

Cyber Threats to Critical Infrastructure in the Baltic Sea Region

Cyber Threats to Critical Infrastructure in the Baltic Sea Region

NATIONAL CYBER
SECURITY CENTRE

Table of Content

1. PREFACE 4

2. LIST OF ABBREVIATIONS 5

3. INTRODUCTION 6

3.1. Context and Objectives of the Project 6

3.2. Approach and Methodology 6

3.3. Proposed Structure of the Study 7

4. EXECUTIVE SUMMARY 8

5. ANALYSIS OF THE CURRENT STATE OF CRITICAL INFRASTRUCTURE IN THE BALTIC REGION 9

5.1. Essential Assets: Prioritizing Critical Infrastructure for Resilience and Security 9

5.2. Challenges in Securing Critical Infrastructure of the Baltic Sea Region 12

5.3. Key Vulnerabilities 16

5.4. Key Threat Actors 20

5.5. Key Attacks Against Critical Infrastructure Sector 24

5.6. Role of CTI in Protecting Critical Infrastructure 25

6. CORRELATION TO THE SITUATION WITH OTHER REGIONS 26

6.1. Western Europe and North America Region 27

6.2. Indo-Pacific Region 29

7. LESSONS FROM UKRAINE: ENHANCING CYBER RESILIENCE 30

7.1. Infrastructure Evaluation and Vulnerability Identification 30

7.2. Case Studies and Success Stories 32

7.3. Enhancement Strategies (Lessons Learned) 33

8. MITIGATIONS AND RECOMMENDATIONS FOR THE CRITICAL INFRASTRUCTURE 36

9. CONCLUSIONS AND WAY FORWARD 40

1. Preface

The Baltic Sea region faces growing cybersecurity challenges that necessitate a proactive and collaborative approach. Globally escalating cyber threats underscore the urgency for the Baltic Sea region states to fortify their critical infrastructure against potential attacks. The Ukrainian experience provides an important case study, emphasizing the multifaceted nature of cyber threats. Ukraine has faced cyberattacks targeting critical infrastructure, ranging from energy grids to government systems. Analysis of the tactics, techniques, and procedures employed in these attacks is crucial for bolstering defences in the Baltic Sea region.

2. List of abbreviations

Term/abbreviation	Meaning/explanation
RCDC	NCSC REGIONAL CYBER DEFENCE CENTRE
CTAC	CYBER THREAT ANALYSIS CELL
ECI	EUROPEAN CRITICAL INFRASTRUCTURE
NIS2	NETWORK AND INFORMATION SECURITY
IRPF	INFRASTRUCTURE RESILIENCE PLANNING FRAMEWORK
EEA	EUROPEAN ECONOMIC AREA
PPP	PUBLIC-PRIVATE PARTNERSHIP
RaaS	RANSOMWARE-AS-A-SERVICE
VPN	VIRTUAL PRIVATE NETWORK
TTP	TACTICS, TECHNIQUES, AND PROCEDURES
GRU	THE MAIN DIRECTORATE OF THE GENERAL STAFF OF THE ARMED FORCES OF THE RUSSIAN FEDERATION
BIG4	RUSSIA, IRAN, NORTH KOREA, CHINA
USAID	UNITED STATES AGENCY FOR INTERNATIONAL DEVELOPMENT

3. Introduction

3.1. Context and Objectives of the Project

Established as a joint initiative of Lithuania and the United States, the NCSC Regional Cyber Defence Center (RCDC) aims to fill the niche of practical cooperation in the field of cyber defence and strengthen the capacity of both Lithuania and the regional partners to ensure cyber security of their states. The RCDC is a regional platform for practical cooperation on assistance in protection of critical infrastructure from cyberattacks. RCDC activities focus on strengthening resilience and cyber defence capacity of critical public service providers.

The overall objective of the Cyber Threats to Critical Infrastructure in the Baltic Sea region project is to develop a comprehensive study of cyber threats targeting critical infrastructure in the Baltic Sea region. This study aims to provide critical infrastructure stakeholders with valuable insights into the current state of the Baltic Sea region critical infrastructure security, main attack vectors, vulnerabilities and threat actors who are interested in this region. Additionally, the study will draw on the lessons learned from previous incidents, particularly focusing on the Ukrainian experience, to offer practical recommendations for strengthening defences against the evolving threats. This proactive approach will equip the Baltic Sea region with the knowledge and strategies necessary to safeguard critical infrastructure effectively and to ensure uninterrupted operations in the face of persistent and sophisticated cyber threats.

3.2. Approach and Methodology

To achieve the Project objectives, the Cyber Threats to Critical Infrastructure in the Baltic Sea region study is based on:

1. Analysis carried out by RCDC experts with assistance from the rotating personnel from Georgia, the United States of America and Ukraine.
2. Secondary research and an in-depth review and analysis of international open-source information and studies.
3. Input from the Baltic Sea region country – Estonia.
4. Analysis and experience from the Indo-Pacific region.

This research aims to deliver a comprehensive analysis of cyber threats to critical infrastructure in the Baltic Sea region, focusing on the objective to develop a clear view of the current security situation. That involves conducting a detailed examination of the region, identifying key assets, challenges, and vulnerabilities, and analysing potential cyber threat actors targeting critical infrastructure. The study will pinpoint the weaknesses that can be exploited by the mentioned

actors while providing valuable insights into the regional security landscape. The research seeks to contribute to the development of effective strategies for safeguarding critical assets in the Baltic Sea region.

3.3. Proposed Structure of the Study

The study is proposed to be divided into several separate parts:

- Chapter 4 is the Executive Summary;
- Chapter 5 analyses the current state of the Baltic Sea region critical infrastructure: main assets, sectors of targeting, challenges in securing it and key vulnerabilities, as well as key threat actors;
- Chapter 6 investigates correlations between different regions;
- Chapter 7 is dedicated to Ukraine's experience;
- Chapter 8 addresses mitigation and recommendations for securing critical infrastructure;
- Chapter 9 is Conclusions and Way Forward.

4. Executive Summary

Key Observations and Conclusions

The Baltic Sea region - Estonia, Latvia, Lithuania, Poland, Germany, Denmark, Sweden, and Finland - is a critical hub for economic and geopolitical activities. Infrastructure in the Baltic Sea region is vital to the energy supply, transportation, and communication with the rest of Europe. However, strategic importance more severe vulnerability to cyber threats.

Key Observations:

1. **Increasing Frequency of Cyber Attacks:** As threat actors get increasingly sophisticated, so do their attacks and their frequency. The Baltic Sea Region is no exception. There had been an increase in targeting of the region ranging from ransomware to sophisticated state-sponsored attacks[1].
2. **Various Threat Actors:** The region is threatened by a variety of actors: state-sponsored groups, hacktivists, and criminal organizations. The motivation behind the attacks varies from espionage and sabotage to financial gain and political influence.
3. **Vulnerable Sectors:** The most targeted sectors are energy, especially oil and gas, transportation sector, including maritime and aviation, and communication networks. These are vital for regional stability and economic vitality.

Conclusions:

The growing cyber-related threats in the Baltic Sea region pose a significant risk to critical infrastructure, potentially disrupting essential services and economic activities. To mitigate these risks, it is crucial to enhance regional cooperation through the development of joint cybersecurity initiatives that focus on sharing threat intelligence and best practices. Additionally, strong public-private partnerships and strategic investments in cybersecurity technologies, including continuous threat monitoring and effective incident response plans, are essential to safeguard critical infrastructure and ensure rapid recovery from cyberattacks.

[1] https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-32-russias-hybrid-threat-tactics-against-the-baltic-sea-region-from-disinformation-to-sabotage/

5. Analysis of the Current State of Critical Infrastructure in the Baltic Region

5.1. Essential Assets: Prioritizing Critical Infrastructure for Resilience and Security

When discussing critical infrastructure assets, it is imperative to identify and prioritize the primary sectors that form the backbone of societal functioning and national security. First and foremost, the energy sector is crucial because it determines the generation, transmission, and distribution of electricity and fuels essential for powering homes, industries, and other critical infrastructure organizations. Disruptions in energy supply can have cascading effects on all other sectors, making it a top priority for resilience planning. For instance, a prolonged power outage can cripple communication networks, halt transportation systems, and disrupt water treatment facilities, highlighting the interconnected nature of these assets. This study focusses on critical infrastructure sectors which are vital for everyday life of society and in an armed conflict situation.

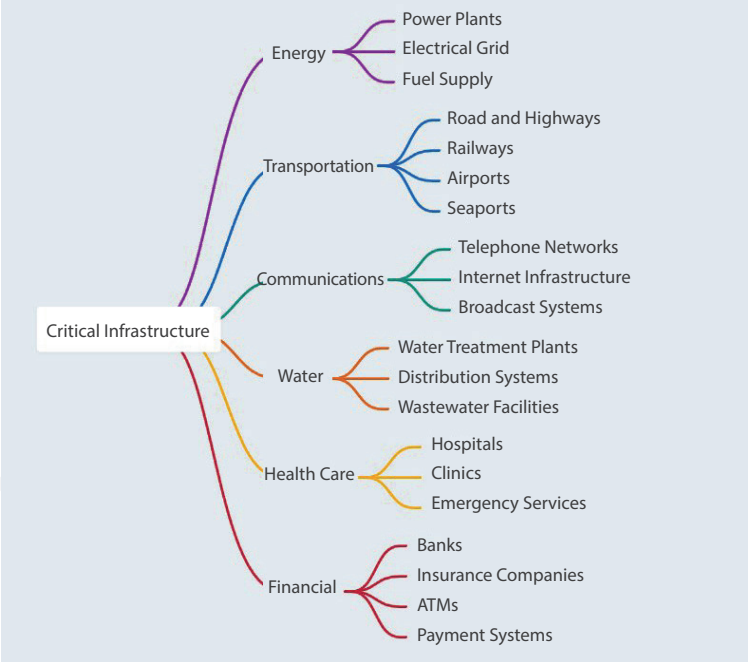


Figure 1. Critical infrastructure sectors and their components

Energy Sector

- **Main Services:** Generation, transmission, and distribution of electricity and fuels.
- **Assets:** Power plants, transmission lines, substations, distribution networks.
- **Threats:** Cyberattacks, extreme weather events (e.g., hurricanes, wildfires), fuel supply disruptions. The increasing digitization of energy systems, such as the adoption of smart grids and renewable energy technologies, introduces new vulnerabilities that cyber adversaries can exploit. These advancements require continuous investment in cybersecurity measures, such as robust protocols, real-time monitoring, and a strong collaboration between public and private sectors to share cyber threat intelligence. A comprehensive approach to securing the energy sector involves not only hardening physical assets but also ensuring the cybersecurity of increasingly interconnected and automated systems.

