International Science Journal of Engineering & Agriculture
2025; 4(1): 103-110
https://isg-journal.com/isjea
doi: 10.46299/j.isjea.20250401.09
ISSN: 2720-6319

INTERNATIONAL
SCIENCE GROUP

The resilience of critical information infrastructure topology in the cyberspace

Georgii Dubynskyi
G.E.Pukhov Institute of Modelling Problems in Energy of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID 0009-0002-5895-9700

Vitalii Zubok
G.E.Pukhov Institute of Modelling Problems in Energy of the National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID 0000-0002-6315-5259

To cite this article:
Dubynskyi Georgii, Zubok Vitalii. The resilience of critical information infrastructure topology in the cyberspace. International Science Journal of Engineering & Agriculture. Vol. 4, No. 1, 2025, pp. 103-110. doi: 10.46299/j.isjea.20250401.09.
Received: 01 06, 2025; **Accepted**: 01 31, 2025; **Published**: 02 01, 2025

Abstract: Modern trends in the decentralization and branching of systems that process, store, and transmit information enhance system resilience. Increasingly, technological systems and operational technologies rely on electronic communications from third-party operators and cyberspace. However, these trends introduce new cybersecurity challenges and contradictions. This article presents risk-informed approaches to designing and modernizing the topology of critical information infrastructure (CII). Such approaches involve making decisions and implementing security measures based on a thorough assessment of organizational risks. By evaluating the likelihood and impact of threats, vulnerabilities, and potential consequences, resources are prioritized to achieve a balance between security, functionality, and cost-effectiveness. The recommendations focus on practices for assessing cybersecurity risks, particularly those arising from cyberattacks targeting external (cyberspace) connections of CII. They also emphasize enhancing the protection of critical information assets from such threats. Unlike general cybersecurity measures, these recommendations specifically address risks associated with CII's cyberspace topology, providing additional or supplementary measures to existing procedures within the information security lifecycle.

Keywords: dynamic systems, critical information infrastructure, dynamic systems, cyber resilience, topology, cyberspace, risk assessment, risk categorisation.

1. Introduction

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use cyber resources, is commonly referred to as cyber resilience and it includes building cyber security systems. The objects of cyber security are elements of critical information infrastructure (CIIO), which are defined by Ukrainian legislation as information and communication systems of critical facilities that are fundamentally important for their functioning. Examples of such systems include power energy networks, transport systems, financial institutions, healthcare systems, government services, public digital services, and more. Their functioning often relies on industrial control systems (ICS), also referred as industrial automation control systems (IACS).

The decentralization and branching of systems that process, store, and transmit information are modern trends that positively impact system resilience. Increasingly, technological systems and operational technologies use electronic communications from third-party operators and cyberspace. However, these trends pose new challenges in terms of cybersecurity, leading to contradictions between inevitable need for scaling, geographical distribution of functions, integration with cloud platforms, from one side, and cyber and data security requirements from the other side.

To better understand, analyse and protect those systems, we require an approach to identify vulnerabilities and develop appropriate security strategies. The first step is usually decomposition, i.e. breaking those objects into smaller components in order to determine the interaction between the components. This paper proposes a topological approach to such an analysis.

2. Object and subject of research

The object of the research is the topology of connections of CII facilities in the cyber space, which include different kinds of electronic communications and remote access technologies between stakeholders of CII functioning.

The subject of the research is methods for increasing the security of the topology of external connections of CII in cyberspace.

3. Research objective

The outcome of this research must become a risk-informed approach to designing and modernizing the topology of critical information infrastructure. Such approaches involve making decisions and implementing security measures based on a thorough assessment of organizational risks. By evaluating the likelihood and impact of threats, vulnerabilities, and potential consequences, resources are prioritized to achieve a balance between security, functionality, and cost-effectiveness.

The recommendations should focus on practices for assessing cybersecurity risks, particularly those arising from cyberattacks targeting external (cyberspace) connections of CII. They also must emphasize enhancing the protection of critical information assets from such threats.

4. Literature analysis

The cybersecurity of critical infrastructure (CI), including industrial control systems (ICS) and industrial automation and control systems (IACS), is a crucial aspect of national security. Modern standards and guidelines, such as documents by the U.S. National Institute of Standards and Technology (NIST) and Ukraine’s regulatory acts, offer comprehensive approaches to protecting critical systems against cyber threats. NIST documents and Ukrainian regulations complement each other, creating a comprehensive approach to CI cybersecurity. They provide both strategic vision and practical recommendations for protecting ICS/IACS and critical information infrastructure, considering contemporary cyber threats.

