-in-venezuela-leaves-its-leaders-casting-blame-in-the-dark accessed 28 January 2026.
[38] BBC, 'Venezuela Blackout: Power Cuts Plunge Country into Darkness' https://www.bbc.com/news/world-latin-america-49079175 accessed 28 January 2026.
[39] Reuters, 'Power Beginning to Return in Venezuela after Nationwide Blackout' https://www.reuters.com/business/energy/venezuelas-capital-caracas-other-regions-face-power-outage-2024-08-30/ accessed 28 January 2026.
[40] Recorded Future, 'Continued Targeting of Indian Power Grid Assets by Chinese State-Sponsored Activity Group' (2022) https://go.recordedfuture.com/hubfs/reports/ta-2022-0406.pdf accessed 28 January 2026.
[41] Government of the Republic of Slovenia, 'Defence Act (ZObr) (PISRS)' (20 December 1994) https://pisrs.si/pregledPredpisa?id=ZAKO532 accessed 12 November 2025.
[42] Government of the Republic of Slovenia, 'Act on the Slovenian Intelligence and Security Agency (ZSOVA) (PISRS)' (7 April 1999) https://pisrs.si/pregledPredpisa?id=ZAKO1884 accessed 12 November 2025.

DOI: 10.46282/blr.2026.10.1.1178

Cyber Security Strategy	Government of the Republic of Slovenia[43]	"Cooperation of stakeholders in cyber security assurance is not formally regulated, however, response centres cooperate informally, unless there is a legal basis for it … Thus, such cooperation has already been established with some banks, telecommunication providers and electricity distributors". (p. 5) "The cyber security assurance system will also include other stakeholders. Operators of critical infrastructure in the private and public sectors are important, particularly in the energy supply sector(electricity producers and distributors), and in information and communication support (telecom operators, information society service providers, etc.)." (p. 9)
Digital Slovenia 2020 - Development Strategy for the Information Society until 2020	Government of the Republic of Slovenia[44]	"Stakeholders in cyber security assurance, rather than being formally regulated, participate on an informal basis mainly between response centres, unless there is a legal basis for it … Thus, such cooperation has already been established with some banks, telecommunication providers and electricity distributors" (p. 81)
Defence White Paper of the Republic of Slovenia 2020	Ministry of Defence[45]	-
Resolution on the National Security Strategy of the Republic of Slovenia (ReSNV-2)	Ministry of Defence[46]	-
Digital Slovenia 2030	Government of the Republic of Slovenia[47]	-

[43] Government of the Republic of Slovenia, 'Cyber Security Strategy: Establishing a System to Ensure a High Level of Cyber Security' (2016) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Slovenia_2016_Cyber_Security_Strategy.pdf accessed 28 January 2026.

[44] Government of the Republic of Slovenia, 'Digital Slovenia 2020 - Development Strategy for the Information Society until 2020' (2016) https://www.gov.si/assets/ministrstva/MDP/DID/Digital-Slovenia-2020-Development-Strategy-for-the-Information-Society-until-2020.pdf accessed 28 January 2026.

[45] Ministry of Defence, 'Defence White Paper of the Republic of Slovenia 2020' (2020) https://www.gov.si/assets/ministrstva/MO/Dokumenti/WP2020.pdf accessed 28 January 2026.

[46] Ministry of Defence, 'Resolution on the National Security Strategy of the Republic of Slovenia (ReSNV-2)' (2020) https://www.gov.si/assets/ministrstva/MO/Dokumenti/ReSNV2.pdf accessed 28 January 2026.

[47] Government of the Republic of Slovenia, 'Digital Slovenia 2030 – An Overarching Strategy for Slovenia's Digital Transformation by 2030' (2023) https://www.gov.si/assets/ministrstva/MDP/Digital_Slovenia_2030.docx accessed 28 January 2026.