Transportation Sector

- **Main Services:** The transportation sector is essential for the movement of people and goods, serving as a critical backbone for economic activity and societal connectivity.
- **Assets:** Roads, bridges, railways, airports, seaports, public transit systems.
- **Threats:** As the sector becomes increasingly reliant on digital technologies and automation, it faces growing cybersecurity threats that must be addressed to ensure resilience. The vast infrastructure encompassing roads, railways, airports, and seaports is not only vulnerable to physical disruptions but also to cyberattacks that could have immediate and widespread impacts on supply chains, emergency responses, and daily commutes. The integration of smart transportation technologies boosts efficiency and safety but also introduces significant cybersecurity risks. Protecting critical infrastructure like railways, airports, and public transit systems requires robust cybersecurity alongside physical upgrades.

Communications Sector

- **Main Services:** The communications sector is vital to modern society, providing the critical infrastructure for connectivity and information exchange. This sector encompasses telecommunications networks, internet infrastructure, broadcasting systems, and satellite communications.
- **Assets:** Fiber optic networks, data centres, broadcast towers, satellite networks.
- **Threats:** The transition to advanced technologies like fiber-optic, 5G, and satellite systems in telecommunications, broadcasting, and satellite communications introduces significant risks, including increased cyber threats, potential data breaches, service disruptions, and vulnerability to space weather events. To counter these risks, robust cybersecurity measures such as encryption, firewalls, continuous monitoring, and contingency planning are essential to ensure the resilience and reliability of these critical communication systems, particularly during emergencies.

Water Sector

- **Main Services:** The water sector, essential for providing clean drinking water, managing wastewater, and supporting agricultural irrigation, is fundamental to public health and ecological balance.
- **Assets:** Reservoirs, treatment plants, distribution networks, sewage systems.
- **Threats:** The water sector faces significant threats from cyberattacks that could compromise water safety, disrupt operational integrity, and lead to severe public health crises and economic losses. The modernization of water treatment technologies and the reliance on digital components increase vulnerability to cyber threats. Distribution networks, including pipelines and pumping stations, are at risk of unauthorized access and manipulation, potentially disrupting water delivery. Similarly, wastewater management infrastructure, which depends on advanced digital controls, is vulnerable to cyber threats. Protecting these systems requires robust cybersecurity measures, including securing control networks, data encryption, and regular security assessments. Measures such as securing SCADA systems, implementing encryption for data transmission, and regular security assessments are essential to protect these critical assets.

Healthcare Sector

- **Main Services:** The healthcare sector is crucial for public health and managing emergencies, encompassing hospitals, clinics, emergency medical services, and public health agencies.
- **Assets:** Medical facilities, emergency response vehicles, digital health technologies.
- **Threats:** The healthcare sector faces significant threats from cyberattacks, including data breaches, ransomware, and disruptions to critical services like emergency medical systems and public health agencies. These attacks can compromise patient data, disrupt communication networks, and hinder the operational continuity of healthcare services. The growing integration of telemedicine and digital health technologies further heightens these risks. Protecting these systems involves implementing comprehensive cybersecurity protocols such as encryption, secure access controls, and continuous network monitoring to guard against data breaches and ransomware attacks. Regular updates and patches to medical devices and IT infrastructure are crucial to addressing vulnerabilities.

Financial sector

- **Main Services:** The financial sector is crucial to economic stability, given its role in payment systems, credit availability, and investment flows.
- **Assets:** Banks, financial institutions, regulatory frameworks.

- **Threats:** The financial sector of the Baltic Sea region is increasingly vulnerable to cyber threats due to the growing digitization of financial services. As banks and financial institutions expand their online offerings and integrate advanced technologies, they become prime targets for cyber-attacks, which can compromise sensitive financial data, disrupt operations, and erode client trust. To defend against cyber threats, Baltic banks should implement stringent cybersecurity measures, including advanced encryption, multi-factor authentication, and continuous network monitoring. Regular security assessments and incident response plans are also vital to protect against data breaches and cyberattacks. Given the sector's close integration with the EU financial architecture and cross-border operations, maintaining secure connections, and adhering to EU regulations are critical. This involves robust defences against phishing, malware, and other cyber threats that could disrupt financial stability.

In summary, the energy, transportation, communications, water, finance, and healthcare sectors are at the core of critical infrastructure. Their continuous operation is essential for societal stability and security, both in peacetime and during conflicts. By prioritizing these sectors, we can ensure a resilient infrastructure capable of withstanding and recovering from various disruptions. This comprehensive approach to infrastructure protection not only enhances national security but also promotes economic prosperity and public well-being. Ensuring the resilience of critical infrastructure is not only a matter of national security but also the foundation of sustainable development and public welfare.

5.2. Challenges in Securing Critical Infrastructure of the Baltic Sea Region

The Baltic Sea region faces several critical infrastructure challenges, largely due to its strategic location and significance. This area is a prime target for both state-sponsored advanced persistent threats (APT) and less sophisticated hacktivist groups. Geopolitical tensions heavily influence cybersecurity in this region, particularly, since Finland and later Sweden became NATO members. The proximity to Russia further exacerbates these tensions, as cyber actors continually attempt to infiltrate critical infrastructure in the region.

- **Complexity of Infrastructure**

The complexity of the critical infrastructure in the Baltic Sea region presents a formidable cybersecurity challenge. It is presented by the integration of diverse systems, technologies, and processes that must work in concert to deliver essential services. These systems often span multiple domains, including energy, transportation, communication, and water management, each with their unique operational requirements and security considerations. System interdependencies mean that vulnerability in one area can have cascading effects across the entire infrastructure. Managing such a complex environment requires comprehensive visibility into all components and their interactions. However, achieving such visibility is difficult due to the heterogeneity of the technologies involved, ranging from legacy systems to innovative IoT devices. This techno-

logical diversity complicates the implementation of standardized security measures and makes it challenging to maintain up-to-date security postures. Furthermore, integration of operational technology (OT) with information technology (IT) introduces additional layers of complexity, as OT systems often lack the security features inherent in modern IT systems.

- **Information Security Management System**

It is critical to understand an organization's business processes and to identify the (IT) assets used in the process to protect the critical infrastructure against cyber threats. It is not possible to protect the organization adequately without implementing a structured and functional information security management approach. An ISMS helps to identify and address threats and opportunities to organizations concerning valuable information and any related assets. It protects from security breaches and shields from disruptions when they happen. An ISMS guarantees sustainability of the information security process in an organization and establishes the capability to learn from incidents, as well as to consider changes in the external environment. It is mandatory for the critical infrastructure to implement an ISMS and to maintain baseline security in an organization.

- **Awareness and Training**

Awareness and training are critical components of cybersecurity strategy for critical infrastructure. Despite the sophisticated technologies deployed to protect these systems, human error remains a significant vulnerability. General awareness training is essential for all employees, covering fundamental security practices: such as recognizing phishing attempts, maintaining strong passwords, and following secure protocols for accessing and handling sensitive information. Training can be delivered through online courses, in-person workshops, and regular updates on emerging threats. For employees responsible for managing and operating critical systems, specialized training is necessary. This includes exhaustive expertise in specific threats and vulnerabilities associated with their systems, secure configuration practices, and incident response protocols. Specialized training can be provided through advanced courses, hands-on labs, and certification programs. Practical exercises and simulations that replicate real-world cyber incidents should be conducted to enhance effectiveness of these training programs. Exercises, such as tabletop exercises and red team/blue team drills, help employees develop the skills needed to respond effectively to actual threats. Continuous education and updates are vital to keep the workforce informed about new threats and changes in security protocols. Monthly newsletters, webinars, and access to updated learning resources can support this ongoing education.

Another critical awareness and training approach is Operational Technology (OT) training ranges that are specialized environments designed to simulate and train professionals in securing industrial control systems (ICS) and critical infrastructure. These ranges offer realistic simulations of OT environments, including SCADA systems and PLCs, enabling hands-on learning through scenario-based exercises. Participants engage in cyber incident simulations specific to sectors, like energy and manufacturing, practicing cybersecurity strategies without risking operational disruptions. OT training ranges foster a multi-disciplinary approach, integrating IT security with

OT operational needs, and utilize advanced technologies, like digital twins and VR/AR, for immersive learning experiences. They adhere to industry standards and compliance frameworks as they prepare professionals to defend OT environments effectively while continuously evolving to address emerging cyber threats.

Finally, fostering a culture of cybersecurity within an organization, where security is viewed as a shared responsibility, can significantly enhance overall security awareness and compliance with best practices. This can be achieved through leadership endorsement, rewards, and recognition programs, and integrating security into daily workflows. By addressing these aspects comprehensively, organizations can better equip their workforce to protect critical infrastructure from cyber threats.