The NIST Cybersecurity Framework, or simply NIST CSF (*National Institute of Standards and Technology,* 2024) is a foundational document providing a systematic approach to cybersecurity, focusing on five key functions: identify, protect, detect, respond, and recover. This framework serves as a basis for managing risks associated with CI, enabling organizations to adapt cybersecurity measures to their specific needs. In Ukraine, the NIST CSF was adapted and adopted as regulation (*On approval of methodological recommendations for the categorization of critical infrastructure,* 2021). Regulation generally repeat the previous version of the CSF, with significant modifications to the national regulatory documents.

The Guide to Operational Technology Security (*Stouffer, 2023*) addresses the specific challenges of ICS cybersecurity, such as protecting real-time network operations and ensuring physical security.

Its recommendations include safeguarding against cyber threats that could disrupt industrial processes and managing access to ICS/IACS components.

NIST Special Publication 800-160 Volume 2, titled "Developing Cyber-Resilient Systems: A Systems Security Engineering Approach" (*Ross*, 2021), focuses on the concept of cyber resilience in the context of system design and engineering. It provides a comprehensive framework for building and maintaining systems that can continue to function effectively even in the face of cyberattacks or disruptions. The publication emphasizes the need for security engineering that integrates resilience into all phases of a system's lifecycle, from design through operation and eventual decommissioning.

Ukrainian regulatory documents, such as ND TZI (Normative Documents on Technical Protection of Information), establish general provisions for information protection in automated systems. For instance, ND TZI 1.1-002-99 (*General provisions on the protection of information in computer systems from unauthorized access*, 1999) and ND TZI 1.4-001-2000 (*Model regulation on the information protection service in automated systems*, 2000) detail requirements for organizing information protection services, managing access, and ensuring confidentiality, which are vital for protecting critical information infrastructure. The collection of ND TZI was sufficiently updated in 2021 for better interoperability with NIST documents (*The procedure for selecting measures to protect information, the protection requirement of which is established by law and not classified, for information systems*, 2021).

State Service of Special Communications and Information Protection of Ukraine is a responsible government body for CI security during martial law. There are several regulations regarding CI and CII classification, categorization, information protection and cyber security, which will be referred further in this paper.

5. Research methods

According to the (*On the basic principles of ensuring cybersecurity of Ukraine, 2024*), a critical information infrastructure object (CII Object) is communication or technological, a cyberattack on which would significantly impact the operational continuity of such critical infrastructure. Thus, CII is a system containing electronic communication elements that can be targeted by cyberattacks. The following terms are also used in these guidelines:

- **Critical Information Asset (CA):** A component of CII whose integrity or unauthorized access directly affects the sustainable functioning of the critical infrastructure (CI).
- **Access Control Mechanism (ACM):** A set of communication or technological systems providing secure access to the CA.
- **Access Control Entity** to Critical Information Assets **(ACE):** A combination of CII components capable of initiating access to the CA. This includes users, administrators, dispatchers, and elements of machine interaction—software tools for CII whose access to CA is critical for the sustainable functioning of CII.
- **Cyberspace of CII:** A subset of cyberspace elements formed by ACM connecting to cyberspace, allowing ACE entities to CA.
- **Supply Chain (SC):** The set of processes, infrastructure, technologies, resources, and interactions between participants ensuring the creation, development, delivery, and support of CII functions for end consumers. Access control mechanisms is part of the SC but do not limit it.

ACM as a set of communication or technological systems providing access to CA, can be considered a supply chain. SC risks are well-documented and standardized in ISO 28000:2007 and later in ISO 28000:2022 (Prazian, 2023). However, since SC risks comprise risks from each individual connection within SC, the accuracy of risk assessment depends on the detail level of the physical and logical topology of electronic communications (*Derzhspozhyvstandart of Ukraine*, 2022).

The guidelines for categorizing CI objects in (*On approval of methodological recommendations for the categorization of critical infrastructure facilities*, 2021) lack specific instructions for categorizing information security risks in CII. However, as per the methodology suggested in the (*Stouffer*, 2023), each OT element (i.e., IT used in cyber-physical systems) must be assessed regarding threats impacting the security goals—confidentiality, integrity, and availability.

Thus, each connection in the SC should be evaluated separately for three types of risk: its impact on confidentiality, integrity, and availability. Example Category Representation:

Category= {**Integrity:** Level,
Confidentiality: Level,
Availability: Level}

In this way, each connection in the topology of external ties of the CII in cyberspace can be categorized. Categorization is necessary because different measures and tools for cybersecurity (in NIST terminology – security controls) are used to ensure availability and confidentiality.

