

Analysis of the Russian Cyber Attacks Impact on Ukraine's Electrical Grid and Communication Infrastructure

Nindia Ayu Lilian^{1, a}

¹University of Darussalam Gontor

a_nindiaayulilian62@student.hi.unida.gontor.ac.id

Abstract: The ongoing Russo-Ukrainian war has been accompanied by intensive cyber operations targeting Ukraine's critical national infrastructure. This study addresses the growing problem of cyber attacks directed at Ukraine's electrical grid and civilian communication systems, which have posed significant risks to national security, public safety, and essential services. The purpose of this research is to analyze the impact of Russian cyber attacks on the stability, resilience, and functionality of Ukraine's electrical grid and communication infrastructure, as well as to assess the cascading effects on civilian life. A qualitative research method is employed, combining case study analysis of major cyber incidents (including the 2015 and 2016 power grid attacks, and ongoing disruptions during the full-scale invasion), review of technical reports from cybersecurity firms, and examination of official statements from Ukrainian government and international organizations. The findings indicate that Russian cyber attacks have caused repeated power outages, hindered emergency communication systems, disrupted internet connectivity, and exacerbated humanitarian challenges. Furthermore, the attacks have demonstrated a pattern of hybrid warfare, where cyber operations are coordinated with kinetic military strikes. The study concludes that Ukraine's infrastructure resilience has improved over time through international technical assistance and adaptive defensive measures, but significant vulnerabilities remain.

Keywords: Cyber warfare; critical infrastructure; Ukraine; electrical grid; Communication systems.

INTRODUCTION

The Russia-Ukraine war that began on February 24, 2022 is not only taking place conventionally, but also in the cyber field (Vailliant, 2018). Russia has been intensively targeting Ukraine's critical infrastructure, particularly the power and communications networks, since before the full-scale war erupted; These two sectors are prime targets because their paralysis can stop public services such as water, hospitals, transportation, as well as early warning systems and military coordination (Agrafiotis, 2018).

Modern power grids and communications are interdependent. Electrical control systems require reliable communication, while communication nodes require a power supply to operate, so a cyberattack on one sector can trigger a chain effect that intelligent measurement infrastructure (AMI) has a wide attack surface, (Sawada, 2024) while demonstrating that weak points are often at the interface between electrical and communication systems. (Tian, 2025) A clear example of this strategy was the attack on satellite service provider Viasat that occurred just before the 2022 invasion. The attack disabled thousands of Ukrainian military and civilian satellite modems, as well as knocking out about 5,800 wind turbines in Germany. (Asren Kazi, 2025) called this attack an "invisible battlefield". (Nicolò Boschetti, 2022) In addition, the Industroyer malware specifically designed to attack power substations is capable of leveraging industrial communication protocols and causing physical damage to the hardware. (Prof. Dr. Pavel Kozák, 2023)

Before the full-scale war of 2022, Ukraine had actually experienced a cyberattack on its power grid in 2015 that impacted 225,000 customers, as well as in 2016 that used an early variant of the Inusroyer malware (Prof. Dr. Pavel Kozák, 2023). However, the intensity of the attacks increased dramatically after 2022 arguing that these attacks were not just a technical glitch, but also a political and psychological tool to suppress public morale. (Szulecki, 2023) added that Russia's cyberattacks are part of a doctrine of "new generation warfare" that combines military, information, and cyber instruments simultaneously. (Pinto, 2024)

To measure impacts systematically, develop a four-layer taxonomy that includes technical, operational, social, and strategic impacts. (Agrafiotis, 2018) On the defense side, Ukraine with the support of international partners has developed various mitigation strategies such as network

segmentation and cyber incident response teams. (Zubok, 2023) noted that civil society is adapting to utilizing Telegram channels as an alternative source of information when official communication infrastructure is disrupted. F (Oleinik, 2024) or other countries, including Indonesia, the Ukraine case is an early warning. The vulnerability assessment model developed by the Transactions of China Electrotechnical Society (2024) and Electric Power Automation Equipment (2026) can be adopted to identify weak points before an attack occurs (Kloba, 2022)

The urgency of this research cannot be ignored for several reasons. The war in Ukraine is still ongoing and cyberattacks continue to evolve, so understanding the patterns of attacks in the past is critical to future defense preparation. In addition, many countries, including Indonesia, use technology similar to Ukraine, so the lessons from this conflict can be directly applied. Last but not least, policymakers need empirical evidence to craft an effective national cybersecurity strategy. (Parmaar, 2024)