Decree on the establishment, tasks and organization of the Information Security Office of the Government of the Republic of Slovenia	Government of the Republic of Slovenia[48]	-

Table 1 – The reference to Cybersecurity of Electrical Grids in the Slovenian Civilian, Cyber and Military National Strategy

The various Slovenian policy papers from 1994 to 2025 demonstrate an overarching awareness of the need to protect the local electrical grid from cyber threats. This is notably reflected by the acknowledgement that "such cooperation has already been established with some banks, telecommunication providers and electricity distributors." However, this recognition is neither consistently nor explicitly embedded across the entire corpus of policy documents. First, most policy papers from this period lack a direct mention or a detailed policy outline for protecting the local electrical grid against cyber threats. Specifically, aside from a single recurring reference, the subject receives no focused strategic treatment. Second, the only explicit and repeated reference to cooperation with electricity distributors, alongside other key sectors, appears in only two policy documents published in 2016: the "Cyber Security Strategy" and the "Digital Slovenia 2020" development strategy. Both documents underscore informal cooperation mechanisms between response centres and critical infrastructure operators, including electricity distributors, yet do not formalise these relationships in a legally binding or systematically structured manner. Third, no comparable references or strategic commitments regarding electrical grid cybersecurity are found in earlier policy documents before 2016, nor in subsequent documents published between 2020 and 2025, including national defence or cybersecurity strategy updates. This absence indicates a concerning lack of continuity and sustained prioritisation of the electrical grid's cyber protection in Slovenia's national cybersecurity policy landscape.

This pattern highlights a fragmented and somewhat inconsistent policy approach: initial recognition and informal cooperative steps emerged around 2016, but these efforts were neither preceded nor followed by similarly explicit concerns or formalised strategic commitments in official policy papers. Consequently, despite broad awareness of cyber risks to critical infrastructure, Slovenian policy lacks a continuous, clear, and direct articulation of the electrical grid's cybersecurity needs from 1994 to 2025. This gap highlights the need for greater strategic focus, formal cooperation frameworks, and sector-specific cybersecurity policies consistently emphasised across all relevant official documents to comprehensively and sustainably address evolving cyber threats.

5.2 Slovenian Legal Framework

Slovenian legal framework for cybersecurity in electrical grids encompasses specific legislation in the electrical energy sector, as well as national security legislation

[48] Government of the Republic of Slovenia, 'Decree on the Establishment, Tasks and Organization of the Information Security Office of the Government of the Republic of Slovenia' (2025) https://pisrs.si/pregledPredpisa?id=ODLO3026 accessed 28 January 2026.

DOI: 10.46282/blr.2026.10.1.1178

to address cyber threats. This normative framework requires a state-of-the-art legislative quality assessment to determine its merit and utility.

The legislative solutions in the Information Security Act (ZInfV-1), the primary legislative framework in cybersecurity, are aligned with the NIS2 Directive, which was fully transposed at the national level in 2025 through amendments to the prior ZInfV.[49] Other relevant legislative acts for the cybersecurity of the Slovenian electrical grid include the Act on Critical Infrastructure, the Electricity Supply Act, the Electronic Communications Act, and the Criminal Code. Most requirements derive from general legislation, with relatively little deferred legislative action. At the same time, energy-sector-specific legislation also regulates cybersecurity for smart metering and user data, outlining responsibility for ensuring the electrical grid's cybersecurity.

The Slovenian legal framework on cybersecurity operates within the broader European Union framework, comprising three instruments that regulate the field. These are the NIS2 Directive (EU) 2022/2555, which deals with cyber risk management and incident reporting, the CER Directive (EU) 2022/2557, which regulates resilience of critical entities, including the energy sector and (specifically for the energy sector) the Network Code on Cybersecurity (NCCS - Commission Delegated Regulation (EU) 2024/1366). NIS2 and CER were both transposed into the Slovenian national legal system in 2025 through the adoption of ZInfV-1. Slovenia went beyond the minimal requirements of transposition and adopted stricter national measures for NIS2 and CER (per NIS2 Art. 1(2) and CER Art. 1(2)). NCCS is directly applicable as a regulation.

The main NIS2 obligations relevant to grid cybersecurity are measures covering supply chain security (Article 21 NIS2), incident reporting with successive stages (Article 23 NIS2), and the definition of essential entities in Annex 1, which designates the energy sector as highly critical. As a member state, Slovenia has the primary obligation under CER to identify critical entities (this will take effect only by July 2026). Per Articles 11 to 15, resilience plans need to be put in place, including cyber scenarios, and all-hazards risk assessments need to be performed. This is partly implemented by ZKI-1, which prescribes individual resilience plans.

While NCCS is directly applicable and imposes specific rules for the electricity sector, namely cybersecurity controls (Article 28) and a cyber-attack classification matrix (Article 37), the Slovenian legal system, in this regard, assigns responsibility for cybersecurity to transmission operators only via special legislation in ZOEE (Article 45). At the same time, other relevant entities, such as distribution and generation, are covered only indirectly via ZInfV-1.