Many factors can be taken into account for categorization, the main one being the category of information accessed through this connection. For example, for information from sensors, the need for availability will have the highest priority. In contrast, for updates to the embedded software of sensors, the highest priority will be the integrity of the information [The NIST Cybersecurity Framework (CSF) 2.0. (2024b). URL: https://doi.org/10.6028/nist.cswp.29.].

To assess impact levels, a common practice is to use at least three degrees: low, medium, and high. The scale of degrees can be broader, for example, "low, moderate, high, extreme." Each degree should be assigned a numerical value for further processing.

5.1 Categorization of Topological Risks According to the Functions and Authority of the Access Entity

To assess the risk of a particular connection between an access entity (ACE)to critical information assets and a Critical Information Asset (CA), it is necessary to make assumptions about the impact that a potential intruder could cause through this connection. The assumption should be that the intruder has gained authority over a certain ACE access entity to critical information assets. This task is similar to constructing an intruder model. The following characteristics of the intruder should be considered: competence, equipment, motivation (goal), and authority within the system.

An example of initial information for risk analysis of a particular external connection:

- ACE category
- ACE Information Categories
- ACE Protocol Security
- Criticality of Availability (Acceptable Downtime for ACE Functions)

Template options may be used for categorizing the impact according to the role of the CIIA. Examples of categorization are presented in Table 1.

Table 1. Examples of Categorization of the Impact of an Intruder According to the Role of the Access Subject

№	Access Subject Category	Impact Weighting Coefficient (WC)
1	Administrator of a Critical Information Asset	1
2	User of a Critical Information Asset	0,2
3	Monitoring or Surveillance Subject	0,5
4	Machine-to-Machine (M2M) Interaction	0,25

Additionally, there are criteria for classifying intruders in the guidelines [НД ТЗІ 1.1-002-99, p.6.5] and [НД ТЗІ 1.4-001-2000, p.4.4].

The product of the categorization according to the impact on confidentiality, integrity, and availability, and the weighting coefficient of the ACErole, determines the assessment of the scale of the damage (consequences), which can be expressed by the following tuple:

$$DSA\ (CA) = (C + I + A) \times WC \tag{1}$$

where DSA is the result of the damage scale assessment, and WC is the weighting coefficient of the impact.

6. Research results

As a result of the study, a descriptive part of measures to increase the cyber resilience of the CIIO topology was developed. In accordance with the descriptive part, methods for quantifying and measuring the effectiveness of measures to improve the topology were proposed.

6.1. Secure Placement of Critical Information Assets

The adoption of Industry 4.0 and IIoT technologies has somewhat bridged the gap between purely informational technologies and operational technologies used in industrial and manufacturing facilities. Consequently, regardless of the operational nature of a Critical Information Infrastructure Object (CIIO) to which a Critical Information Asset (CA) belongs, there are several architectural solutions for its placement.

One of the most significant factors influencing the topology of a CIIA is the choice of a foundational architectural solution—deploying the system either on the organization's own hardware and software infrastructure (on-premises) or in a rented "cloud." Despite advancements in cloud solutions, many companies continue to favor local (on-premises or in-house) deployments. This preference is based on the belief that on-premises systems provide better control over sensitive data, ensuring that the data is stored, transmitted, and processed within infrastructure fully controlled by the organization. However, on-premises deployments introduce additional requirements for ensuring the secure operation of CAs, including enhancing cyber resilience (*Ross*, 2021).

- Provision of autonomous power supply using modern high-capacity batteries or generators.
- Geographic distribution of primary and backup servers to avoid the impact of regional disruptions, such as major power outages.
- Modification of disaster recovery procedures to account for realistic recovery time and data recovery points during prolonged outages.
- Installation of monitoring and management systems that enable remote control of the system and infrastructure even during power outages, ensuring rapid response to issues and optimal recovery times.

As a result, many organizations have reevaluated their approach to sensitive data confidentiality in favor of accessibility, aligning better with business continuity objectives. However, a cloud solution means in fact transferring logical access to the data to another participant in the SC. An alternative to on-premises or rented cloud solutions is deploying CAs in specialized data center facilities (DCF) while using the owner's hardware. This approach, known as colocation, mitigates threats associated with confidentiality in cloud environments. Certified data centers, such as those meeting Tier Certification standards (*Uptime Institute*, n.d.) or (*ISO/IEC*, 2021), are designed to offer a level of physical security and energy autonomy that would require substantial capital investment for individual CA owners. The cost-effectiveness of such investments must be carefully considered.

