TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

ENGINEERING-ORIENTED CYBER RISK ASSESSMENT FRAMEWORK FOR CRITICAL ENERGY INFRASTRUCTURE: APPLICATION TO OFFSHORE AND PIPELINE SYSTEMS IN THE BLACK SEA REGION

Alexandru GEORGESCU, Carmen-Elena CÎRNU, Andreea DINU, Tina ANDOLJŠEK

Abstract: *Critical Energy Infrastructures (CEI) are complex cyber-physical systems integrating operational technology (OT) and information technology (IT) components whose disruption may generate severe operational, safety, environmental, and economic consequences. This paper develops a structured engineering-oriented framework for assessing cyber risks to CEI, grounded in industrial control system security principles and aligned with international standards such as IEC 62443 and NIST Cybersecurity Framework 2.0. The study applies a systematic review of recent cyber incidents (2023–2026) and organizes them into an engineering-based threat and vulnerability taxonomy. The framework is subsequently applied to two representative infrastructure types relevant to the Black Sea region: offshore oil and gas platforms and cross-border pipeline SCADA systems. The analysis identifies critical attack propagation paths between IT and OT layers, highlights vulnerabilities in supply-chain integration and remote access mechanisms and proposes technically grounded resilience measures. The paper moves beyond descriptive geopolitical analysis by providing a structured analytical model and operational recommendations applicable to engineering practice in the energy sector.*

Keywords: *Industrial Control Systems (ICS); SCADA security; cyber-physical systems; operational technology (OT); IEC 62443; resilience engineering; critical energy infrastructure; risk assessment*

1. INTRODUCTION

The Black Sea security environment is becoming increasingly complex and volatile, with critical implications for regional stability and infrastructure resilience. Critical Energy Infrastructure (CEI) forms the backbone of modern industrial societies. Electricity generation, oil and gas extraction, and energy transportation systems rely on tightly integrated cyber-physical architectures that combine Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) platforms, Programmable Logic Controllers (PLCs), and enterprise IT environments.

The increasing digitalization of energy systems, integration of remote monitoring, adoption of Industrial Internet of Things (IIoT) technologies, and expansion of cross-border energy networks have significantly enlarged the cyber-attack surface of CEI. Unlike traditional IT systems, CEI environments are characterized by legacy hardware constraints, long equipment lifecycles, safety-critical operations, and strict availability requirements.

Consequently, cyber incidents in such environments may lead not only to data loss but also to physical damage, environmental hazards, or large-scale service disruptions.

The Black Sea region represents a relevant case due to the coexistence of offshore extraction platforms, submarine energy assets, and transnational pipeline networks. However, existing literature often addresses these infrastructures primarily from strategic, policy, or geopolitical perspectives. There remains a need for an engineering-oriented analytical

approach that systematically evaluates cyber-physical risks at the architectural level.

This paper addresses that gap by developing a structured cyber risk assessment framework tailored to CEI environments.

The contribution of this work lies in: (1) developing a structured threat-vulnerability-impact categorization model; (2) applying the model to offshore and pipeline infrastructures relevant to the Black Sea region; (3) formulating operational resilience measures aligned with international engineering standards.

2. OVERVIEW OF CYBER THREATS TO CEI SYSTEMS

2.1 The increased urgency of the cyber threat to CEI systems

While this article's results are geared towards cyber resilience for CEI in the Black Sea region, the high level of interconnection between CEI within this region and beyond it make it a foregone conclusion to analyze the cyber threat environment in its entirety.

As of 2026, the energy sector is navigating a "polycrisis" where traditional cyberattacks are being amplified by artificial intelligence and escalating geopolitical friction. Beyond the foundational threats of ransomware and data breaches, new vectors specifically target the unique architecture of modern, decentralized grids. In recent years, the threat landscape for critical energy infrastructure has shifted from theoretical "pre-positioning" to active, destructive engagement. Recent events, such as the major coordinated strike on Poland's grid in late 2025, have provided specific blueprints for how modern energy systems are being targeted.