The Act on Critical Infrastructure (ZKI-1) clearly designates the Slovenian energy sector as critical infrastructure in Article 7. Thus, in addition to sectoral legislation, the principles of resilience and those transposed from European Union law must be respected.[50] According to Article 2 of the ZKI-1, such protection includes safeguarding infrastructure, designating critical subjects, adhering to the principles of harm prevention and continuous operation, and maintaining data protection standards. While Slovenia's Resilience and Recovery Plan has been relatively underdeveloped in the past [51]. This has

[49] Niels Vandezande, 'Cybersecurity in the EU: How the Nis2-Directive Stacks Up Against Its Predecessor' (Social Science Research Network, 9 March 2023) https://doi.org/10.2139/ssrn.4383118 accessed 27 November 2025.

[50] Ajda Fošner and others, 'Risk Analysis of Critical Infrastructure with the MOSAR Method' (2024) 10(4) *Heliyon* e26439 https://doi.org/10.1016/j.heliyon.2024.e26439 accessed 27 November 2025.

[51] Polona Domadenik Muren and Valentina Franca, 'National Recovery and Resilience Plan: Slovenia' (2022) 15(1S) I*talian Labour Law e-Journal* https://doi.org/10.6092/issn.1561-8048/15691 accessed 27 November 2025.

been mitigated by implementing NIS2 via ZInfV-1. Under Articles 13, 14, and 15 of ZKI-1, each designated critical subject must be considered in developing the national resilience plan. These individual plans should include risk assessments and resilience measures to ensure effective management. In the electricity sector, pursuant to Article 5, paragraph 1 of the Electricity Supply Act (ZOEE), this includes entities involved in electricity generation, supply, trading, storage, aggregation, system operation, market operation, and distribution.

With respect to cybersecurity, the Information Security Act (ZInfV-1) governs information security. It prescribes measures to achieve a high level of protection for networks (including electricity grids) and information systems in the Republic of Slovenia. It limits itself to those networks and systems essential to the state's smooth functioning across all security situations and to the preservation of key social and economic activities in Slovenia.[52] ZInfV-1, Article 1, establishes the security and incident reporting requirements. This includes safeguarding information essential to the state's smooth functioning, as well as legal provisions governing chain risks and penalties.

Article 5 of ZInfV-1 provides definitions that clarify the concepts of cyber threats, cybersecurity, cyber defence, and cyberattacks within the Slovenian legal system. Knowledge of these particular definitions is crucial for understanding Slovenia's approach to cybersecurity and cyber defence.

Thus, a cyber threat is any potential circumstance, event, or action that could damage, disrupt, or otherwise adversely affect networks, information systems, their users, and other individuals. Cyber hygiene is a set of practices for maintaining security and protecting information in digital environments, encompassing measures and procedures to safeguard computer systems, networks, and data against security threats. A large-scale cyber incident disrupts beyond the Republic of Slovenia's capacity to respond, or significantly affects at least two Member States of the European Union. Cyber defence encompasses the measures, activities, and capabilities of state bodies, local self-government bodies, economic companies, institutes, and other organisations, as well as citizens, necessary to protect and safeguard cyberspace against cyber threats and incidents. Cyberspace is the global information environment, comprising information systems and networks, data, digital devices, and their users. Cybersecurity encompasses the activities necessary for protecting network and information systems, their users, and other individuals affected by cyber threats. Note that a cyber-attack is not explicitly defined as a separate term in this article, which is a move away from the legal framework under ZInfV.[53]

Based on the above definitions, a normative framework has been developed that encompasses the government's designation of essential entities and the measures for managing cybersecurity. According to Articles 29 and 30 of ZInfV-1, each significant incident must be reported to the Slovenian Computer Emergency Response Team (SI-CERT) within 24 hours. A full notification must follow within 72 hours, and a final report must be prepared within one month. Under the general criteria outlined in Article 36 of ZInfV-1, the response team classifies each incident into levels C1 to C6, ranging from

[52] Laris Gaiser, 'Slovenia: A Fragmented Cyber Security' *Routledge Companion to Global Cyber-Security Strategy* (Routledge 2021).