Incident Response and Recovery

Effective incident response and recovery are essential for minimizing the impact of cyberattacks on critical infrastructure. However, developing and maintaining robust incident response capabilities is challenging due to the complexity and scale of the systems involved. Incident response plans must be comprehensive, detailing the steps to be taken in the event of diverse types of cyber incidents, from malware infections to large-scale coordinated attacks. Operational continuity and physical safety must be given top priority in critical infrastructure incident response plans. Effective network segmentation, specialized security solutions made for OT environments, and cooperation with OT engineers and operators are all crucial. The identification of vulnerabilities and enhancement of defences necessitates the implementation of real-time monitoring and anomaly detection, resilient system design, and periodic security audits and penetration tests. To further improve the capacity to respond to and recover from incidents and guarantee the safety and continuity of critical infrastructure operations, incident response drills and training catered to over-the-horizon scenarios, as well as reliable patch management and secure remote access solutions must be thought-out.

Public-Private Partnerships

Public-private partnerships play a vital role in enhancing the cybersecurity of critical infrastructure. These collaborations improve the general security posture by facilitating the exchange of threat intelligence and best practices between public and private sectors. Advanced cybersecurity tools and technologies are often inaccessible to individual entities; however, through public-private partnerships, they can be made accessible. Additionally, they offer a venue for a coordinated reaction to cyber incidents, guaranteeing more rapid and efficient threat mitigation.

Critical infrastructure public-private partnerships face difficulties and factors that are not usually present in other industries. These include handling difficult regulatory compliance requirements, dealing with issues related to national security, and handling the serious risks associated with cyberattacks that could jeopardize both economic stability and public safety.

In the Baltic Sea region, several successful public-private partnerships have been implemented to enhance critical infrastructure. One notable example is the Vilnius Declaration, where eight Baltic Sea countries pledged to collaborate on securing offshore energy infrastructure.[2]



Figure 2. Technological Tensions: The Nexus of Global Commerce and Cyber Surveillance

Legacy Systems

Legacy systems continue to pose significant cybersecurity challenges to the critical infrastructure in the Baltic Sea region. Outdated technologies often lack modern security features, rely on unsupported software and hardware and, therefore, are more vulnerable to cyber threats. Presence of legacy systems in critical infrastructure creates numerous technical challenges that must be addressed to enhance the overall security. Within the critical infrastructure sector, legacy systems are common because of the excessive costs and complexity associated with upgrading or replacing them. Since many of these systems are deeply embedded in essential functions and were constructed decades ago, it is difficult to switch to newer technologies without significantly affecting operations. Additionally, the specialized nature and customization of these systems often make finding compatible modern solutions difficult, further entrenching their use.

One of the primary challenges is integration of legacy systems with modern technologies. It often requires specialized interfaces and protocols which can introduce additional vulnerabilities if not properly secured. Furthermore, the process of upgrading or replacing legacy systems can be

[2] https://balticwind.eu/baltic-sea-countries-pledge-closer-collaboration-to-secure-critical-offshore-energy-infrastructure/

complex and resource-intensive, requiring careful planning and coordination to avoid disruptions in essential services. To mitigate the risks associated with legacy systems, organizations must implement compensatory security measures, such as network segmentation, and use virtual private networks (VPNs) to isolate and protect vulnerable systems. Regular security assessments and audits are also essential for identifying and addressing potential vulnerabilities. Additionally, organizations should develop strategic plans for a gradual replacement of legacy systems with more secure and modern alternatives, ensuring that critical infrastructure remains resilient in the face of evolving cyber threats.

5.3. Key Vulnerabilities

Vulnerabilities of the critical infrastructure in the Baltic Sea region can be broadly categorized into physical vulnerabilities, logical (cyber) vulnerabilities, persona (cyber) vulnerabilities, supply chain dependencies, interconnected systems, human factors, and social engineering, zero-day vulnerabilities, and the remote work infrastructure. Together, they form a complex web of risks that requires a multifaceted approach for an effective mitigation.

- **Supply Chain Dependencies**

Supply chain dependencies introduce a complex layer of vulnerabilities to the critical infrastructure in the Baltic Sea Region. The interconnected nature of modern supply chains means that the security of critical infrastructure is only as strong as its weakest link. Many components and services are sourced from a multitude of external suppliers, each of which can become a potential point of failure or attack. It is possible to find a few notable examples regarding supply chain and its dependencies specific to the Baltic Sea region.

Talking about energy supply, the region heavily depends on undersea pipelines, countries are also dependent on oil terminals, particularly around gulf of Riga and Gulf of Finland Electricity on the other hand is also a challenge: interconnected systems exist between Nord's and Balts power markets throughout undersea cables, ensuring both stability and creating dependency as Baltic countries are working hard to fully synchronize their electrical grids with continental Europe and exit the post-soviet BRELL ring.

Transportation plays a key role in the Baltic Sea region – since countries are surrounded by the Baltic Sea, all of them have at least one port which is crucial for all matters, from shipping goods to serving military needs. A severe cyber-attack on ports infrastructure may cause millions of euros loss. Rail and road networks are also vital for regional connectivity.

Key point is understanding that supply chain dependencies are one of main vulnerabilities for this region, as it is highly interconnected.

Interconnected Systems

In the critical infrastructure sector interconnected systems present specific vulnerabilities that can lead to significant disruptions and spillover effect to other sectors. In the energy sector, for example, cyber-attacks targeting SCADA systems can disrupt power grids, causing widespread blackouts affecting other critical sectors. The transportation sector is no exception when it comes to interconnected systems. This sector highly relies on interconnected systems for port and railway networks, making it vulnerable to attacks that can severely impact logistics and supply chains. Similarly, in the water supply sector, attacks on interconnected control systems managing water treatment and distribution can result in contamination and service outages causing mayhem and impacting the broad public and other organizations.

To defend against cyber-attacks on interconnected critical infrastructure, organizations should implement multi-factor authentication to secure access, conduct regular penetration testing to identify vulnerabilities, and use behavioural analytics to detect abnormal activities. Employing application whitelisting ensures only approved software runs on critical systems. Securing the supply chain, deploying deception technology like honeypots, and establishing continuous threat hunting programs are vital in keeping critical infrastructure safe and out of reach to adversaries.

Human Factors and Social Engineering

Human factors and social engineering represent some of the most challenging vulnerabilities in the critical infrastructure of the Baltic Sea region that need to be addressed. Cybercriminals frequently exploit human psychology using such techniques as phishing, pretexting, and baiting to gain unauthorized access to systems and data. Phishing attacks, for example, involve tricking individuals into revealing their credentials or clicking on malicious links, which can lead to system compromise or data breaches.

Insider threats, whether intentional or accidental, also pose significant risks. Employees with legitimate access to critical systems can be manipulated or coerced into performing actions that compromise security. This risk is exacerbated by inadequate access controls and insufficient monitoring of user activities. To counteract these human-related vulnerabilities, comprehensive cybersecurity training programs are essential. These programs should educate employees about common social engineering tactics and promote the culture of vigilance and security awareness. Implementing robust access controls and continuously monitoring user activities can also help in detecting and preventing unauthorized actions.

Zero-Day Vulnerabilities

Zero-day vulnerabilities represent a particularly serious threat to cybersecurity of the critical infrastructure in the Baltic Sea region. These vulnerabilities are unknown to software vendors and therefore have no existing patches or fixes which makes them particularly dangerous. Attackers who

discover zero-day vulnerabilities can exploit them to gain unauthorized access, disrupt operations, or steal sensitive data before the vulnerability is detected and mitigated. The unpredictability and the potential level of severity of zero-day attacks require a proactive approach to cybersecurity. This includes implementing advanced threat detection and prevention technologies, such as intrusion detection systems (IDS) and endpoint protection platforms (EPP), which can identify and respond to suspicious activities indicative of zero-day exploits. Additionally, fostering a culture of continuous improvement and rapid patch management is crucial to minimize the window of exposure to such vulnerabilities.

One of the primary challenges in addressing zero-day vulnerabilities in networking equipment is the difficulty in detecting them. Unlike known vulnerabilities, zero-day exploits do not have existing signatures that can be detected by traditional security tools. Attackers can use these exploits to remain undetected for extended periods, conducting espionage, data theft, or preparing for larger, more destructive attacks. This stealthy nature makes zero-day vulnerabilities particularly dangerous, as they can undermine the security of critical infrastructure without triggering immediate detection. The impact of zero-day vulnerabilities in networking equipment can be particularly severe in the context of supply chain security. Networking equipment is often sourced from a variety of global manufacturers and suppliers which creates a complex supply chain difficult to secure comprehensively. Compromised equipment provided by a supplier can introduce zero-day vulnerabilities into critical infrastructure and give attackers a covert method of infiltration. To address this risk, it is essential to implement stringent supply chain security measures, including thorough vetting and continuous monitoring of suppliers, as well as establishing strong contractual requirements for cybersecurity standards. Mitigation of the risks associated with zero-day vulnerabilities in networking equipment requires a multifaceted approach. Firstly, organizations must adopt advanced threat detection and prevention technologies that go beyond traditional signature-based detection. Behavioural analysis, machine learning, and artificial intelligence can help to identify anomalies and suspicious activities indicative of zero-day exploits. For instance, network traffic analysis can detect unusual patterns that may signal an ongoing zero-day attack, enabling prompt response and mitigation efforts.

Secondly, fostering a culture of continuous improvement and rapid response is crucial. This includes maintaining a robust incident response plan that can be activated swiftly in case of a zero-day attack. Regularly updating and patching all network devices, even those not currently known to be vulnerable, can help close potential security gaps. Additionally, organizations should engage in proactive vulnerability research and collaborate with security researchers and industry peers to stay ahead of emerging threats.