Key statistics from 2024 and 2025 reveal that CEI has become one of the most targeted sectors globally. The landscape is characterized by a sharp rise in the frequency of attacks, an increase in destructive wiper malware, and a growing financial burden for utility operators. Ransomware has shifted from a data-theft tool to an operational weapon. Key statistics are presented in Table 1.

Table 1

Key statistics regarding cyber-attacks on CEI

Datacategory	Key statistics
Frequency and Volume of Attacks	70% Increase in the US: In 2024, the United States saw a 70% hike in cyberattacks on utilities compared to 2023 [1][26]. 1,000 Attempts Per Day: Renewable energy companies in the UK reportedly faced approximately 1,000 attempted cyberattacks every single day throughout 2024. Doubling in Europe: Between 2020 and 2022, cyberattacks on the European power sector doubled, with 48 successful major attacks hitting EU energy infrastructure in 2022 alone [2].
Ransomware and Data Encryption	67% Victimization Rate: Approximately 67% of energy, oil, and gas organizations reported being hit by ransomware in 2024. [28] High Encryption Success: 80% of ransomware attacks on energy firms resulted in successful data encryption, significantly higher than the cross-sector average of 70% [3] Backup Compromise: In an alarming trend, 98% of attackers attempted to compromise the victim's backups during the assault, with a 79% success rate, which is the highest of any industry [3].
Financial and Operational Impact	Recovery Costs: The mean cost for an energy organization to recover from a ransomware attack in 2024 was $3.12 million. [28] Global Cybercrime Costs: Estimates suggest global cybercrime will cost the world $10.5 trillion annually by 2025, with the energy sector bearing a disproportionate share of the business interruption costs [4]. Device Impact: On average, 62% of a utility's computers are impacted during a successful ransomware attack, compared to a 49% average in other sectors.
Vulnerability and Workforce Trends	Rapidly Expanding Attack Surface: Susceptible points on the global electrical grid are estimated to grow by 60 new points per day as smart meters and IoT devices are integrated. [5] Talent Shortage: Despite 75% of the industry utilizing Generative AI for defense, there remains a 42% shortfall in cybersecurity personnel within the energy sector. [6] Human Element: Approximately 68% of successful breaches in the sector involved a human element, such as falling for a spear-phishing link [7].

2.2 Cyber Threats to CEI

Table 2 presents in a synthetic manner the main threat categories to CEI. In addition to these, we emphasize the following emerging issues facing CEI:

- AI-Driven Autonomous Attacks – threat actors are now using agentic AI to conduct rapid, automated reconnaissance of power grid protocols. These AI agents can identify zero-day vulnerabilities in Programmable Logic Controllers (PLCs) and adjust their payloads in real-time to bypass traditional behavior-based security [8]. The gap between disclosure and weaponization has shrunk to minutes in 2026 due to the use of autonomous AI agents. Adversaries use Large Language Models (LLMs) to reverse-engineer software patches for Industrial Control Systems (ICS) almost as soon as they are released. This creates an environment of perpetual zero-days, where utilities cannot patch legacy hardware fast enough to stay ahead of automated exploit generators
- Synthetic Insider Threats – using deepfake audio and video (vishing), attackers impersonate high-level grid engineers or executives to authorize malicious firmware updates or provide emergency access to restricted network segments [9].
- Cognitive and Disinformation Attacks – malicious actors spread AI-generated disinformation regarding grid stability or impending blackouts to trigger panic-buying or mass changes in consumer energy consumption, which can physically destabilize the grid's load balance [10] [25].
- Convergence of IT/OT and Legacy Vulnerabilities – the rapid digitalization of smart grids connects legacy equipment, never designed for internet connectivity, to modern software. This creates security gaps that allow attackers to jump from corporate email systems to physical grid controllers. Attackers exploit unpatched legacy hardware that cannot handle modern encryption or authentication. The U.S. Department of Energy (DOE) and NERC warn that electrical networks are gaining approximately 60 new susceptible points per day as smart meters and IoT devices are added.