Based on the background that has been described, this study aims to analyze the technical and operational impact of two significant Russian cyberattacks on Ukraine's electrical and communications infrastructure, namely the Viasat attack in 2022 and the Industroyer2 attack in 2022. The analysis was carried out using the taxonomic framework of the impact of and at the same time identifying the pattern of chain effects between the electricity sector and the communication sector. More specifically, this study seeks to answer three main questions, namely how the Viasat and Industroyer2 attacks affected Ukraine's electricity and communication infrastructure, and how chain effects arose between the two sectors as a result of these attacks. (Agrafiotis, 2018)

METHODS

This study uses a type of descriptive qualitative research with a library research approach. This means that this study does not conduct experiments, surveys, or direct observations in the field. Instead, all data and information is obtained from documents that have already been published, such as academic journals, conference proceedings, and credible technical reports. This approach was chosen because cyberattacks on Ukraine's critical infrastructure are ongoing in the war zone, making it impossible to conduct primary data collection directly on site.

The evidence base consists of academic literature identified in the original manuscript as Scopus-indexed publications, including peer-reviewed journal articles and conference proceedings, supplemented for incident verification by primary and institutional cybersecurity sources. For the revised analysis, priority was given to official incident reports and established cybersecurity research because these sources provide traceable technical and operational evidence.

The documentation search used the following keywords and combinations: "Russian cyber attack Ukraine electrical grid", "Viasat cyber attack", "Industroyer2 Ukraine", "critical infrastructure cybersecurity Ukraine", and "communication infrastructure attack Ukraine". For the revision, the incident evidence was re-checked on 27 August 2026 using official and institutional sources, including Viasat, CERT-UA, ESET, the UK National Cyber Security Centre (NCSC), and EU cybersecurity materials. Inclusion criteria were: (1) direct relevance to Russian cyber operations against Ukraine; (2) direct relevance to the Viasat or Industroyer2 incidents or their documented infrastructure impacts; (3) identifiable authorship or institutional provenance; and (4) publication in English or an authoritative institutional source. Duplicates, unsupported commentary, and sources that could not be traced to an identifiable publication or institution were excluded.

A source-quality assessment was applied before evidence was used in the analysis. Tier 1 sources consisted of official incident reports and government cybersecurity assessments, such as Viasat, CERT-UA, NCSC, and EU statements. Tier 2 sources consisted of established cybersecurity research and peer-reviewed academic studies. Tier 3 sources were institutional or technical analyses used only for contextual interpretation. Numerical and causal claims were retained only when supported by Tier 1 or Tier 2 evidence, or when independently corroborated. The original search process did not preserve a dated database log or database-level hit counts; therefore, the exact number of records retrieved and screened from the original search cannot be reconstructed reliably and is not fabricated in this revision.

Instead, the revised manuscript reports the documented evidence retained for each case and makes the source hierarchy explicit.

RESULTS AND DISCUSSION

The Impact of the Viasat Attack (2022) on Communication and Electricity Infrastructure

The Viasat attack occurred on February 24, 2022, approximately one hour before Russia launched its full-scale invasion. The attack targeted the KA-SAT satellite network used for fixed broadband services. Viasat reported that the incident affected several thousand customers in Ukraine and tens of thousands of other fixed-broadband customers across Europe. The UK NCSC and the EU subsequently assessed or attributed the operation to Russia. (Viasat, 2022; NCSC, 2022; Council of the EU, 2022).

In technical terms, the attack exploited a misconfiguration in a VPN appliance to obtain access to the trusted management segment of the KA-SAT network. The attacker then used legitimate management commands to overwrite key data in the flash memory of residential modems, making many of them unable to reconnect until they were reset, updated, or replaced. Viasat reported that the affected modems were not permanently destroyed and that the satellite itself and its supporting ground infrastructure were not directly compromised. These documented findings provide a stronger basis for describing the incident as a compromise of communication-network management and endpoint equipment rather than as a direct attack on the electrical grid. (Viasat, 2022).