[53] Andrej Abramov, 'Cybersecurity in the Republic of Slovenia - One Can Never Be Too Careful' (2024) 79 *Pravnik: Revija za Pravno Teorijo in Prakso* 471 https://heinonline.org/HOL/Page?handle=hein.journals/pravnik79&id=471&div=&collection= accessed 28 January 2026.

DOI: 10.46282/blr.2026.10.1.1178

critical, with widespread adverse effects across multiple sectors (C1), to no detectable negative impact (C6).

A state of heightened threat may be declared upon detection of critical incidents, prompting immediate notification to the National Security Council (SNAV) and, if warranted, a government declaration of a state of crisis (Article 12 of ZInfV-1). The public may be notified if the assessment indicates it is required. In such cases, the national competent authority is tasked with preparing public communication, in collaboration with the government service for public communication, which relevant media outlets must publish unchanged (Article 12, paragraph 7 of ZInfV-1).

When cyber defence is activated in response to specific threats, it takes place in accordance with the national response plan for cyber incidents, large-scale incidents, and crises (Article 12 of ZInfV-1), as well as in alignment with procedures for incident management and cooperation protocols defined in the plan that the government is tasked with adopting.

Several stakeholders, including the competent national authority for information security and the national Computer Security Incident Response Team (SI-CERT, as part of CSIRT groups per Articles 13 and 15), with the participation of the Ministry of Defense, the Ministry for Digital Transformation, the Police, the Slovenian Intelligence and Security Agency (SOVA, as the central body for hybrid threats), and other national bodies such as sector regulators and critical infrastructure operators, are each tasked with acting within their respective competencies to ensure national security (Articles 10, 12, 13, and 15 of ZInfV-1). Article 10 details the national authority's tasks, including coordinating the national information security system and developing cyber defence capabilities. Articles 13 and 15 set out the roles of CSIRTs in monitoring threats, providing guidance, cooperating internationally, and securing information exchange.

The solutions from ZKI-1 are reflected in sectoral *lex specialis* legislation. In addition to the Electricity Supply Act (ZOEE), the Electronic Communications Act (ZEKom-2) is particularly relevant, given the role of smart metering and the importance of information systems to the grid's overall functioning.

Article 45 of ZOEE assigns responsibility for cybersecurity to the system operator of transmission networks. Although no similar responsibility is found in the provisions of ZOEE for distribution operators and other relevant entities, it nevertheless stems from the general rules of appropriate conduct for professional entities, as outlined in Article 6, paragraph 2, of the Obligation Code (OZ), and from the principle of analogy.[54] Nevertheless, it is somewhat suboptimal that the existence of such responsibility must be inferred from systemic and teleological interpretations.[55]

Specific requirements, however, are given for the security of advanced meters. Data communication on advanced meters, as well as the privacy and security of personal data, must comply with European Union cybersecurity legislation and the General Data Protection Regulation (GDPR). Per Article 29 ZOEE, this must be done using the best

[54] Fabrizio Macagno and Douglas Walton, 'Argument from Analogy in Law, the Classical Tradition, and Recent Theories' (2009) 42(2) *Philosophy & Rhetoric* 154 https://doi.org/10.2307/25655348 accessed 28 November 2025.

[55] Helen Xanthaki, 'Legislative Reform in the EU – The Role of Drafting in Legislative Quality' (Social Science Research Network, 18 January 2024) https://papers.ssrn.com/abstract=4695537 accessed 28 November 2025.

available techniques, while taking into account costs and the principle of proportionality. This is appropriate and in line with the state of the art in legal doctrine.[56]

In paragraphs 26 and 27 of Article 3, ZEKom-2 defers to the relevant provisions of ZInfV-1. The phrasing is designed to accommodate potential changes in information security law. In Articles 120 and 121, ZEKom-2 outlines procedures for security incidents and cyberattacks involving transmission and distribution grid operators. It focuses on the role of the information security authority and its cooperation with the agency and the national CSIRT. The law stipulates that critical incidents and cyberattacks must be reported immediately to the government and the Slovenian National Security Office, and that the information security authority may require operators to implement measures to prevent or mitigate such incidents. It also governs procedures in the event of a heightened threat, when there is a high probability of serious incidents and ongoing or anticipated cyberattacks.