Table 2

Main threat categories to CEI

Threat Category	Key Mechanisms	Potential Impact
Advanced Persistent Threats (APTs)	Spear-phishing, long-term infiltration, credential theft.	Long-term surveillance or automated manipulation of grid protocols (e.g., Industroyer) [11].
Ransomware	Data encryption of IT/OT systems, extortion via Ransomware-as-a-Service (RaaS).	Shutdown of critical supply chains and significant financial losses (e.g., Colonial Pipeline) [12] (Canadian Centre for Cyber Security, 2024).
Denial of Service (DoS/DDoS)	Flooding communication protocols (Modbus, DNP3) or jamming wireless signals.	Loss of situational awareness for grid operators, leading to instability or blackouts [11].
Cyber-Physical Attacks	Manipulation of Safety Instrumented Systems (SIS) or PLC firmware.	Physical damage to hardware, risk of explosions, or environmental disasters (e.g., Triton/Trisis) [13].
Supply Chain & Hybrid Threats	Compromised third-party vendors, poisoned hardware/firmware, economic coercion.	Systemic vulnerabilities across borders; difficulty in verifying the integrity of foreign-made equipment [14].

2.3 Main Malware Threats to CEI

As of 2026, the energy sector is facing a new generation of high-impact malware and ransomware. Recent intelligence from late 2025 and early 2026 highlights a shift toward purely destructive payloads (wipers) and agentic AI tools that automate the identification of vulnerabilities in industrial control systems.

2.3.1 Destructive Wiper Strains (State-Aligned)

Wipers are becoming a preferred tool for geopolitical sabotage, designed not to extort money, but to permanently destroy operational data and render industrial hardware inoperable.

DynoWiper was first detected in a coordinated strike against over 30 wind and solar farms and a

large combined heat and power (CHP) plant in Poland in December 2025. The threat group ELECTRUM is linked to Sandworm which is identified as Unit 74455 of the GRU [27]. Unlike past attacks that targeted central control centers, this focused on the "distributed edge." Attackers exploited vulnerable perimeter devices (e.g., FortiGate firewalls) without multi-factor authentication to gain access to Remote Terminal Units (RTUs) and Smart Inverters. The new data-wiping malware is used to corrupt the firmware of Hitachi and Mikronika controllers, effectively destroying the communication links between wind/solar farms and the grid operator [14], [15].

LazyWiper is often deployed alongside DynoWiper. This strain is used as a secondary payload to ensure that even if the primary attack is mitigated, residual system files are corrupted, preventing rapid recovery of SCADA (Supervisory Control and Data Acquisition) systems.

2.3.2 Advanced Industrial Ransomware

New Ransomware-as-a-Service (RaaS) groups are increasingly recruiting specialists who understand industrial protocols like Modbus and DNP3.

One example is Sinobi which recently gained notoriety for targeting critical infrastructure, including a high-impact incident involving a Romanian energy provider in late December 2025. Unlike generic ransomware, Sinobi employs disciplined intrusions that map out a utility's internal network before triggering encryption, ensuring that both IT and OT backups are compromised.

Another is Qilin which was once a standard ransomware group. By 2025, it had evolved into a full-spectrum extortion provider. In early 2025, it was operationally adopted by North Korean state-sponsored actors (Moonstone Sleet) for geopolitical operations. It has been linked to the exploitation of zero-day vulnerabilities in FortiGate firewalls, frequently used to protect remote energy substations.

2.3.3 Specialized ICS/OT Malware

These are not ransomware as such and should be seen as surgical tools built to manipulate the physical behavior of energy assets. The best-known recent example is VoltRuptor, a malware is developed by the "Infrastructure Destruction Squad" and identified in early 2026. It features multi-protocol support specifically for power grid communications. It is capable of persistence (staying hidden for months) and has advanced anti-forensics features to hide its presence from security audits. VoltRuptor is designed to change setpoints in electricity distribution, potentially causing physical damage to transformers through induced overloads.