Operationally, the attack disrupted satellite broadband services for several thousand customers in Ukraine and tens of thousands of customers elsewhere in Europe. It also disrupted remote monitoring and control access for more than 5,800 Enercon wind turbines in Germany because their communications depended on the affected satellite network. The turbines themselves continued operating, but operators temporarily lost remote monitoring and control capabilities. This provides a documented example of how disruption to communication infrastructure can affect the operation and visibility of energy infrastructure beyond the original geographic target. (Viasat, 2022; NCSC, 2022).

The social impact was primarily related to the loss of reliable communication and internet access. The EU reported communication outages affecting public authorities, businesses, and users in Ukraine, while the broader European disruption affected civilian users as well. The evidence supports describing reduced access to communication and information as a documented consequence; stronger claims about panic, evacuation behavior, or psychological effects should be treated as interpretations unless supported by direct empirical evidence. (Council of the EU, 2022).

Strategically, the Viasat incident demonstrated that a cyber operation against a commercial satellite communication network can produce cross-border consequences and affect both military-relevant and civilian services. The EU and UK publicly attributed the operation to Russia, highlighting its relevance to the broader conflict. The incident therefore illustrates the strategic importance of protecting shared communication infrastructure and managing dependencies on third-party satellite services. (Council of the EU, 2022; NCSC, 2022).

The Viasat case also illustrates a documented cross-sector dependency. The cyberattack did not directly target a power plant or wind turbine control system; instead, it disrupted the communication link used for remote monitoring and control. The loss of that communication link affected the operators' ability to monitor and control more than 5,800 wind turbines in Germany. This distinction is important: the evidence supports a communication-to-energy dependency, but it does not establish that the attack directly caused a loss of electricity generation. (Viasat, 2022; NCSC, 2022).

From a strategic perspective, the incident raised wider concerns about the security and resilience of commercial satellite infrastructure used by both civilian and government users. Rather than claiming that the attack directly changed NATO or EU policy, the evidence more safely supports the conclusion that it demonstrated the strategic risks created by dependence on shared satellite communication infrastructure and the potential for cross-border spillover effects. (Council of the EU, 2022; NCSC, 2022).

The Impact of the Industroyer2 Attack (2022) on Electricity Infrastructure

The Industroyer2 incident was identified in April 2022 as a new variant of the earlier Industroyer malware. ESET and CERT-UA reported that the Sandworm group attempted to deploy Industroyer2

against high-voltage electrical substations in Ukraine. The malware was designed to interact with industrial control systems and issue commands relevant to substation operations. Importantly, the planned destructive action was prevented before it produced the large-scale power outage that the attackers intended. Therefore, the documented 2022 case should be described as an attempted disruption of the electrical grid rather than as a confirmed blackout. (ESET, 2022; CERT-UA, 2022).

The operational impact of the 2022 Industroyer2 incident was primarily the threat and attempted disruption of electricity distribution infrastructure, together with the deployment of CaddyWiper against Windows-based systems and destructive scripts against Linux-based equipment. CERT-UA reported that the planned shutdown of electrical substations and associated infrastructure was prevented. Claims about hospitals, water systems, banking services, or heating failures should not be presented as direct consequences of this specific 2022 incident unless supported by separate evidence from documented outages. (CERT-UA, 2022; ESET, 2022).

The social impact of the 2022 Industroyer2 incident must likewise be stated cautiously. Because the planned substation shutdown was prevented, the available evidence does not support attributing widespread civilian hardship or psychological effects directly to this incident. Such effects may be relevant to earlier successful attacks on Ukraine's power grid, but they should be distinguished from the documented consequences of the Industroyer2 attempt. This distinction strengthens the causal accuracy of the analysis.

Strategically, the Industroyer2 incident demonstrates the importance of defending industrial control systems and maintaining the ability to detect and contain attacks before they reach the intended operational stage. CERT-UA reported cooperation with international partners and the sharing of malware samples and threat information with other Ukrainian energy-sector organizations. These documented response measures support the conclusion that information sharing and rapid incident response contributed to prevention and resilience. (CERT-UA, 2022; ESET, 2022).

The Industroyer2 case represents an evolution of the earlier Industroyer capability, but the comparison should be made carefully. ESET reported that Industroyer2 was a new variant used by Sandworm in the April 2022 attempt against a Ukrainian energy provider. Unlike the successful 2016 power-grid attack, the 2022 operation was prevented before the intended shutdown could be completed. The evidence therefore supports a comparison of capabilities and defensive outcomes, but not a claim that Industroyer2 itself caused the same scale of blackout as the 2016 incident. (ESET, 2022; CERT-UA, 2022).