From the perspectives of legislative quality and drafting, ZEKom-2 and ZInfV-1 employ somewhat different wording in the provisions governing the evaluation of cybersecurity incidents and the applicable measures. Although the provisions appear, in essence, very similar, unnecessary differences in lexical descriptors may create legal uncertainty in borderline cases.[57] This can be further complicated because it is not entirely clear which of the two legal acts should be preferred under the *lex specialis* principle.[58]

A general comment relevant to the systematisation of provisions in the Slovenian legal framework is that they are unnecessarily scattered across numerous general legal acts.[59] A general cybersecurity law would suffice, with relevant provisions broad enough to be incorporated into sectoral legislation, namely the ZOEE. With ZInfV-1, the legislator had a good opportunity to address this, but limited their activities to transposing EU-level legislation.

The Slovenian legal framework, thus, although improved with ZInfV-1, still leaves much to be desired in terms of systematisation and legislative clarity.[60] This is ameliorated by the government's strategy, which is much more transparent and straightforward. It is to be understood as secondary legislation, given that a specific legal authorisation exists and specifies the rights and obligations under the ZInfV-1 and other relevant legal acts on cybersecurity in Slovenia.

The Slovenian Cybersecurity Strategy thus identifies key risks, including increasingly sophisticated malware and ransomware attacks, the exploitation of vulnerabilities in interconnected systems, and the rising prevalence of social engineering tactics such as phishing, all of which are compounded by the potential for state-

[56] Luka Martin Tomažič, 'Best Available Techniques Principle: International Treaties and Drafting in National Legislation' (2022) 14(2) *LeXonomica* 153 https://doi.org/10.18690/lexonomica.14.2.153-172.2022 accessed 28 November 2025.
[57] Michał Araszkiewicz and Monika Florczak-Wątor, 'AI and the Principles of Proper Legislation: Enhancing Quality, Understandability, and Consistency in Legal Texts' (2025) 13(3) *The Theory and Practice of Legislation* 353 https://doi.org/10.1080/20508840.2025.2559165 accessed 28 November 2025.
[58] Silvia Zorzetto, 'The Principle Lex Specialis: A Critical Explanation' (2024) 46 *Revista de Derecho Privado* 15 https://heinonline.org/HOL/Page?handle=hein.journals/revdpriv46&id=10&div=&collection= accessed 28 January 2026.
[59] Gaiser (n 52).
[60] Tímea Drinóczi and Ronan Cormacain, 'Introduction: Illiberal Tendencies in Law-Making' (2022) 9(3) *The Theory and Practice of Legislation* 269 https://doi.org/10.1080/20508840.2021.1955483 accessed 28 November 2025.

sponsored cyber espionage and attacks.[61] It includes definitions of stakeholders and the areas of strategy implementation, with a focus on prevention, response, and awareness-raising.

Strategic cybersecurity goals for electrical grids are not sector-specific. Still, they are set out in general terms in the Slovenian Cybersecurity Strategy: safeguarding citizens in cyberspace, protecting the economy from cyber threats, and ensuring the functionality of critical information and communication infrastructure. Furthermore, securing public safety, combating cybercrime, developing national cyber defence capabilities, and maintaining the availability of critical systems, such as electrical grids, are key priorities during emergencies.

While the Slovenian legislative framework appears somewhat lacking in detail on sector-specific cybersecurity and cyber threat response, there are relevant provisions at the secondary legislative level. The problems with provisions lacking a sufficient basis in primary legislation, as required by the principle of legality,[62] have been mitigated by the adoption of ZInfV-1. Article 3 of the Act on the rules for monitoring the quality of electricity supply explicitly includes terrorist attacks but only implicitly includes cyberattacks under the general clause on outside causes of electricity supply disturbances. These enable system operators to perform grid manipulations to ensure supply stability, in accordance with system operating instructions, for distribution and transmission networks, thereby maintaining the supply of electrical energy.

Finally, the Slovenian Criminal Code (KZ-1) reinforces the legal framework by criminalising acts of terrorism and attacks on information systems.[63] This provides a crucial layer of general and specific deterrence against cyberattacks targeting the electrical grid. This inclusion highlights the state's acknowledgement that cybersecurity threats may constitute criminal offences.

6. DISCUSSION

This study examined three interconnected research questions concerning cybersecurity threats to Slovenia's electrical grid and the adequacy of its regulatory framework in addressing these challenges.