Lastly, FrostyGoop (and others such as Pipe Dream) is a specialized ICS malware that targets the Modbus protocol directly. It has been used to shut down heating and cooling systems in municipal energy grids, causing physical pipes to freeze or crack during winter months.

3. KEY CYBERSECURITY FRAMEWORKS FOR CEI

This section provides cross-section of important governance frameworks for cybersecurity in the CEI sector, including mandatory legislation, industry standards and best practices. Table 3 summarizes this analysis.

Table 3

Selection of framework for the enhancement of the cyber resilience of CEI

Framework	Primary Target	Key Strength
NIST CSF 2.0	Boardroom/Governance	Flexibility; aligns security with business risk.
IEC 62443	Engineering/Plant Floor	Deep technical controls for physical hardware (OT).
C2M2	Program Managers	Measures "maturity" and guides budget priorities.
EU Network Code	Regulated Utilities	Ensures legal compliance for cross-border energy safety.
NERC CIP	Bulk Electric System in US	Standards CIP-002 through CIP-014 - physical security, electronic security perimeters, and "Supply Chain Risk Management."
NIS 2	Governance and Supply Chain	Cross-border cooperation

4. CASE STUDIES

This section applies the analytical framework introduced above to two representative types of Critical Energy Infrastructure relevant to the Black Sea region:

1. Offshore oil and gas extraction platforms
2. Cross-border natural gas pipeline systems

The objective is not to describe entire sectors in general terms, but to analyze representative cyber-physical architectures and identify concrete vulnerability patterns and risk propagation paths.

4.1 Oil and Gas Industry

In the oil and gas (O&G) sector, the air gap that once protected physical assets has effectively vanished. A typical offshore oil and gas installation in the Black Sea region integrates the following subsystems:

- Subsea control modules and blowout preventers
- Programmable Logic Controllers (PLCs) governing drilling operations
- Supervisory Control and Data Acquisition (SCADA) layer
- Satellite or microwave communication links
- Enterprise IT systems for logistics, billing, and data analytics.

These components form a layered cyber-physical system where operational technology (OT) interacts with enterprise IT environments. The increasing reliance on remote connectivity, Industrial Internet of Things (IIoT) devices, and digital monitoring platforms has significantly reduced the effectiveness of the traditional “air gap” model that once characterized offshore platforms. As of 2026, the industry faces a unique mix of new risks: aging legacy hardware, increased remote connectivity to offshore/remote sites, and high-value targets that attract both state-sponsored saboteurs and professional extortionists.

Among the specific threats to extraction and upstream operations, we find:

- Extraction sites, particularly offshore rigs (such as in the Black Sea) and remote wellheads, are increasingly vulnerable due to their reliance on satellite communications and the Industrial Internet of Things (IIoT).
- The firmware hijacking of subsea controllers for complex subsea manifolds and blowout preventers which are vital to modern extraction operations. Attackers target the Electronic Control Units (ECUs) and sensors that monitor pressure and flow. By injecting malicious firmware, attackers can manipulate sensor data to hide an imminent malfunction or pressure surge, potentially causing a catastrophic blowout or environmental disaster [16].
- The theft of seismic and reservoir data as a form of economic espionage. Upstream companies spend billions on proprietary seismic imaging. In 2024 and 2025, there was a recorded spike in silent intrusions targeting High-Performance Computing (HPC) clusters used for reservoir modeling. Groups like APT33 (linked to Iran) continue to focus on stealing this data to gain a competitive edge in global bidding wars [17].
- GNSS/GPS spoofing against dynamic positioning systems of offshore rigs which are used to stay over a wellhead. Recent research and real-world simulations have shown that attackers can spoof GNSS (Global Navigation Satellite System) signals, tricking the rig's thrusters into moving the vessel, which can snap subsea connections and cause massive spills [18].