The social and psychological consequences discussed elsewhere in relation to prolonged power outages should not be attributed directly to the prevented Industroyer2 operation. For this case, the stronger conclusion is that the incident exposed the potential for cyber operations against industrial control systems to create serious consequences for essential services if defensive measures fail. This distinction between intended impact and documented impact is essential for a reliable assessment.

Evidence classification. To avoid overstating causality, the comparison distinguishes three levels of evidence: (1) documented consequences directly reported by incident or official sources; (2) secondary interpretations supported by technical literature; and (3) analytical implications inferred from infrastructure interdependence. Only the first category is presented as an observed outcome of the two incidents. Potential cascading effects are explicitly identified as analytical implications unless supported by incident-specific evidence.

Comparative Impact Matrix

Table 1 compares the two incidents using the same four impact dimensions. The matrix separates observed/documented effects from intended or potential consequences.

Chain Effect Patterns between Electricity and Communication

The two cases demonstrate two possible directions of cross-sector dependency, but the evidence differs in strength. The Viasat incident provides direct evidence that disruption of communication affected remote monitoring and control of energy assets. By contrast, the Industroyer2 incident was prevented before a large-scale power outage occurred, so any communication-sector consequences from an actual blackout remain analytical rather than documented for this case. The first direction is an

attack on communication impacting electricity. The Viasat attack provides the clearest documented example in the cases examined. reported that a wind turbine in Germany controlled via satellite also shut down because its communications were cut off. Similar dependencies may exist in other energy assets that rely on satellite communication, but this manuscript does not treat such effects as documented consequences of the Viasat incident without case-specific evidence. (Oberghaell, 2024) explains that hierarchical control systems on modern power grids rely heavily on real-time communication. When communication is interrupted, operators lose visibility to grid conditions, and automated systems cannot provide control commands. In some cases, the automatic security system at the power plant considers the loss of communication as an indication of a malfunction and automatically shuts down the plant to prevent damage. This is a safety feature that actually backfires when communication is disrupted due to a cyberattack. (Sawada, 2024)

The second direction, the attack on electricity has an impact on communication. A successful disruption of electricity could affect communication infrastructure that depends on grid power, particularly where backup capacity is limited. However, this was not a documented consequence of the prevented Industroyer2 operation and is therefore treated here as a potential chain effect rather than an observed outcome. (Prof. Dr. Pavel Kozák, 2023) noted that as a result, mobile communications and the internet were blacked out in the area, even if there was technically no direct attack on the communication infrastructure. Such an outage could reduce the ability of civilians and technical teams to communicate during recovery, but these effects should not be attributed directly to the prevented 2022 Industroyer2 incident. They had to return to the office for instructions, which slowed down the recovery process. Examples from other documented outage contexts may illustrate this dependency, but they should be cited separately and should not be presented as direct consequences of the Industroyer2 incident. (Weiho, 2026)

Cumulative effects and vicious circles: What aggravates is the cumulative effects of these two directions. The IEEE Transaction shows that intelligent measurement infrastructure (AMI) that is supposed to help early detection of attacks is actually paralyzed when power or communication is disrupted. AMI relies on two-way communication between the electricity meter in residents' homes and the control center. When communication is off, the control center cannot know where the outage occurred (Bhalja, 2024). They have to rely on manual reports from citizens, which are obviously slower and inaccurate. In a successful cross-sector attack, a potential vicious cycle could emerge: power disruption may reduce communications availability, reduced communications may complicate coordination, and slower coordination may prolong recovery. In the present cases, this is an analytical model rather than a fully documented sequence of consequences. (Giles, 2020) estimates that this chain effect could extend the duration of the outage by up to twice as long as if only one sector was affected. In the case of a combined attack, an outage that would have lasted only 4 hours could drag on to 8-10 hours. He added that to break this vicious cycle, a combination of early detection technology, mature recovery procedures, and real-time updated threat intelligence is needed. (Islam, 2019)