The findings reveal that electrical grids face multifaceted cyber threats stemming from their increasing digitalisation and interconnectedness. The primary vulnerabilities identified include high interdependence with information and communication technologies, particularly through Industrial Control Systems (ICS) networks; legacy systems that lack modern security updates; and remote access points that enable malicious actors to gain entry. The proliferation of IoT devices and distributed energy resources has significantly expanded the attack surface, while supply chain vulnerabilities introduce risks through third-party hardware and software components.

[61] Darko Galinec, Darko Možnik and Boris Guberina, 'Cybersecurity and Cyber Defence: National Level Strategic Approach' (2017) 58(3) *Automatika* 273 https://doi.org/10.1080/00051144.2017.1407022 accessed 28 January 2026.

[62] Matic Zavodnik, 'Pomen Načela Zakonitosti v Povezavi z Drugimi Ustavnimi Načeli: Analiza Odločbe Ustavnega Sodišča: UI-155/20–24.' [The Meaning of the Principle of Legality in Connection with Other Constitutional Principles: An Analysis of the Constitutional Court Decision UI-155/20-24] (2025) 103 *Dignitas* 199.

[63] Damjan Korošec, Katja Filipčič and Helena Devetak, 'Veliki Komentar Posebnega Dela Kazenskega Zakonika KZ-1' (Veliki komentar posebnega dela kazenskega zakonika KZ-1 | Uradni list, 2023) [The Large Scientific Commentary on the Special Part of the Criminal Code (KZ-1)] https://www.uradni-list.si/knjigarna/knjiga/veliki-znanstveni-komentar-posebnega-dela-kazenskega-zakonika-kz-1-1 accessed 28 November 2025.

These technical vulnerabilities give rise to four categories of consequences. First, cyberattacks can cause system instability and cascading failures, potentially leading to widespread blackouts affecting critical services. Second, they pose risks of economic instability through direct costs of system repairs and indirect impacts on productivity and investor confidence. Third, state-sponsored Advanced Persistent Threats (APTs) targeting electrical infrastructure can confer a strategic advantage on adversaries during geopolitical conflicts. Fourth, successful attacks have a profound psychological and social impact, undermining public confidence in government institutions and essential services.

Analysis of eight Slovenian policy documents published between 1994 and 2025 reveals significant gaps in strategic focus. Only two papers from 2016, the Cyber Security Strategy and Digital Slovenia 2020, explicitly reference efforts to protect the electrical grid from cyber threats, noting informal cooperation with electricity distributors. Subsequent policy papers from 2020 to 2025, including the Defence and National Security Strategy, contain no specific references to electrical grid cybersecurity, suggesting a concerning lack of sustained strategic attention despite initial awareness.

To minimise the policy gap relating to mitigating cyber threats to the local electrical grid, Slovenia should (1) reinstate and strengthen electrical grid cybersecurity as an explicit strategic priority in all relevant policy documents, moving beyond general critical infrastructure language to sector-specific commitments; (2) formalise cooperation mechanisms between government agencies and electrical sector operators, replacing the informal arrangements noted in 2016 with structured frameworks including regular joint exercises, threat intelligence sharing protocols, and coordinated incident response procedures; (3) develop a dedicated electrical grid cybersecurity strategy as a subsidiary document to the national cybersecurity strategy, with concrete implementation timelines, responsibility assignments, and measurable objectives; and (4) establish regular strategic review cycles to ensure electrical grid cybersecurity remains prominently addressed in policy documents, preventing the erosion of attention observed between 2016 and 2025.

The regulatory and policy framework governing the cybersecurity of the Slovenian electrical grid requires further analysis, in accordance with state-of-the-art legislative and drafting approaches, to ascertain the perceived quality of the solutions. To achieve this, a simplified Xanthakian qualitative test will be employed, focusing on the combination of effectiveness and precision, clarity and unambiguity of solutions and the legislative text. Gender neutrality and plain language, which are a part of Xanthaki's broader test, will be omitted in terms of this analysis because they are arguably less relevant to the problem of ensuring appropriate cybersecurity of the electrical grid.

Within the Xanthakian Framework, effectiveness is connected to the extent to which legislation's primary objectives (so-called *telos*) are achieved.[64] The core objectives of cybersecurity legislation for the electric grid are to prevent, detect, and respond to cyber threats, thereby ensuring the resilience of the distribution and transmission grids (see ZKI-1, Article 2 and ZInfV-1, Article 1).