A modern approach is the use of hybrid cloud infrastructure, combining private environments (on-premises, private cloud, or colocation) with public clouds. The use of public cloud resources can vary dynamically depending on specific workflow demands. Hybrid infrastructure allows sensitive data to remain securely stored locally in a private environment, while applications and virtual machines leverage the public cloud's advantages, such as rapid scalability.

Modern ICS (IACS) often employ hybrid architectures, integrating on-premises assets with private or public clouds that are integral to specific platforms (a common approach in Industrial IoT). Organizational and technical risks associated with cloud computing are extensively outlined in ENISA recommendations (*European Union Agency for Cybersecurity*, n.d.).

6.2. Selecting an Effective Cyber Topology for Critical Information Assets

Selecting a cloud service provider, colocation provider, or Internet access provider must account for threats originating from the global Internet routing system, such as route hijacking and route leaks. These incidents often impact the network address space used by CAs, leading to their inaccessibility via external channels and, in some cases, posing risks to the integrity and confidentiality of transmitted information.

If the address space for CAs is provided by a colocation or Internet service provider, preference should be given to providers with more effective topologies for external connections (*Zubok*, 2022).

For CAs using address spaces directly managed by the Critical Information Infrastructure Asset (CIIA) owner, the goal is to connect the CA to at least two Internet service providers with effective external connection topologies. Additionally, continuous measures should be implemented, including:

- **Routing policy control** at external gateways.
- **Monitoring network prefix statuses** using data from Internet registries and specialized services like BGPmon or QRator.Radar.
- **Proper publication of routing policies.**
- **Electronic certification of route sources.**

6.3. Securing Communications with Access Entities

Information exchange between CAs and their respective ACEentities is subject to various attacks, particularly man-in-the-middle (MitM) attacks. Therefore, secure protocols that ensure authentication and access control should be used. Encryption should be employed to secure connections over external networks (those outside the CIIA's ownership), such as corporate CI IT networks or the Internet. For geographically distant ACE, secure connections are often established over leased networks or public networks (e.g., the Internet). Connections to virtual private networks (VPNs) should utilize encryption protocols such as **Transport Layer Security (TLS)** or **Internet Protocol Security (IPsec)** to safeguard data (Stouffer, 2023). VPNs encompass a set of protocols designed to ensure reliable authentication and encryption for communication security. They create private networks that overlay public infrastructure, maintaining confidentiality and integrity.

- **IP Security (IPsec):**

Supports two encryption modes:

  - **Transport mode:** Encrypts only the data payload of packets, leaving the header intact.
  - **Tunnel mode:** Adds a new header and encrypts both the original header and payload for enhanced security. An IPsec-compatible device at the receiver end decrypts the packets.

- **Transport Layer Security (TLS):**

Establishes a secure channel between machines, encrypting the contents of each packet. Known for protecting HTTP traffic as HTTPS, TLS is versatile and can secure various application-layer protocols, such as email. Only TLS 1.2 or newer should be considered, as earlier versions are obsolete.

- **Secure Shell (SSH):**

A command-line interface and protocol for secure access to remote computers, file transfers, command execution, and tunneling other application-layer protocols. SSH is widely used for remote management of Linux servers, included in most UNIX distributions, and available for other platforms as a third-party package.

6.4. Resilience of CIIA During Large-Scale Power Outages

In the context of attacks on critical infrastructure, selecting communication technologies should focus on minimizing reliance on power supply and maximizing functionality under intermittent conditions.

The key criteria for assessing the feasibility of implementing specific solutions are:

- Minimally acceptable system functionality
- Affordable recovery costs
- Target recovery time

The study (*Zubok*, 2023) compares various "last mile" communication technologies typically used to connect end-users, including Ethernet, DOCSIS, xDSL, FTTx, xPON, and various satellite broadband systems (VSAT, Starlink, OneWeb). Selecting the most effective combinations of these options may require further refinement to identify the best solution based on a set of metrics m:

- **Feasibility of implementation** (m1);
- **Speed of implementation** (m2);
- **Low implementation cost** (m3);
- **Effectiveness of implementation** (m4).

Since critical infrastructure is at stake, faster recovery is the highest priority. Implementation effectiveness can be reflected in either a reduction in recovery time or recovery costs within a defined recovery point objective (RPO) as part of the damage scale assessment (3).

Example: The xPON broadband network technology is considered the most resilient to power shortages if only the endpoints are provided with autonomous power. This technology ensures high data availability for exchanges between CAs and ACE during large-scale power outages. This is especially valuable as uninterrupted operation (i.e., faster recovery) is the highest priority for critical infrastructure organizations.