Thirdly, implementing network segmentation and micro-segmentation can limit the impact of zero-day vulnerabilities by isolating critical systems and sensitive data from the rest of the network. This approach ensures that even if a zero-day vulnerability is exploited, the attack is contained and does not spread across the entire infrastructure. Regular security audits and penetration testing

of networking equipment can also help identify and address potential vulnerabilities before they can be exploited by attackers.

Remote Work Infrastructure

Transition to remote work, accelerated by global events like the COVID-19 pandemic, has introduced new vulnerabilities to the critical infrastructure in the Baltic Sea region. Remote work technologies, including virtual private networks (VPNs), remote desktop protocols (RDP), and cloud services, expand the attack surface, offering cybercriminals more opportunities to exploit weaknesses. Insecure home networks, personal devices, and inadequately protected remote access points can all serve as entry points for attackers. To protect remote work infrastructure, strong security measures, such as multi-factor authentication (MFA), must be implemented to ensure that only authorized users can access critical systems. Regular updates and patches for remote access technologies, using encrypted communication channels, and conducting security awareness training for remote employees are also vital steps. By reinforcing these security practices, organizations can mitigate the risks associated with remote work and safeguard their critical infrastructure from potential cyber threats.

Cyber attackers exploit vulnerabilities in tools like Atlassian Confluence and Citrix's NetScaler ADC to gain unauthorized access and potentially disrupt essential services and operations. Reliance on VPNs has become crucial for secure access to internal networks, but vulnerabilities within VPN technologies also present significant risks to organizations in the Baltic region. In February 2024, the Ivanti incident highlighted two zero-day vulnerabilities in Ivanti's Connect Secure and Ivanti Policy Secure products, identified as CVE-2023-46805 and CVE-2024-21887. These vulnerabilities exposed critical weaknesses in the security of VPN solutions allowing attackers to bypass authentication measures and execute malicious commands on the Ivanti VPN appliances. Exploiting CVE-2023-46805, attackers could sidestep the need for proper credentials to access restricted resources. Attackers executed specially crafted commands on compromised VPN appliances using CVE-2024-21887 and seized control of the systems.

A notable vulnerability, CVE-2024-20301, affects Cisco Duo Authentication for Windows Logon and RDP, allowing authenticated, physical attackers to bypass secondary authentication and gain unauthorized access to Windows devices. By exploiting the failure to invalidate locally created trusted sessions post-reboot, attackers can compromise devices with primary user credentials while circumventing permission requirements. Similarly, CVE-2023-36790 targets Windows RDP Encoder Mirror Driver, enabling attackers to elevate privileges and potentially access critical systems or data. Furthermore, CVE-2024-20337 exposes vulnerabilities in the SAML authentication process of Cisco Secure Client. Attackers can conduct carriage return line feed (CRLF) injection attacks, executing arbitrary script code in victims' browsers to access sensitive information, including valid SAML tokens. Leveraging these tokens, attackers can establish remote access VPN sessions with privileges of the affected users.

- **Ransomware Attacks Targeting Critical Infrastructure**

Prevalence of ransomware attacks, such as the ESXi ransomware campaign, poses a significant threat to the critical infrastructure in the Baltic Sea region. These attacks exploit vulnerabilities in critical systems, leading to data encryption and monetary loss. Proliferation of Ransomware-as-a-Service (RaaS) models presents a significant threat to critical infrastructure. These models empower less sophisticated cybercriminals with access to sophisticated attack tools thus broadening the pool of potential attackers. The recent cyberattack on Change Healthcare, a major healthcare technology provider in the United States, exemplifies the catastrophic consequences of RaaS attacks on critical infrastructure.

A successful attack on a provider can trigger cascading effects, potentially paralyzing infrastructure across region. This reality was vividly illustrated in the May 2023 cyberattack on MOVEit transfer software orchestrated by the notorious CL0P ransomware group. In one of the most far-reaching attacks the CL0P ransomware group exploited a previously unknown SQL injection vulnerability (CVE-2023-34362) in the MOVEit transfer software. A 2023 Survey of cybersecurity professionals from organizations worldwide revealed that 36% of the organizations suffered ransomware attacks because of exploited vulnerabilities. Credential compromise was the second most common cause of successful ransomware attacks, while malicious e-mail ranked third. Against the backdrop of geopolitical tensions, the spectre of cyberattacks targeting critical infrastructure looms large. Latvian officials are expressing fear of increased cyberattacks on their energy sector and critical infrastructure, especially considering the war in Ukraine and potential spillover effects.
In conclusion, ransomware attacks are here to stay and threat actors are continuously working on making ransomware more sophisticated and impactful, so it is crucial to take steps to protect your infrastructure. Protecting infrastructure from ransomware attacks requires thorough planning and a multi-layer approach in preventive, detective, and responsive measures.

5.4. Key Threat Actors

This section aims to identify key cyber security threat vectors and actors targeting critical infrastructure in the Baltic Sea region, providing insights into the tactics, techniques, and procedures employed by threat actors as well as comparing with threat actor activities in Ukraine.

Baltic Sea region	Ukraine
NoName057(16)	**Gamaredon**
Attack Types	
Distributed Denial of Service (DDoS), website defacement	Cyber espionage, data theft
Targeted Sectors	
Various sectors, often focusing on political targets	Ukrainian government, military organizations

Notable Events	
Numerous DDoS attacks on government and private sector websites	Persistent attacks on Ukrainian government entities since 2013
Trends & Predictions	
Continued use of DDoS attacks to disrupt services, Potential for more sophisticated defacement tactics	Continued cyber espionage efforts
TTPs	
T1071.001: Application Layer Protocol: Web Protocols, T1499: Endpoint Denial of Service	T1059: Command and Scripting Interpreter, T1071.001: Application Layer Protocol: Web Protocols
Ghostwriter	**APT28**
Attack Types	
Cyber espionage, support of disinformation actions	Cyber espionage, data theft, support of information actions and operations
Targeted Sectors	
Media organizations, government entities	Government agencies, media organizations
Notable Events	
Influence operations targeting elections in European countries	In July 2022, Fancy Bear exploited a Microsoft zero-day vulnerability targeting the Ukrainians. Phishing campaigns in 2024 targeted NGOs in Europe, the South Caucasus, Central Asia, and the Americas. Persistent attacks on Ukrainian government entities continue since 2013
Trends & Predictions	
Increased use of social media for disinformation, targeting upcoming European elections	Increased targeting of election systems, continued cyber espionage efforts
TTPs	
T1071.001: Application Layer Protocol: Web Protocols, T1566.002: Phishing: Spear phishing Link	T1059: Command and Scripting Interpreter, T1071.001: Application Layer Protocol: Web Protocols
Cyber Army of Russia Reborn	**Sandworm**
Attack Types	
DDoS attacks, cyber espionage	Cyber espionage, Destructive attacks, support of InfoOps and PSYOPs

Targeted Sectors	
Government agencies, military organizations	Military, government entities, energy, Telecommunications
Notable Events	
Attacks on NATO websites and critical infrastructure	In April 2022, Sandworm attempted a blackout in Ukraine using Industroyer2. Cyberattacks on Ukrainian power grids and critical infrastructure in 2023-2024
Trends & Predictions	
Increased coordination with state-sponsored activities, enhanced capabilities for espionage and disruption	Continued targeting of critical infrastructure, increasing use of wiper malware
TTPs	
T1071.001: Application Layer Protocol: Web Protocols, T1499: Endpoint Denial of Service	T1485: Data Destruction, T1071.001: Application Layer Protocol: Web Protocols
Killnet 2.0	**UAC-0050**
Attack Types	
Distributed Denial of Service (DDoS), website defacement	Data theft, cyber espionage
Targeted Sectors	
Government agencies, financial institutions, healthcare organizations	Ukrainian government, Critical infrastructure
Notable Events	
Attack on Lithuanian government websites in 2022	Cyberattacks on Ukrainian critical infrastructure in 2023-2024
Trends & Predictions	
Increased frequency of DDoS attacks, Targeting critical infrastructure in NATO countries	Continued focus on disrupting Ukrainian operations, potential expansion to other Eastern European targets
TTPs	
T1071.001: Application Layer Protocol: Web Protocols, T1499: Endpoint Denial of Service	T1059: Command and Scripting Interpreter, T1071.001: Application Layer Protocol: Web Protocols
Rhysida	**UAC-0006**
Attack Types	
Ransomware attacks, data exfiltration	Ransomware attacks, data exfiltration

Targeted Sectors	
Healthcare, education	Various sectors, with a focus on high-value targets
Notable Events	
Ransomware attack on a major hospital in 2023, attacks on one of Lithuania's universities in 2023	Ransomware attacks on Ukrainian enterprises in 2023-2024
Trends & Predictions	
Increasing sophistication of ransomware payloads, expansion to other critical sectors	Increased sophistication and targeting of critical infrastructure, potential collaboration with other threat actors
TTPs	
T1486: Data Encrypted for Impact, T1071.001: Application Layer Protocol: Web Protocols	T1569.002: System Services: Service Execution, T1499: Endpoint Denial of Service, T1486: Data Encrypted for Impact, T1071.001: Application Layer Protocol: Web Protocols
Inc. Ransom	**Lazarus Group**
Attack Types	
Ransomware attacks, double extortion (encrypting and threatening to release data)	Cyber espionage, financial theft, ransomware
Targeted Sectors	
Small to medium-sized enterprises, critical infrastructure	Financial institutions, defence contractors, government agencies
Notable Events	
High-profile ransomware attack on a logistics company in 2022	2014 Sony Pictures hack, 2017 WannaCry ransomware attack. In March 2022, Lazarus Group stole $600 million from the Ronin Network
Trends & Predictions	
Growth in ransomware-as-a-service (RaaS) offerings, increasing ransom demands	Continued focus on financial gains, increasing use of cryptocurrency theft
TTPs	
T1486: Data Encrypted for Impact, T1078: Valid Accounts	T1059: Command and Scripting Interpreter, T1071.001: Application Layer Protocol: Web Protocols

Table 1. Key threat actors in the Baltic Sea region versus Ukraine.