Cybersecurity issues on the vendor side are among the most critical vulnerabilities for O&G CEI, especially offshore. The industry's reliance on a global web of specialized contractors, software providers, and equipment manufacturers creates numerous blind spots that state-sponsored actors and cybercriminals actively exploit, as seen table 4.

A) Third-Party Remote Access

O&G facilities rely on vendors for specialized maintenance. Vendors often require remote access to Supervisory Control and Data Acquisition (SCADA) systems to troubleshoot or update hardware. Vendors frequently set up unauthorized gateways or VPNs to simplify their work. These “shadow access points” often bypass the operator’s main security firewalls,

creating an unmonitored backdoor into the heart of the OT) network. Attackers often target the smaller, less-secure engineering firms that provide services to high level companies. By stealing a single technician's credentials, an attacker can gain legitimate, high-privileged access to dozens of different oil platforms or pipeline control centers. This vulnerability corresponds to a high exposure pathway between IT and OT zones under IEC 62443 segmentation principles.

B) Software Supply Chain Compromise

Modern O&G operations use specialized software for reservoir modeling, drilling automation, and pipeline monitoring. Attackers can use a sophisticated threat in the form of malicious updates, which represents the insertion of a backdoor into a legitimate software update from a trusted vendor. Because the software is trusted by the operator, the update is installed without scrutiny, granting attackers full access to the network (a strategy used in the SolarWinds and Stuxnet attacks). Another form of supply chain poisoning is through vulnerable component libraries, since vendors often build their software using open-source libraries. If these libraries contain zero-day vulnerabilities, every operator using that vendor's software becomes vulnerable simultaneously.

C) Hardware-Level Vulnerabilities

The hardware used in extraction and upstream processes is often manufactured in global regions with varying security standards. There is a growing concern regarding firmware tampering, an example of poisoned hardware, where malicious code is embedded into the firmware of a controller at the manufacturing plant before it is even shipped to the oil field. At the same time, many O&G assets use legacy hardware that is decades old. These devices often lack modern authentication or the ability to be patched. If a vendor stops supporting a piece of hardware, it becomes a perpetual vulnerability that cannot be easily secured without replacing the entire system.

Table 4

Types of vendor risk for the O&G sector

Vendor Risk Category	Specific Impact on O&G	Key Defense Mechanism
Remote Access	Unauthorized SCADA manipulation	Multi-Factor Authentication (MFA) & Session Logging
Software Supply Chain	Silent lateral movement	Software Bill of Materials (SBOM) & Sandboxing
Hardware Integrity	Physical equipment damage (blowouts)	Network Segmentation (IEC 62443)
Managed Services	Cascading data breaches	Rigorous Third-Party Risk Management (TPRM)

The interactions between different generations of hardware or of industrial control systems (analog to digital to interconnected) also generate new risks, vulnerabilities and threats.

D) Risks from Managed Service Providers (MSPs)

As O&G companies outsource their IT and cybersecurity operations to save costs, they become heavily dependent on MSPs, which is a form of single point of failure risk. An MSP manages the data and security for multiple energy clients. A breach at the MSP level can lead to a cascading effect, where an attacker can move laterally from the MSP's infrastructure into the private networks of several O&G companies at once. There are also issues related to espionage and, in a European context, data sovereignty. High-performance computing clusters used for reservoir modeling are often hosted by third-party cloud providers. This raises the risk of industrial espionage, where proprietary geological data is stolen to give competitors an advantage in global bidding wars.

From an architectural perspective, the most critical vulnerabilities in offshore systems include:

- Weak segmentation between enterprise IT and OT layers

- Excessive vendor access privileges
- Limited firmware validation mechanisms
- Dependency on satellite communications
- Legacy PLC authentication limitations

4.2 Cross-Border Pipeline SCADA Systems

A typical pipeline transmission system in the Black Sea region includes:

- Compressor stations
- PLC-controlled valve systems
- Remote Terminal Units (RTUs)
- Centralized SCADA monitoring
- Corporate IT integration

In accordance with IEC 62443, the system may be structured into:

- Zone 1: Corporate IT
- Zone 2: Supervisory SCADA
- Zone 3: Field control devices

Cyber risk primarily arises at the interfaces between these zones.