An essential factor is the practical feasibility of using certain solutions to improve network access availability in a specific location or building. A numerical evaluation approach can be applied by assigning weights to each parameter. An example is presented in Table 2.

Table 2. Measuring the Resilience of CIIA

	m_1	m_2	m_3	m_4	**Metric Sum m_2 - m_4**
1. Reliable "Last Mile"					
• FTTN	yes	3	3	1	7
• GPON	yes	4	3	5	12
• Starlink	yes	2	1	5	8
• LTE	yes	1	2	2	5
2. Autonomous Power for ACE					
• Standard UPS	yes	5	8	1	14
• UPS with High-Capacity Batteries	yes	3	5	5	13
• Hybrid with Renewable Sources	yes	1	1	10	12
• Hybrid with Fuel Generator	no				
3. Security of CA Placement					
• on-premises	yes	3	1	9	13
• colocation	yes	4	5	9	18
• Public Cloud	no				
• Hybrid	yes	2	3	9	14

7. Conclusions and discussion

The risk-informed approaches to organizing the topology of critical information infrastructure (CII) during its design and modernization . Methodological recommendations are presented for prioritizing resource allocation to improve CII topology based on the likelihood and potential impact of threats.

The approaches outlined enable translating the complex task of achieving an optimal balance between security, functionality, and cost-efficiency into practical application. The introduces practices for assessing the risks of cyber incidents originating from external connections (cyberspace links) of critical information infrastructure objects, as well as for enhancing the cyber resilience of critical information assets.

References:

1) National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

2) *On approval of methodological recommendations for the categorization of critical infrastructure facilities*. (2021). State Service for Special Communications and Information Protection of Ukraine: Order No. 23. https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

3) Stouffer, K. (2023). *Guide to operational technology (OT) security* (NIST Special Publication 800-82r3). https://doi.org/10.6028/nist.sp.800-82r3

4) Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing cyber-resilient systems* (NIST Special Publication 800-160 Volume 2 Revision 1). https://doi.org/10.6028/nist.sp.800-160v2r12

5) *General provisions on the protection of information in computer systems from unauthorized access* (1999). State Service of Special Communications and Information Protection of Ukraine.. *ND TZI 1.1-002-99:*. Approved by order No. 22, April 28, 1999.

6) *Model regulation on the information protection service in automated systems*. (2000). State Service of Special Communications and Information Protection of Ukraine. *ND TZI 1.4-001-2000.* Approved by order No. 53, December 4, 2000.

7) *The procedure for selecting measures to protect information, the protection requirement of which is established by law and not classified, for information systems (2021)*. State Service of Special Communications and Information Protection of Ukraine. *ND TZI 3.6-006-2021:* Approved by order No. 570, July 3, 2024.

8) *On the basic principles of ensuring cybersecurity of Ukraine, Law of Ukraine № 2163-VIII* (2024). https://zakon.rada.gov.ua/laws/show/2163-19#Text

9) Prazian, M. (2023). Resilience for better sustainability: ISO 28000: 2022 vs 2007 comparative analysis. *Nuclear and Radiation Safety, 1*(97), 67–70. https://doi.org/10.32918/nrs.2023.1(97).08

10) Derzhspozhyvstandart of Ukraine. (2022). *DSTU EN IEC 31010:2022 Risk management – Risk assessment methods (EN IEC 31010:2019, IDT; IEC 31010:2019, IDT)*. Official edition.

11) Uptime Institute. (n.d.). *Tier certification overview*. Retrieved May 12, 2024, from https://uptimeinstitute.com/tier-certification

12) ISO/IEC. (2021). ISO/IEC 22237: *Information technology — Data center facilities and infrastructures — Part 1: General requirements and operational performance (International Standard)*. International Organization for Standardization. https://www.iso.org/standard/76263.html

13) European Union Agency for Cybersecurity (ENISA). (n.d.). *Cloud computing: Benefits, risks, and recommendations for information security*. Retrieved November 11, 2024, from http://www.enisa.europa.eu/media/news-items/cloud-computing-speech

14) Zubok, V. Yu., and Mohor, V. V. (2022). *Cybersecurity of INTERNET topology* (1st ed.). Kyiv: IPME im. G.E. Pukhov. https://doi.org/10.5281/zenodo.6795229

15) Zubok, V 2023 IOP Conf. Ser.: Earth Environ. Sci. 1254 012039ю https://iopscience.iop.org/article/10.1088/1755-1315/1254/1/012039