5.5. Key Attacks Against Critical Infrastructure Sector

Critical infrastructure in the Baltic Sea Region is permanently under threat from cybercrimes advancing in complexity and based on reporting done by CTAC in the second half of 2023 and first half of 2024, the number of attacks are increasing on a regular basis (328 in 2023 and 475 in 2024). Below is comparison of attacks throughout 2023 and 2024. Based on these attacks, it can ne seem that the number of them has increased and will continue to increase throughout 2024. Looking into specific types of attacks, it is noticeable that the four most common types of attacks (website defacement, remote code execution, denial of service and phishing) remain the same with slight changes in the number in observed count.

These threats focus on the main sectors of energy, transportation, and communication. Not only does it have strategic importance, but it is also very closely interlinked, making it a high-profile target for several types of threat actors. These acts of cybercrime may have massive implications: if, for instance, an attack is launched and is successful, it will potentially disrupt critical services, cause economic losses, or even threaten national security. Moreover, the infrastructures in the region are not independent; therefore, if a cyberattack on one country proves to be a success, that may spell something like other neighbouring countries. What further complicates the threat landscape is this geopolitical tension in the region: state-sponsored actors can well carry out cyber operations to achieve influence and, in an extreme case, to cause instability.

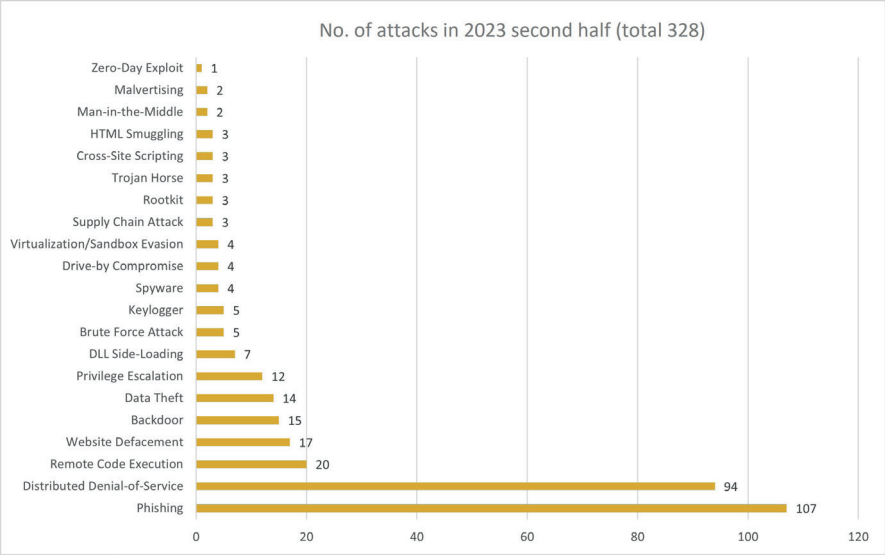


Figure 3. Number of attacks in 2023 second half (based on reporting done by CTAC)

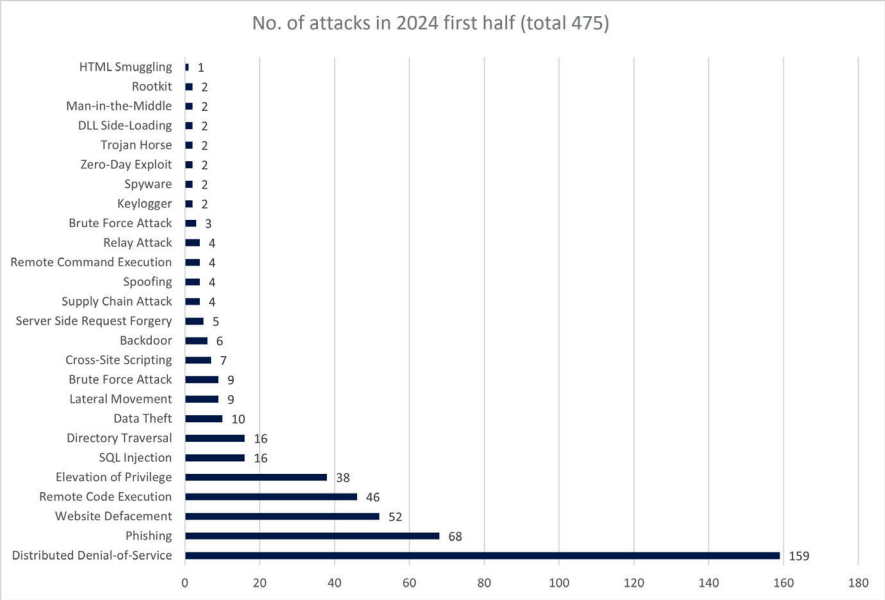


Figure 4. Number of attacks in 2024 first half (based on reporting done by CTAC)

5.6. Role of CTI in Protecting Critical Infrastructure

Cyber threat intelligence (CTI) collection and analysis are critical components of a proactive defence measure. Dedicated teams working on this field can provide crucial information about threats, active vulnerabilities, and attackers motivations. This valuable intelligence can help mitigate threats. Despite some countries are still new in this field, CTI has been mentioned as early as 2004. However, to provide quality products, many steps are needed to be taken first. Starting with CTI cycle, it is crucial to understand the benefits of your work, the products you are creating, and the maturity of your organization in terms of CTI.

It is particularly important to understand that in general CTI is a complex task requiring both human resources and specific tools to achieve it. Not all critical infrastructure subjects are able to afford these services at the top level. More mature organizations can have a dedicated CTI team to fulfil its threat intelligence needs, however others can rely on national cyber security authorities like NCSCs and request it to assist the organization with CTI requests. In general, critical infrastructure subjects must understand that it is advisable not to ignore CTI power in mitigating threats.

RCDC CTAC started doing daily cyber threat intelligence reports or CTIREPS on September 2023 each day to improve critical infrastructure subjects' and the member nations of RCDC cyber security posture and provide broader view on cyber threat landscape. Reports are aimed to provide general information daily for a particular sector. Early warnings of DDoS attacks, constant social media or dark web monitoring are just the part of these reports.

6. Correlation to the Situation with Other Regions

When protecting critical infrastructure, one of key components is collaboration. It is important to keep up with other critical infrastructure stakeholders both in different sectors and regions. Knowing what other sectors and regions are facing allows to draw the bigger picture, better understand the adversary and prepare for the future risks.

The table below provides a comparative overview of cyber threats faced by four key regions: the Baltic Sea region, Western Europe/North America, the Asia-Pacific, and Ukraine. While these regions contend with distinct geopolitical and infrastructural challenges, they share several common cyber threat vectors, such as DDoS attacks, phishing, and various forms of malware. The primary aggressors vary by region, with Russia, China, and state-sponsored groups frequently involved. Despite these differences, there are notable overlaps in the tactics used, the critical sectors targeted, and the motives behind these cyberattacks, reflecting the global nature of the cybersecurity landscape.

	Baltic Sea region	Western Europe/ North America	Asia-Pacific	Ukraine
Threat vectors	DDoS attacks, phishing, software vulnerabilities	DDoS attacks, phishing, ransomware	DDoS attacks, phishing, ransomware	DDoS attacks, phishing, malware
Targeting countries (primary)	Russia	Russia/China	China	Russia
Targeting countries/groups (general)	Russia, pro-Kremlin groups, ransomware gangs	Big4 (Russia, China, North Korea, Iran)	China, state-sponsored actors (Lazarus Group, Sandworm)	Russia, pro-Kremlin groups
Targeted critical infrastructure sectors	Energy, finance, government	Finance, healthcare, government	Healthcare, finance, technology	Energy, government
Common threat actors	Pro-Kremlin hacker groups, ransomware gangs	State-sponsored actors, ransomware gangs	State-sponsored actors (Lazarus Group, Sandworm), ransomware gangs (LockBit 3.0, ALPHV, CL0P)	Pro-Kremlin hacker groups

Common tactics and techniques	DDoS, phishing, software exploits	DDoS, phishing, ransomware, zero-day exploits	DDoS, phishing, double extortion, zero-day exploits	DDoS, phishing, malware
Motives behind attacks	Geopolitical influence, financial gain	Financial gain, geopolitical influence, ideological agendas	Financial gain, geopolitical influence, espionage	Geopolitical influence, financial gain
Key similarities with other regions	Like the Indo-Pacific in terms of attack vectors and threat actors	Overlaps with both the Baltic Sea region and the Indo-Pacific in terms of threat actors and tactics	Like the Baltic Sea region in terms of threat vectors and threat actors	Like the Baltic Sea region in terms if in pro-Kremlin hacker activities

Table 2. Overview of cyber threat landscape across different regions.

6.1. Western Europe and North America Region

In the Baltic Sea region, the sources of cyber threats originate from Russian APT groups and hacktivists. They engage in cyber espionage to achieve strategic, economic, and political gains, and the region is witnessing a steady rise in frequency, particularly with geopolitical issues flaring up. The primary interests in most cases are destabilization and intelligence gathering, and Russia's cyber-operations - against governments networks, critical infrastructure, and private sector entities - are executed using advanced methods.