The two-directional cascading effects identified in this study attacks on communication disrupting electricity, and attacks on electricity disrupting communication create a vicious cycle that exponentially amplifies the damage of any single cyberattack. This finding aligns with (Radanliev, 2024), who argue that traditional risk assessment methods often fail to capture such cascading effects because their approach is overly linear and sectoral. In reality, when a cyberattack causes a power outage, communication networks fail; when communication networks fail, recovery teams cannot coordinate; when recovery is delayed, the outage duration extends; and when outages persist, cascading failures spread to other sectors like water, transportation, and healthcare. (Bhamare, 2024) note that this amplification effect can extend the duration of an outage by up to twice as long as if only a single sector was affected. For policymakers, this means that investing in sectoral cybersecurity separately is insufficient; what is needed is a cross-sectoral resilience strategy that specifically addresses the interdependencies between electricity and communication networks.

Breaking this vicious cycle requires a combination of technical and organizational measures. On the technical side, (Zeadally, 2015) advocate for built-in redundancy in both electricity and communication systems, so that the failure of one network does not automatically trigger the collapse of the other. This includes backup power for communication nodes and alternative communication channels for grid

operators that do not rely on the public internet. On the organizational side, (Islam, 2019) emphasize the importance of real-time threat intelligence sharing between sectors and across national borders. Ukraine's resilience has been supported by technical defenses, information sharing, international assistance, and adaptation of defensive strategies; however, the relative contribution of each factor requires separate empirical assessment. For countries like Indonesia, this suggests that building cyber resilience is not merely a technical exercise but also a diplomatic and institutional one. Establishing clear protocols for cross-sectoral coordination and international information sharing may be just as important as deploying the latest cybersecurity software.

Evidence verification note: The incident-level claims in the revised analysis were checked against primary or authoritative sources, including Viasat's KA-SAT incident report, CERT-UA's report on the Industroyer2 operation, ESET's technical analysis, and the UK NCSC and EU attribution statements. These sources were prioritized over unsupported secondary claims for dates, attribution, technical mechanisms, and numerical impacts.

CONCLUSION

This study analyzed two Russian cyberattacks affecting Ukraine's electricity and communications infrastructure using the impact taxonomy from Agraftis et al. (2018). The Viasat attack (2022) primarily affected communication services and produced documented cross-border operational effects, while the Industroyer2 operation (2022) targeted electrical infrastructure but was prevented before the planned shutdown could be completed. The two cases therefore illustrate different impact profiles and different defensive requirements.

The Viasat attack disrupted several thousand customers in Ukraine and tens of thousands of other fixed-broadband customers across Europe. It also caused the loss of remote monitoring and control access for more than 5,800 wind turbines in Germany, although the turbines continued operating. In contrast, Industroyer2 was an attempted attack on high-voltage substations that was detected and prevented before the intended destructive action could cause a large-scale blackout. These distinctions are important because they separate documented consequences from intended or potential consequences. (Viasat, 2022; NCSC, 2022; ESET, 2022; CERT-UA, 2022).

The comparison nevertheless demonstrates a clear cross-sector dependency. The Viasat incident shows how disruption to communication infrastructure can impair remote monitoring and control of energy assets, while the Industroyer2 incident shows how communication and industrial-control dependencies can become part of an attack pathway against the electricity sector. The evidence supports the need for cross-sectoral resilience, but it does not justify assuming that every cyber disruption will automatically produce a physical blackout or a twofold increase in outage duration. Such effects should be assessed case by case using documented operational evidence.

Interestingly, the study also found that Russia's cyberattacks on Ukraine show a pattern of learning and improvement over time. The Industroyer attack in 2016 was still relatively crude and left a lot of digital footprints, but the Industroyer2 variant used in 2022 was much more subtle, harder to detect, and more targeted at specific targets. This shift indicates that Russia is actively learning from the successes and failures of previous attacks. The implication for other countries is that cyber threats are not static; The adversary will continue to improve its capabilities, so cyber defense must also continue to evolve. Relying on the same strategy as five years ago will most likely not be enough to deal with future attacks.