Pipelines are the most visible cyber-physical targets due to their geographical span and the precedent set by the Colonial Pipeline incident. We will mention three issues, but this is not an exhaustive list. The first is the growth of integrity-impact malware such as FrostyGoop and PipeDream. New malware families like FrostyGoop specifically target the Modbus protocol, which is the language used by pipeline pumps and valves. Unlike ransomware, which locks files, this malware directly interacts with the ICS to shut down heating or cooling systems, causing physical pipes to crack or seize [14].

The second is related to "living off the land" in SCADA systems. Groups like VOLTZITE have been found pre-positioning within the Supervisory Control and Data Acquisition systems of major pipeline operators. They use legitimate administrative tools (like PowerShell) to hide, ensuring they can remotely close valves or stop pumps during a geopolitical crisis without triggering standard antivirus alerts. State-sponsored actors (specifically Volt Typhoon from China) employ built-in network commands to blend in with normal traffic, instead of using identifiable malware. This allows them to maintain quiet access to systems for months or years. It had been noted before by the World Economic Forum that mean dwell times in European systems are over one hundred days, which is the time between penetration and detection. Their goal is not immediate theft but the ability to disrupt physical valves or circuit breakers during a future geopolitical conflict [19].

Lastly, we have the issue of Ransomware-as-a-Service (RaaS). In Q1 2025, ransomware attacks on industrial entities rose by 46%. Groups such as DragonForce and Cl0p target the billing and logistics side of pipelines. Even if the oil keeps flowing, the inability to track shipments or bill customers often forces a manual shutdown of the entire line [14], [20]. In 2024, ransomware attacks on energy and utilities reportedly increased by 80%, with attackers specifically targeting OT networks to halt production and force payouts. The World Economic Forum (WEF) Global Cybersecurity Outlook 2025 notes that ransomware is no longer random but a planned effort to disrupt vital infrastructure (e.g., the Halliburton breach in August 2024).

Table 5

Key frameworks for enhancing cyber resilience for pipelines

Framework	Primary Target	Key Strength
TSA Security Directive Pipeline-2021-01C	US Pipelines	Mandatory, pipeline operators strictly vet their third-party software and report vendor-related incidents.
API Standard 1164:	Global Pipelines/SCADA	Industry Standard, roadmap for O&G companies to integrate cybersecurity into their procurement processes.
OG-86	Offshore, SIS	Industry standard, mainly meant for inspectors and operators of major hazard sites.
DNV-RP-G108	Offshore/Upstream	Best Practice, IEC 62443 adaptation for OT and ICS in O&G.

The pipeline industry follows specialized frameworks that go beyond general IT security and are summarized in Table 5. The pipeline case reveals three dominant structural weaknesses:

1. Insufficient IT/OT segmentation

2. Remote telemetry exposure
3. Backup and recovery system compromise

5. ENGINEERING-ORIENTED RECOMMENDATIONS FOR ENHANCING CEI RESILIENCE

The measures below directly address the dominant risk propagation paths observed at IT/OT convergence points, vendor interfaces, and supply-chain dependencies. They are structured as operational engineering actions rather than general policy guidance.

5.1 Addressing vendor-side risks

Both case studies identified vendor remote access and supply-chain exposure as primary cyber-physical risk vectors. The traditional trust-based relationship between operators and suppliers must be replaced by verifiable, technically enforced controls.