In contrast, the threats posed by state-sponsored hackers in Western Europe and North America are more diverse. Apart from the Russian APT groups, their cyber operatives are also targeted by the Iranian, Chinese, and North Korean operatives. These threats vary in aspiration and methodology and the threat landscape is a surprisingly complex one. For example, China is actively sponsoring intellectual property theft to erase the technology barriers hindering individuals in climbing the technological advancement ladder. Their forceful methodology has motivated or forced the Chinese cyber actors to compete with Western corporations seeking such intelligence. In contrast, Iran has resorted to launching destructive attacks, most of which have affected critical infrastructures, while North Korean operatives conduct operations driven by financial motives to evade international sanctions and generate cash.

Of interest to state-sponsored hackers in Western Europe and North America are the finance and healthcare sectors. Financial organizations have been targeted by cybercriminals seeking to create prospects for high financial returns. They deploy ransomware, business email compromise, and spear-phishing techniques against organizations to hijack computer systems and reap hefty

amounts of ransom money from the victims. For example, in 2021, the U.S. witnessed a cyber-infrastructural attack in which the Colonial Pipeline ransomware attack seriously crippled the fuel infrastructural supply chain. The increasingly sensitive data handled makes health organizations even more vulnerable. The COVID-19 pandemic brought great chaos to the world and more opportunity for cyberattacks. Healthcare facilities with clinical data have become an attractive prey. For example, a ransomware attack on a hospital can disrupt provision of critical medical services, potentially leading to the loss of patient lives and data.

The types of attacks in this region markedly differ from those in the Baltics. The Baltic Sea region is more often targeted by Distributed Denial of Service (DDoS) attacks, malware, and phishing activities. DDoS attacks are a generic form of attacks in this region, for example, DDoS incidents have led to significant interruptions in online services. DDoS attacks flood the traffic inbound to online service servers, thus making them slow and not easily accessible. Malware that includes spyware and Trojans is also placed in the victim systems to enable continuous data extraction. Phishing activities, mostly through misleading emails or pages, are aimed at spanning sensitive information, such as login credentials or financial information.

On the other hand, Western Europe and North America are two other common victims of ransomware attacks. Such attacks encrypt victim data and seek a ransom payment to release the information. Organizations are rich and data-dependent, which is the incentive of the attacks, like in the notorious WannaCry attack which happened in 2017 and impacted the UK National Health Service and many other global organizations. The root of ransomware attacks is very deep; the monetary loss they cause is tremendous and it even ruins the operation and reputation of organizations. The cyber actors emanating from the different regions are becoming advanced and use advanced approaches to ensure their actions remain undetected and have maximum impacts. The approach of double extortion which involves attacking networks of organizations with data encryption and ransom notes has been growing common. This puts more pressure on the victim to pay the ransom because publication of the data, which is usually sensitive, may attract heavy fines for breach of regulations and laws, as well as damage to reputation. The cyber landscape in this regard also requires a comprehensive and adaptive strategy for cybersecurity measures within organizational setups from entities in the target regions. Thus, investments in advanced threat detection and response capabilities, employee training, and incident response plans are fundamental. Collaborative efforts between government agencies and the private sector are also important in combating such threats. Sharing initiatives in the United States, for example – partnership programs led by the Cybersecurity and Infrastructure Security Agency (CISA) – make a critical contribution to strengthening collective defence.

6.2. Indo-Pacific Region

The Indo-Pacific Region is characterized by diverse economies and extensive critical infrastructure networks making it a prime target for cyber threats. Like the Baltic Sea region, this region has seen various cyberattacks on critical infrastructure sectors. In the previous RCDC study "How to recognize China Cyber Threats" it was stated that the country is rapidly growing as one of the primary sources of malicious cyber activity. Ransomware gangs like LockBit 3.0, ALPHV, and CL0P have been active in targeting organizations across the region, including healthcare, finance, and technology sectors. These groups employ such tactics as double extortion and zero-day exploits to maximize the impact of their attacks and extort victims for financial gain.

State-sponsored threat actors, such as the Lazarus Group and Sandworm, have also been identified in the Indo-Pacific region conducting cyber operations against financial institutions, government organizations, and critical infrastructure. Their sophisticated malware and reconnaissance techniques pose significant threats to the security and stability of critical infrastructure networks.

Despite being geographically distant, there are notable similarities in the cyber threat landscape between the Baltic Sea region and the Indo-Pacific Region. Both regions experience attacks from pro-Kremlin hacker groups, ransomware gangs, and state-sponsored threat actors targeting critical infrastructure sectors.

Furthermore, common tactics and techniques, such as DDoS attacks, phishing campaigns, and exploitation of software vulnerabilities, are observed in cyberattacks across both regions. That indicates a correlation of strategies employed by cyber actors, regardless of geographical location.

Moreover, the motives behind cyberattacks in both regions often revolve around financial gain, geopolitical influence, or ideological agendas. Whether it is disrupting operations, stealing sensitive information, or causing reputational damage, cyber threats to critical infrastructure pose significant risks to the economic and national security of countries in both regions. The correlation between cyber threats to critical infrastructure in the Baltic Sea region and the Indo-Pacific Region underscores the global nature of cybersecurity challenges. As cyberattacks continue to evolve and become more sophisticated, cooperation and information sharing between nations is essential in strengthening cyber resilience and mitigating the risks to critical infrastructure. By understanding the commonalities and differences between cyber threats across regions, policymakers, cybersecurity professionals, and infrastructure operators can develop effective strategies to protect vital systems and safeguard national interests in an increasingly interconnected world.

7. Lessons from Ukraine: Enhancing Cyber Resilience

The ongoing aggression of the Russian Federation against Ukraine once again emphasizes the importance of the issue of cyber resilience of the national information and communication infrastructure, as well as the awareness of cybersecurity actors about the current cyber threat landscape. Russia's cyber actions against the Ukrainian digital infrastructure indicate that Russian cyberattacks, as well as conventional strikes, do not recognize any rules and norms of national or international humanitarian law. Infrastructure facilities of security and defence sector and critical infrastructure facilities are both under attack.

7.1. Infrastructure Evaluation and Vulnerability Identification

Cyberattacks on Ukraine's critical infrastructure is still a high priority for Russia's hacker groups, even as they focus on their "special military operation." These groups, linked to the GRU, are rather good at carrying out cunning and complicated cyber ops. Their main targets are the energy sector (like power grids and plants), big telecom providers like Kyivstar, important data centres like the Parkovy Data Center, and basic utilities like water and waste management.

They use a variety of techniques and tools to conduct their attacks, including wiper malware to delete data and repurposing legitimate tools like SDelete to cause damage. Sometimes they exploit vulnerabilities in public web services to get a foot in the door. When they do manage to break into a system, they usually rely on human error, like weak password policies, not having enough control over who can be an admin, and not having their networks properly segmented, to gain persistence. Even if they manage to get into a system, poorly configured SIEM systems can make it hard for defenders to spot them right away.

The tactics the hacker groups use can vary. For example, the Gamaredon group has been known to spread malware using USB drives. The Sandworm group, on the other hand, has been caught carrying out attacks that target both virtual and physical infrastructures at the same time. In December of 2023, they launched a two-stage attack on Kyivstar, hitting both their virtual and physical infrastructures. While the virtual side was successful (they got in and did some damage), the physical side did not go as well because the defenders were quick to react and there were internal issues. These attacks are not something that just happens overnight. They involve a lot of planning and reconnaissance, like figuring out what vulnerabilities are available, how to exploit them, and gathering of information across multiple intelligence sources, like HUMINT and OSINT. To defend against these threats, it is important to have strong password policies, properly segment networks, make sure SIEM systems are properly configured, train staff on cybersecurity best practices, and limit the use of removable devices.

Analysis of these destructive cyberattacks show that they often follow a five-stage scheme when targeting Ukraine's critical infrastructure. DDoS attacks are often used to distract the defenders making it hard for them to spot the real attacks. It is important to regularly monitor and diagnose software and hardware configurations for vulnerabilities to improve cyber resilience in critical infrastructure. In Ukraine, the USAID (*United States Agency for International Development*) has created a Cybersecurity Diagnostics Program to help operators of critical infrastructure do just that. This program provides preliminary assessments, helps them define their target states, and gives them detailed recommendations for improvement, followed by reassessments to make sure they are always getting better.



1 Living on the Edge	2 Living off the Land	3 Going for the GPO	4 Disrupt and Deny	5 Telegraphing "Success"
Leveraging compromised edge infrastructure to gain and regain entry into target networks	Using pre-existing tools for recon, lateral movement and information theft on target networks, aiming to evade detection	Creating persistent, privileged access from which wipers can be deployed using a tried-and-true script	Deploying "pure" wipers and disruptive tools to fit a variety of scenarios	Amplifying the narrative of successful disruption via hacktivist personas, regardless of the actual impact of the operation

Figure 5. Kill-chain of destructive cyberattacks against critical infrastructure in Ukraine

The overall vulnerability overview in Ukraine's critical infrastructure is no different from what the Baltic Sea region faces: heightened risk of DDoS attacks, exploitation of known vulnerabilities in both hardware and software, as well as zero-day exploits. Cyber espionage, where threat actors are gathering the necessary information for future attacks, is also on the list. The only difference on top of Ukraine being constantly faced with cyber threats to its critical infrastructure, the country is also fighting in a physical war against same enemy. A previous RCDC study researching the about lessons learned during the war in Ukraine showed a clear correlation pattern between kinetic and cyberattacks. This just proves that Ukraine is facing twice the threat, missiles and cyberattacks.

7.2. Case Studies and Success Stories

In the third year of the full-scale war, the Russian cyber activities remain the primary threat to Ukraine's cybersecurity and critical infrastructure. The Russian Federation's war of attrition ensures a continued high intensity of cyberattacks. According to CERT-UA, 1006 cyber incidents were recorded in the first quarter of this year alone, accounting for about 40% of all cyber incidents in 2023.