The findings of this research have direct implications for Indonesia because the country also depends on interconnected information and operational technology across strategic sectors. Indonesia's Presidential Regulation No. 82 of 2022 on Critical Information Infrastructure Protection defines critical information infrastructure as electronic systems that may operate independently or interdependently with other systems and whose disruption can seriously affect public interests, public services, defense and security, or the national economy. The regulation identifies eight strategic sectors, including energy and mineral resources and information and communication technology, and assigns sectoral responsibility while designating BSSN as the coordinator of critical information infrastructure protection. This governance structure is relevant to the Ukrainian cases because both cases demonstrate that a disruption in one infrastructure can create consequences for another. For Indonesia, the comparable

dependency between energy systems and communication or information systems means that risk assessment should not be limited to individual sectors. Cross-sector dependency mapping, network segmentation, redundancy, backup communication, and coordinated incident response should be incorporated into the protection of critical information infrastructure. (Presidential Regulation No. 82/2022).

The governance mechanism also provides a basis for coordinated incident response. Presidential Regulation No. 82 of 2022 provides for national, sectoral, and organizational cyber incident response teams, while BSSN is assigned a coordinating role. In addition, the National Cyber Security Action Plan 2024–2028 provides a national framework for translating cybersecurity priorities into planned activities, targets, responsible institutions, and indicators. These mechanisms do not make Indonesia identical to Ukraine, and the Ukrainian wartime environment cannot be directly transferred to the Indonesian context. Rather, the comparison indicates a practical lesson: Indonesia's existing governance framework can be strengthened by testing cross-sector incident scenarios in which communication and energy systems are disrupted together, and by ensuring that recovery procedures remain functional when one supporting infrastructure is unavailable. (BSSN Regulation No. 5/2024).

REFERENCES

- Agrafiotis, D. (2018). A taxonomy of cyber-harms: Defining impacts of cyber-attacks. *Journal of Cybersecurity (Oxford)*, <https://doi.org/10.1093/cybsec/tyy006>.
- Arsheen Kazi, S. K. (2025). Invisible Battlefields: Analyzing the Viasat Attack and its Broader Implications. *Scientific Buletin*, Vol.30 No.1,<https://doi.org/10.2478/bsaft-2025-0007>, 62-63.
- Asren Kazi, S. K. (2025). Invisible Battlefields: Analyzing the Viasat Attack and its Broader Implications. *Sciend*, <https://doi.org/10.2478/bsaft-2025-0007>.
- Basharina, A. E. (2025). Comprehensive Assessment of Criticality of Energy System Elements Based on Service-Oriented Approach . *Programming And Computer Software*.
- Bhalja, A. A. (2024). Deep Learning-based Detection and Mitigation Strategy for Cyber-attacks on Advanced Metering Infrastructure. *2024 IEEE International Systems Conference (SysCon)*, <https://doi.org/10.1109/SysCon61195.2024.10553479>.
- Bhamare. (2024). Detecting the cyber-physical-social cooperated APTs in high-DER-penetrated smart grids: Threats, current work and challenges. *Computer Networks*, Vol.254, <https://doi.org/10.1016/j.comnet.2024.110776>.
- Council of the European Union. (2022, May 10). Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union.
- Galushchenko, O. (2024). Cybersecurity and geopolitical dimensions of external information interventions in Ukraine: Analysis of current tren. *Data dan Metadata*, <https://doi.org/10.56294/dm2024.345>.
- European Union Agency for Cybersecurity. (2022). [Use only if retained in the final manuscript after source verification.]
- ESET. (2022, April 12). Return of Industroyer: New cyberattacks against Ukraine's energy sector.
- Giles, V. A. (2020). Russia's Cyber and Information Warfare. *Asia Policy*, <https://doi.org/10.1353/asp.2020.0014>.
- Igor Kotenko, I. S. (2024). An Approach to Detecting Cyber Attacks against Smart Power Grids Based on the Analysis of Network Traffic Self-Similarity. *Energies*, Vol.19 No.13, <https://doi.org/10.3390/en13195031>.
- Islam, H. I. (2019). Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. *Journal of Universal Computer Science*, <https://doi.org/10.3217/jucs-025-11-1478>.
- Katarina Ivancova, J. K. (2025). Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations. *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, <https://doi.org/10.1109/SAMI63904.2025.10883298>.