The Slovenian policy framework demonstrates moderate effectiveness in response and deterrence, with preventive measures still receiving insufficient attention in both regulatory and practical terms. Relevant reactive mechanisms include incident reporting and CSIRT coordination; however, gaps in prevention undermine proactive resilience. Supply chain risks are not adequately addressed, and the framework lacks

[64] Xanthaki (n 55).

DOI: 10.46282/blr.2026.10.1.1178

enforceable upgrade timelines and vendor-auditing procedures. Resilience plans partially and indirectly mitigate the economic and mass-psychological impact of outages, but implementation remains ad hoc. The Slovenian regulatory and policy framework aligns well with European Union requirements. Still, it falls short in practice and evidence-based enforcement, with no mandated routine grid simulations to test against different cyber-attack scenarios. Regarding clarity, precision, and unambiguity, it is necessary first to recognise that these are three related but distinct concepts. Clarity is the quality of being easily perceived and understood, so that the message received is the same as the intent of the legislator. Precision relates to the appropriate level of semantic inclusion in the text, avoiding overly broad or overly narrow definitions. Ambiguity refers to the possibility of multiple meanings at the level of a word, phrase, sentence, or paragraph. All three need to be analysed to ascertain potential issues of clarity, excessive ambiguity, or imprecise formulations that could adversely affect legislative quality. Such analysis is by its nature argumentative and qualitative.

Clarity is diminished, *inter alia*, by the use of different wording for the same concepts, as evidenced by the incongruence between ZEKom-2 and ZInfV-1 regarding key descriptors of cybersecurity incidents. Furthermore, because the provisions are not consolidated in a single act but are scattered across several general legal acts, this hinders clarity of the legislator's intent and impedes straightforward application of the law, especially in complex cases, where a swift response based on clear legal rules is of utmost importance.

The precision is generally appropriate in legal acts concerning cybersecurity, as they do not appear to risk under- or over-inclusion of real-life situations that necessitate a response. The connected regulatory frameworks are also sufficiently broad to facilitate understanding of the requirements and relevant responses. However, due to a lack of normative definition in the sectoral legislation, which specifically mentions only obligations for transmission network operators and leaves the inclusion of other actors to general legislative cybersecurity frameworks and to analogical reasoning, precision is also lacking in sectoral cybersecurity legislative drafting.

Regarding ambiguity, it is generally at an appropriate level; however, specific provisions may present practical implementation issues and should be clarified to improve effectiveness. Most notably, the definition of essential entities in Article 7 of ZInfV is too vague. It may cause individual entities (especially smaller ones) to misclassify themselves, leading to either unnecessary burdens or insufficient adherence by entities essential to cybersecurity to the relevant legal frameworks that aim to foster cyber resilience.

While it is commendable that a best available techniques-inspired principle is enshrined in Article 22 of ZinfV-1, the terminology used, namely "most advanced and appropriate European and international measures," is innovative. In this case, this is a disadvantage. It is suboptimal because it leaves too much room for interpretation, and including the term "European" may diminish the effectiveness of the measures if European standards do not align with global standards. Furthermore, the term "European" is unclear in itself, as it is not ascertainable from the legal text whether it refers to the European Union or the broader geographical region.

The definition of incidents in Article 29 employs several open-ended notions, such as "serious" and "could influence", leaving them susceptible to excessive interpretation by the legal subjects to whom the provision applies. This may compromise the effectiveness and speed of cyber resilience due to misclassification of incidents by relevant entities. The definition of a person with a legitimate reason for access under Article 33 is also unclear.

The Slovenian framework formally transposes the EU triad—namely, the NIS2 Directive (EU) 2022/2555, the CER Directive (EU) 2022/2557, and the directly applicable NCCS (Commission Delegated Regulation (EU) 2024/1366)—primarily through ZInfV-1 and ZKI-1. However, substantive implementation gaps persist in areas where EU law expressly permits stricter national measures (NIS2 Art. 1(2); CER Art. 1(2)).

NIS2 Article 21 supply-chain risk management is transposed only generally; ZOEE lacks mandatory vendor auditing or Software Bill of Materials (SBOM) requirements. CER Articles 12 (cross-border coordination) and 15 (resilience plan content) are implemented ad hoc in ZKI-1 Articles 13-15, without mandatory cyber-physical scenario testing or the national CER strategy, due by January 2026. (c) NCCS Arts. 28–29 (common electricity cybersecurity controls), Article 33 (supply-chain recommendations), and Article 37 (cyber-attack classification) are not yet mirrored in secondary legislation or operator protocols for ELES and SODO.