Among the autonomous systems that were most often targeted for attacks were: Google, Hurricane, Google-Cloud-Platform, Cloudflarenet and DigitalOcean-ASN.

The most common cybercriminals exploited harmful programs from the SmokeLoader, Agent Tesla, Snake Keylogger, Remcos and Formbook families.

This surge takes place as an effort of hacker groups to maintain, regain, or establish new unauthorized access points to critical automated systems. The historical impact of the Russian cyberattacks from 2014 to 2022 prompted Ukraine to develop stringent cyber defence requirements for critical infrastructure mandated by a 2019 Cabinet of Ministers' Resolution. These requirements align with global standards and are rigorously tested in Ukraine's unique conflict conditions. They include comprehensive information security policies, strict access management, user identification and authentication, event registration and audits, network protection, and stringent requirements for using removable devices, software, and hardware.

These measures have enabled Ukraine to defend against cyberattacks effectively. For instance, in March 2024, Ukraine thwarted a significant cyberattack by the Russian Sandworm group targeted at the energy, water, and heat supply sectors across ten regions. The attack involved sophisticated malware, like LOADGRIP and BIASBOAT, designed for Linux systems to control SCADA processes. Despite identifying compromised supply chains and vulnerabilities, CERT-UA noted issues like improper server segmentation and unpatched software, which facilitated the attack.

The Russian cyberattacks against the Ukrainian critical infrastructure are multifaceted and primarily aimed at disrupting or disabling information systems, as well as acquiring confidential data and supporting psychological operations. These attacks also aim to heighten public tensions already exacerbated by constant missile and air strikes. Latest trends show that the Russian hacker groups, controlled by special services, focus on telecommunications, electricity, and water supply facilities. Unlike in the previous years, there has been no recorded attacks on the transport sector since early 2023, due to the enhanced cyber defences and subsided civil transport activities. The capacity of the Russian Federation to execute complex cyberattacks remains robust, as evidenced by the new malware, AcidPour, used by the Sandworm group for targeting various network devices. Additionally, Russian hackers increasingly exploit legitimate services, such as Microsoft Graph API used by the APT28 group, for covert communication. Recent activities of the Gamaredon group suggest a return to older methods, like relying on the UltraVNC utility for remote access, thus highlighting their adaptability and persistence in cyber warfare.

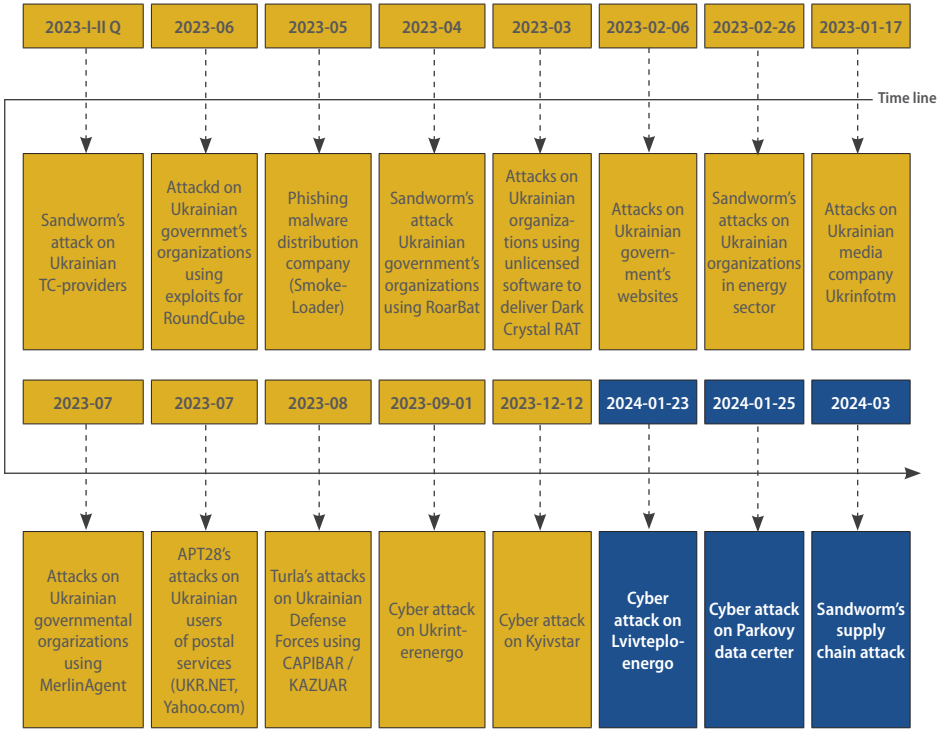


Figure 6. Timeline of major cyberattacks of 2023-2024

7.3. Enhancement Strategies (Lessons Learned)

In modern conditions, according to the experience of responding to the destructive Russian cyberattacks in 2022-2024, the following mandatory and additional technical cyber security enhancement measures for critical infrastructure facilities can be distinguished.

Mandatory cyber defence measures currently include:

- Network segmentation;
- Two-factor authentication (2FA) for all services at the perimeter;
- Protection of web resources using WAF (Web Application Firewall) type F5/Imperva;
- Complex passwords with a length of at least 10 characters;
- Active Directory (AD) updates to the latest version and upgrades of administrator workstations to Windows 11;

- Implementation of cloud EDR (Endpoint Detection and Response);
- Prohibition of storing passwords in files on computers;
- Ensuring that backups are physically isolated from the network.

Additional measures:

To increase cyber resilience of a critical infrastructure facility in the future, it is advisable to apply the following additional measures:

- **Monitoring and detection of anomalies:**
  - Using a behaviour analysis system and machine learning to detect anomalies;
  - SIEM (Security Information and Event Management) integration for log collection and analysis.
- **Multi-Layered Protection:**
  - Implementation of multi-level authentication (MFA);
  - VPN and encryption of your data.
- **Patch Updates & Management:**
  - Regular updates of software and systems to eliminate known vulnerabilities;
  - Automated patch management systems.
- **Incident Management and Response:**
  - Implementation of automated incident response systems (SOAR);
  - Development and testing of recovery plans after cyberattack.
- **Training & Awareness:**
  - Regular training of employees as the basics of cybersecurity measures;
  - Conducting simulations and training in cybersecurity.
- **Integration with Physical Security Measures:**
  - Physical protection of IT infrastructure;
  - Access control systems and video surveillance.
- **Threat Analysis and Risk Management:**
  - Threat Intelligence to predict and identify potential threats;
  - Regular analysis of risks and vulnerabilities.
- **DDoS Protection:**
  - Implementation of a system for protection against distributed denial-of-service attacks;
  - CDN and other technologies for load balancing.

- **Access Control and User Rights Management:**
  - Implementation of the principle of least privilege;
  - Regular audit of access rights and their updates.
- **Cooperation with relevant government agencies and partners:**
  - Sharing threat and incident information with government agencies and other companies;
  - Participation in industry forums and cybersecurity initiatives.
- **Development of a process for constant improvement of security systems:**
  - Regular simulations of cyberattacks;
  - Penetration testing (annually, after major configuration updates);
  - Regular competitions to improve the level of knowledge;
  - Annual events to improve knowledge.

In the context of the constantly growing potential of cyber threats and regular changes in their operational approach, the above measures will not provide to a critical infrastructure facility a 100% cyber protection of information and communication infrastructure, but they can significantly reduce the risk of successful intrusions and cyberattacks.

8. Mitigations and Recommendations for the Critical Infrastructure

The critical infrastructure sector is the backbone of a nation's security, economy, public health, and safety. Given the increasing sophistication of cyber threats and the potential for catastrophic consequences if these infrastructures are compromised, it is essential to adopt a comprehensive and proactive approach to security. The following recommendations are designed to enhance the resilience of critical infrastructure by focusing on robust training and education programs, fostering collaboration, and ensuring continuous improvement through regular evaluations and reporting.

1. IT/OT Collaboration

In critical infrastructure, the seamless integration of Operational Technology (OT) and Information Technology (IT) is vital for maintaining secure and reliable operations. However, collaboration between these domains can be challenging due to differing priorities and operational cultures. To bridge this gap, it is essential to foster a collaborative environment with joint teams that include both OT and IT experts, regular cross-functional training, and shared responsibility for security initiatives. By aligning their efforts, OT and IT teams can ensure that security measures are comprehensive and that operational disruptions are minimized. This constructive collaboration is crucial for protecting the integrity and continuity of critical infrastructure systems, which often rely on the seamless interaction between OT and IT components.

2. Diverse Training Topics

Given the complex and varied nature of critical infrastructure, training programs must cover a broad range of topics. These should include general cybersecurity principles, but more importantly, in-depth technical training tailored to the specific needs of OT environments. The training should address the unique security challenges associated with legacy systems, SCADA (Supervisory Control and Data Acquisition) networks, and other industrial control systems (ICS) that are often integral to critical infrastructure. Additionally, sector-specific scenarios-such as the protection of energy grids, water supply systems, or transportation networks-should be included to ensure that all participants are prepared to handle the threats relevant to their operational contexts.

3. Regular Exercises for Reinforcement

To maintain a prominent level of preparedness, it is essential to conduct regular, realistic exercises that simulate potential cyber-attacks or operational disruptions within critical infrastructure systems. These exercises should include discussion-based workshops and tabletop exercises involving multiple agencies and stakeholders. Additionally, full-scale drills that replicate real-world scenarios, such as coordinated cyber-attacks on power grids or communication networks, should

be organized. These simulations allow participants to practice their responses in a controlled environment, helping to identify and address any weaknesses in their current strategies. Regular exercises ensure that teams remain vigilant and can respond effectively to actual incidents, minimizing the risk of failures.