- Kloba, L. K. (2022). Cyber threats of the banking sector in conditions of war in Ukraine. *Financial and Credit Activity: Problems of Theory and Practice*, <https://doi.org/10.55643/fcaptp.5.46.2022.3883>.
- Luo, Y. (2025). Invulnerability analysis of urban power system based multi-layer heterogeneous complex network considering high-security level. *Reliability Engineering & System Safety*, <https://doi.org/10.1016/j.ress.2025.110860>.
- National Cyber Security Centre. (2022, May 10). Russia behind cyber attack with Europe-wide impact an hour before Ukraine invasion.
- Nicolò Boschetti, N. G. (2022). Space cybersecurity lessons learned from the viasat cyberattack. *American Institute of Aeronautics and Astronautics (AIAA), ASCEND*, <https://doi.org/10.2514/6.2022-4380>, 4380.
- Obergfaell, A. C. (2024). Cyber attacks on critical infrastructures and satellite communications. *International Journal of Critical Infrastructure Protection (IJ CIP)*, <https://doi.org/10.1016/j.ijcip.2024.100701>.
- Oleinik, A. (2024). Telegram Channels Covering Russia's Invasion of Ukraine: A Comparative Analysis of Large Multilingual Corpora. *Journal of Computational Social Science*, <https://doi.org/10.1007/s42001-023-00240-9>.
- Parmaar, S. S. (2024). The Cyberwar Between Russia and Ukraine: Impacts and Implications. *SSRN Electronic Journal (Social Science Research Network)*, <https://doi.org/10.2139/ssrn.5019998>.
- Pinto, D. J. (2024). Thematic Section: Contemporary geopolitics and cyber security and defense challenges. *Relações Internacionais (R:I)*, <https://doi.org/10.23906/ri2024.82>, 67.
- Presidential Regulation of the Republic of Indonesia No. 82 of 2022 on Critical Information Infrastructure Protection. (2022, May 24).
- Prof. Dr. Pavel Kozák, I. K. (2023). Industroyer cyber-attacks on Ukraine's critical infrastructure. *2023 International Conference on Military Technologies (ICMT)*, <https://doi.org/10.1109/ICMT58149.2023.10171308>, 4-5.
- Radanliev, P. (2024). Cyber Risk Assessment in Critical National Infrastructure: Lessons from Ukraine. *Journal of Cyber Policy*, Vol.9 No.2, <https://doi.org/10.1080/23738871.2024.2341248>, 192.
- Regulation of the National Cyber and Crypto Agency (BSSN) No. 5 of 2024 on the National Cyber Security Action Plan 2024–2028. (2024, June 7).
- Saunders, L. A. (2024). Private-public initiatives for cybersecurity: the case of Ukraine. *Journal of Cyber Policy*, <https://doi.org/10.1080/23738871.2025.2451256>, 400-402.
- Sawada, K. O. (2024). Model Reconstruction via Hierarchical Supervisory Control with Cyber Attacks. *IEEE Conference*, <https://doi.org/10.1109/ICCE59016.2024.10444174>.
- Szulecki, L. G. (2023). Interpreting cyber-energy-security events: experts, social imaginaries, and policy discourses around the 2016 Ukraine blackout. *European Security*, Vol.32 No.1, <https://doi.org/10.1080/09662839.2022.2082838>, 117-119.
- Tian, P. H. (2025). Dual graph-based vulnerability evaluation for power grids considering fault correlation by utilizing improved e-index method. *Physica Scripta*, <https://doi.org/10.1088/1402-4896/ae0f5c>.
- Vaillant, M. A. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly* Vol.12 No.3, <https://doi.org/10.2307/26430819>, 75-76.
- Viasat. (2022, March 30). KA-SAT network cyber attack overview.
- Weiho, W. (2026). Vulnerability assessment method of urban electricity-water coupling network based on meta-learning. *Electric Power Automation Equipment*, <https://doi.org/10.16081/j.epae.202511011>, 28-29.
- Yilu, Y. (2024). Vulnerability Assessment of Urban Power Grid Based on Electricity-Water Cross-Layer Coupling Model. *Transactions of China Electrotechnical Society*, <https://doi.org/10.19595/j.cnki.1000-6753.tces.230870>.

Zeadally, C. A. (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection*, <https://doi.org/10.1016/j.ijcip.2014.12.002>, 58-60.

Zolanvari, D. B. (2024). Cybersecurity for smart grids: A comprehensive survey. *Computer Networks*.

Zubok, A. D. (2023). Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War. *CyCon 2023*, <https://doi.org/10.23919/CyCon58705.2023.10181813>.