Thus, regulatory and policy approaches could be improved, particularly where NIS2 and CER permit the enactment of stricter measures by legislation. Especially relevant would be improvements to sector-specific legislation, mandating annual cyber stress tests for operators such as ELES, enforcing supply chain auditing protocols that strengthen NIS2 obligations, and integrating AI-driven threat modelling. In this regard, the national cybersecurity strategy should be updated and aligned with legislative change. These enhancements would improve precision and effectiveness, directly mitigating the identified legislative quality issues.

7. CONCLUSION

Thus, the Slovenian cybersecurity framework for the electrical grid, while generally effective in promoting cyber-resilience through broad risk management measures, is hindered by reduced clarity due to inconsistent terminology and fragmented provisions across acts, imprecise sectoral definitions that risk under-inclusion of key actors, and ambiguities in critical concepts such as entity classification and incident severity. These shortcomings could impede its effective implementation, underscoring the need for consolidated, refined legislative drafting. While the national provisions are broadly EU-compliant, the substantive issue is the reactive rather than proactive orientation of solutions, as well as the lack of mandatory cyber stress-testing scenarios, which would, among other things, build resilience against cascading failures and IoT manipulation. Our main proposal is thus to make relevant improvements in both substance and legislative drafting. These improvements primarily involve adopting sector-specific legislation, notably through ZOEE, which requires annual cyber stress tests to be incorporated into national resilience plans and other relevant strategies. The European Union Agency for Cybersecurity (ENISA) defines a cyber stress test as "a targeted assessment of the resilience of individual organisations and their ability to withstand and recover from significant cybersecurity incidents, ensuring the provision of critical services, in different risk scenarios".[65]

Supply-chain auditing protocols—the documented, systematic procedures to examine and verify compliance, quality, and cybersecurity risk across all tiers of the commercial supply network (including SBOM verification and recurring third-party audits)

[65] The European Union Agency for Cybersecurity (ENISA), 'Handbook for Cyber Stress Test' (2025) https://www.enisa.europa.eu/sites/default/files/2025-05/2025.04311_01_ms_v2.0_Handbook%20for%20Cyber%20Stress%20Tests_en.pdf accessed 28 January 2026.

DOI: 10.46282/blr.2026.10.1.1178

should be formalised via a new provision in ZInfV-1 Art. 21 and ZOEE.[66] AI-driven modelling should likewise be integrated into the Slovenian Cybersecurity Strategy. In purely drafting terms, unified terminology should be employed across the relevant legal acts.

Potential for further research is vast. In-depth comparative studies could be conducted, bridging disciplines and involving computer engineers, legal researchers, and security researchers, to identify the most effective policy and legal solutions and to determine which might be applicable in Slovenian circumstances. Benchmarking should be performed against Estonia's approach to advanced grid defences (an early NIS1/NIS2 adopter with strong supply chain risk monitoring) and Poland's recent NIS2 implementation (the amended UKSC Act of April 2026, which broadens scope and OT security requirements, informed by real-world energy cyberattacks). These experiences can usefully inform Slovenia's sector-specific measures in ZOEE and national resilience planning. Empirical and engineering-based investigations are necessary for various technologies and solutions in the Slovenian electrical energy system to identify potential risks and establish adequate resilience.

Ultimately, adequately fortifying the cybersecurity of the electrical grid will require not only legal precision as a fundamental prerequisite but also a proactive national commitment. True resilience will turn potential vulnerabilities into strengths through improvement, ensuring that Slovenia's liberties are safeguarded and that the lights stay on.

[66] Chivu Cezarina and others, 'Evaluation, Monitoring and Auditing of Suppliers in Supply Chain Management' (2021) 1 *International Journal of Manufacturing Economics and Management* 6 https://doi.org/10.54684/ijmem.2021.1.2.6 accessed 28 January 2026; Kamal Fahmy Salama and others, 'The Value of Auditing Supply Chains' (2009) 119 *International Journal of Production Economics* 34 https://doi.org/10.1016/j.ijpe.2008.12.018 accessed 9 May 2026.