CEI operators should implement the following measures:

- Strict vetting of third-party software and service providers, in line with TSA Security Directive Pipeline-2021-01C, which requires pipeline operators to report vendor-related cybersecurity incidents and validate third-party security controls [21].
- Integration of cybersecurity requirements into procurement processes, consistent with API Standard 1164, ensuring that secure software development practices, update validation procedures, and vulnerability disclosure obligations are contractually binding [22].
- Mandatory multi-factor authentication (MFA) for all remote vendor access sessions.
- Time-bound and role-based access control following least-privilege principles.
- Continuous session logging and real-time monitoring of vendor interventions.
- Elimination of unauthorized “shadow” VPN gateways or unmanaged remote access paths.
- Implementation of Zero-Trust Architecture principles, where identity verification, device integrity checks, and contextual access control are enforced regardless of network location.

Additionally, operators should conduct periodic red-team or penetration-testing exercises simulating vendor compromise scenarios, including full SCADA loss conditions, as encouraged by multiple industrial frameworks.

5.2 Development of structured information-sharing mechanisms

The interdependence of CEI systems in the Black Sea region, including offshore platforms, cross-border pipelines, and emerging electricity interconnections (e.g., the undersea high-voltage cable projects linking Azerbaijan to Romania and the EU), necessitates structured information exchange.

Building upon the model of European Information Sharing and Analysis Centers (ISACs) and Cyber Hubs [30], regional CEI operators should:

- Establish sector-specific information-sharing mechanisms focusing on ICS/OT incidents.
- Develop standardized reporting templates for cyber-physical anomalies affecting energy assets.
- Facilitate cross-border exchange of anonymized threat intelligence among operators in EU and non-EU countries, including Turkey and Azerbaijan.
- Incorporate risk assessments for new infrastructure projects at the design stage, especially those involving submarine cables, renewable energy platforms, and thermal generation assets.

Such mechanisms reduce detection latency and support coordinated mitigation of systemic threats affecting interconnected infrastructures.

5.3 Structured adoption of recognized cybersecurity frameworks

The analysis demonstrated that inconsistent implementation of established standards contributes to segmentation weaknesses and inadequate incident response preparedness.

Black Sea CEI operators should:

- Align organizational cybersecurity strategies with internationally recognized frameworks such as IEC 62443 for OT segmentation and NIST CSF 2.0 for enterprise risk governance.

- Clearly define IT and OT security responsibilities within organizational structures.
- Conduct periodic maturity assessments (e.g., aligned with C2M2 principles) to identify resilience gaps.
- Ensure that Safety Instrumented Systems (SIS) and critical control layers meet appropriate security levels under IEC 62443 (e.g., SL3 where feasible).

Adopting best practices must move beyond formal compliance toward measurable architectural hardening and technical validation [23].

5.4 Sustainable and controlled adoption of digital emerging technologies

The rapid adoption of AI, digital twins, and blockchain technologies in CEI environments introduces efficiency gains but also expands the attack surface [32].

Given the probabilistic and adaptive nature of AI systems [31], operators should implement structured validation and separation principles:

- Limit deployment of AI-driven tools within industrial control environments until adequate resilience testing and certification processes are established.
- Strictly separate enterprise AI applications (e.g., HR, billing, logistics automation) from safety-critical control networks to prevent cross-domain compromise [31].
- Conduct adversarial red-teaming exercises tailored to AI-enabled systems, recognizing that probabilistic behavior requires dynamic testing rather than static code audits [29].
- Validate AI systems within cyber-range environments prior to operational deployment.
- Explore defensive AI applications capable of detecting anomalous OT traffic patterns, identifying vulnerability exposures, and accelerating patch management [32].
- Develop long-term AI governance strategies integrated into broader cybersecurity roadmaps, including considerations for post-quantum cryptographic transition.

These measures address both the opportunity and risk dimensions of AI integration in CEI environments.

5.5 Development of specialized resilience infrastructure

The case studies highlight that static controls alone are insufficient against adaptive adversaries employing living-off-the-land techniques and ICS-specific malware.