4. Fostering Collaboration and Trust

Effective collaboration and trust among various stakeholders are crucial for protecting critical infrastructure. Joint exercises not only reinforce training but also build the relationships necessary for coordinated responses during a crisis. By regularly engaging in these collaborative efforts, including both public and private sector participants, critical infrastructure entities can enhance their ability to communicate and cooperate during actual incidents. Trust and established communication channels are vital for ensuring a quick, coordinated response, especially when dealing with cross-sector dependencies and potential cascading effects that can arise during infrastructure failures.

5. Integration into Academic Curricula

To secure the future of critical infrastructure, it is important to integrate cybersecurity and resilience fundamentals into academic curricula, particularly for engineering, computer science, and emergency management programs. Educational institutions should offer specialized courses that focus on the unique challenges of securing OT environments, SCADA systems, and other critical infrastructure technologies. Training students in risk assessment, incident response, and infrastructure protection, along with advanced planning techniques and the understanding of risks, will prepare them to effectively protect and manage critical systems. By producing a workforce that is well-versed in both theoretical and practical aspects of infrastructure security, the sector can maintain resilience against emerging threats.

6. Periodic Evaluations of Program Effectiveness

The rapidly evolving threat landscape in critical infrastructure necessitates regular evaluations of training and security programs to ensure their continued effectiveness. Implementing consistent performance metrics, tailored specifically for OT and IT environments within critical infrastructure, allows for meaningful comparisons and customization of programs. These evaluations should document performance, identify gaps, and guide corrective actions, ensuring that the programs remain relevant and effective. Regular assessments help organizations adapt to new threats, technologies, and regulatory requirements, enhancing overall resilience.

7. Regular Performance Reporting

In the critical infrastructure sector, regular performance reporting is essential for maintaining a prominent level of cybersecurity readiness. These reports should document progress in implementing security measures, identify areas where improvements are needed, and track adjustments

made to enhance resilience against cyber threats. By maintaining transparency and accountability, organizations can better allocate resources, prioritize security initiatives, and share lessons learned with other stakeholders. Regular performance reporting also helps in aligning with regulatory requirements and standards specific to critical infrastructure, ensuring continuous improvement in security practices.

8. Data Collection and Analysis

Effective data collection and analysis are critical for understanding and mitigating risks in the critical infrastructure sector. Defined processes for data collection should focus on capturing relevant information specific to OT systems and ICS environments, where traditional IT-centric data may not provide a complete picture of the risks involved. Collaboration with government agencies and other stakeholders is essential to overcome challenges related to proprietary concerns and to facilitate the sharing of anonymized data. By analysing this data, organizations can identify trends, anticipate potential threats, and develop more effective, sector-specific defence strategies that enhance overall security and resilience.

Critical Infrastructure Protection & Resilience Cheat Sheet

- **IT/OT Collaboration:**
  - Foster seamless integration between Operational Technology (OT) and Information Technology (IT) through joint teams, cross-functional training, and shared security responsibilities to enhance critical infrastructure resilience.
- **Diverse Training Topics:**
  - Cover general cybersecurity principles and best practices.
  - Provide in-depth technical training tailored to the specific needs of the critical infrastructure sectors in a concrete region.
- **Regular Exercises for Reinforcement:**
  - Conduct discussion-based workshops and tabletop exercises involving multiple agencies.
  - Organize specific drills and full-scale exercises that simulate real events to enhance skills and preparedness.
- **Fostering Collaboration and Trust:**
  - Exercises to build relationships and improve coordinated responses during actual incidents.
- **Integration into Academic Curricula:**
  - Focus on cybersecurity and resilience fundamentals in college and university programs.
  - Training students in assessment techniques and education on infrastructure protection, advanced planning, and impact of cascading failures.

- **Periodic Evaluations of Program Effectiveness:**
  - Implementation of common and consistent performance metrics for comparison and customization.
  - Metrics for establishment of accountability, document performance, identify gaps, and guiding corrective actions.
- **Regular Performance Reporting:**
  - Document progress and adjustments necessary to improve resilience against cyber threats.
- **Data Collection and Analysis:**
  - Clearly defined processes for data collection and analysis.
  - Collaboration with government agencies to overcome challenges related to proprietary concerns.

Critical infrastructure stakeholders should implement these general recommendations to their cyber security ecosystem as it would benefit organisations cyber security posture. Keeping up with cyber trends, educating workers and performing reporting of systems is essential in keeping critical infrastructure safe and protected. That being said, there is no 100% fool-proof way of protecting from every threat. In the unfortunate event of compromise, organisations must make to recover from the incident. Please refer to Chapter 7 Lessons from Ukraine: Enhancing Cyber Resilience to better understand what steps organisation can make to recover and learn from occurring incidents.

9. Conclusions and Way Forward

The critical infrastructure in the Baltic Sea region is vulnerable to a variety of cyber threats, which are complicated by the region's geopolitical tensions. The growing digitization and automation within these critical infrastructure sectors, while enhancing efficiency and service delivery, also introduce new vulnerabilities that require robust cybersecurity measures. Specific challenges include securing legacy systems within these sectors, managing supply chain dependencies, and addressing human factors such as social engineering. The interconnected nature of critical infrastructure means that disruptions in one sector, such as energy or communications, can have cascading effects across others, underscoring the need for a holistic and coordinated approach to infrastructure protection. Additionally, these sectors face significant threats from advanced persistent threats, ransomware, and zero-day vulnerabilities.

To counter these threats and bolster the resilience and security of critical infrastructure in the Baltic Sea region, key steps include strengthening cybersecurity measures through advanced technologies and regular security assessments, fostering public-private collaboration for coordinated threat response, and addressing legacy systems by upgrading or isolating them. Enhancing employee training, improving incident response plans, mitigating supply chain risks. Additionally, prioritizing research and innovation to address emerging threats will further bolster global cyber resilience, emphasizing the necessity of a collaborative approach to safeguarding critical infrastructure.

The CTAC team's cyber threat reporting analysis highlights the crucial role of collaboration in safeguarding critical infrastructure across various regions. A comparative examination of the cyber threat landscape in the Baltic Sea region, Western Europe/North America, the Asia-Pacific, and Ukraine reveals that, despite geographical and geopolitical differences, these regions encounter similar cyber threats. These threats include DDoS attacks, phishing, ransomware, and other forms of malware, often driven by state-sponsored actors and ransomware groups. The globalized nature of these cyber challenges is evident, with consistent tactics, techniques, and motivations - such as financial gain, geopolitical influence, and ideological agendas - across different regions. The analysis also shows that while the specific sectors targeted may differ by region, critical infrastructure - such as energy, finance, healthcare, and government sectors - remains a key focus for cyber attackers.

To enhance the security of critical infrastructure worldwide, it is essential to strengthen international cooperation, develop region-specific cybersecurity strategies, and promote cross-sector collaboration. This includes sharing threat intelligence in real-time, conducting joint exercises, and investing in advanced cyber defence technologies like AI-driven threat detection. Continuous training and awareness programs tailored to regional needs are crucial, alongside coordinated incident response plans that enable swift, unified action across borders.

The conflict between Russia and Ukraine highlights the vital need for strong cyber resilience in national information and communication infrastructure. Russia's cyberattacks on Ukraine's critical systems demonstrate the brutal and law-defying nature of these operations, often ignoring both national and international legal frameworks. Assessments of Ukraine's infrastructure vulnerabilities reveal that the country is under constant and sophisticated cyber threats, particularly from state-sponsored hacker groups like Gamaredon and Sandworm, which have shown the capability to disrupt essential services such as energy, telecommunications, and water management. The similarities in vulnerabilities and threats between Ukraine and other regions, such as the Baltic Sea, emphasize the widespread challenges in protecting critical infrastructure from cyber threats. Ukraine's experience, especially during an ongoing physical conflict, offers valuable insights into modern cyber warfare, where both kinetic and cyberattacks often intersect, intensifying the overall threat landscape. The case studies provided in Chapter 7 demonstrate Ukraine's progress in strengthening its cybersecurity defences, as seen in its ability to fend off significant cyberattacks despite the ongoing conflict. The combination of mandatory and supplementary cybersecurity measures reflects a comprehensive approach to building cyber resilience. However, the ever-changing nature of cyber threats requires continuous adaptation and enhancement of defensive strategies.

Learning from Ukraine's experience it is important to point out that to enhance the resilience of critical infrastructure against cyber threats, it is essential to adopt a multi-faceted approach. Key strategies include strengthening infrastructure resilience through continuous monitoring and timely patch management, implementing multi-layered security measures such as network segmentation and isolated backups, and enhancing incident response capabilities with automated systems and regular simulations. Integrating physical and cybersecurity measures, leveraging advanced threat detection technologies, and continuously improving security systems are also crucial steps. While these measures will not guarantee absolute security, they significantly reduce the risk and impact of cyberattacks, thereby improving national infrastructure resilience against evolving threats.

In conclusion, cybersecurity of the critical infrastructures in the Baltic Sea region requires a comprehensive and coordinated approach. cyber resilience in the area can improve even further through a comprehensive approach with enhanced strategies, efficient coordination and information-sharing, collaboration with international partners, and adaptation to emerging threats. A secure cyber environment is a joint effort with state institutions, the private sector, and international partners at its advantage. Threats in cyber environment keep dynamically morphing and call for the critical regional infrastructures to maintain constant vigilance, use innovative solutions, and practice collaboration to keep the edge in prosperity and security.



REGIONAL CYBER DEFENCE CENTRE

Cyber Threats to Critical Infrastructure in the Baltic Sea Region