To enhance systemic resilience, operators and regional authorities should:

- Develop and deploy sector-specific early warning mechanisms for OT anomalies.
- Establish federated cyber ranges dedicated to energy infrastructure simulation.
- Use cyber-range platforms to simulate:
  - Vendor compromise scenarios
  - Supply chain poisoning
  - SCADA manipulation
  - Total loss-of-control events
- Conduct joint cross-border exercises reflecting the interconnected nature of Black Sea CEI.

Federated cyber-range initiatives, such as the NATO Science for Peace and Security project referenced in this study, demonstrate the feasibility of structured simulation environments supporting scenario generation, contingency planning, and specialized training for both operators and public authorities.

Such infrastructures enable continuous testing of resilience assumptions under realistic cyber-physical stress conditions.

5.6 Priority engineering actions

Across offshore and pipeline systems, the most impactful resilience improvements concentrate on:

1. Architectural segmentation and IT/OT boundary enforcement
2. Vendor access control and supply chain validation
3. OT-aware monitoring and anomaly detection
4. Controlled and validated AI integration
5. Continuous simulation and training through cyber-range environments

These measures directly address the highest-impact vulnerability pathways identified in this study and provide a technically grounded roadmap for strengthening the cyber-physical resilience of CEI in the Black Sea region.

6. CONCLUSION

The Black Sea region is currently host to very strong hybrid threat campaigns, melding state actors and geopolitical interests with organized crime groups having profit and ideological motives. This hybrid threat landscape relies significantly on cyber-attacks as a high cost to benefit ratio attack option [24], leveraging structural, technological and governance vulnerabilities in critical infrastructures. This article analyzed the Critical Energy Infrastructures. It traced the principal elements of the cyber threat environment and the CEI susceptibility to these attacks, described the emerging threats and practices with a particular emphasis on the 2025-2026 period, that chronicled enduring changes to how cyber warfare is waged against CEI, and listed the main frameworks for improving cyber resilience both in Europe and the US (which serves as a source of best practices). Case studies on the oil and gas sector and on the pipelines were developed, which serve to emphasize the incredible diversity of CEI and, consequently, the diversity of the threats they face, Lastly, recommendations were developed, based on best practices elsewhere, to improve the cyber resilience of the CEI, including from the perspective of the inevitable implementation of digital emerging technologies such as AI in a utilitarian, defensive and offensive role. Due to limits in size and scope, the article did not provide a case study on the nuclear CEI which is quite relevant in regional security dynamics, though many of the findings are applicable to it as well. Another key omission, though it was hinted at in certain sections, is the role that disinformation, fake news and propaganda through the digital medium (including through the leveraging of AI deepfakes and personalized content generation) plays in the overall cyber threat environment. These can be considered future areas of research, alongside in-depth analyses of the implementation of the various recommendations such as the development of sustainable AI implementation strategies, the setting up of region ISACs for information sharing also with regional CEI beyond EU and NATO borders, as well as the setting up of federated cyber ranges to provide training for CEI personnel, as well as cyber defense planning and scenario generation. In the current cybersecurity environment, CEI operators and authorities are “condemned to cooperate” also in a crossborder setting.

7. ACKOWLEDGEMENT

This research was conducted with the support of the NATO Science for Peace and Security (SPS) Programme, project SPS G6313, “Cyber Polygon: A Cyber Range Platform Specialized on the Energy Sector with Automatic Generation of Virtual Scenarios.”

8. REFERENCES

[1] North, M. (2025). *Why the energy transition means more cyberattacks.* Mitsubishi Heavy Industries (MHI). Spectra. https://spectra.mhi.com/why-the-energy-transition-means-more-cyberattacks

[2] Eurelectrics. (2025) *Cybersecurity in the power sector*. https://www.eurelectric.org/in-detail/cybersecurity-in-th e-power-sector/

[3]. Sophos. (2025). The state of ransomware 2025. A Sophos Whitepaper. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

[4] eSentire. (2026). The Industrialization of Cybercrime: Identities are Under Attack 2025 Year in Review, 2026 Threat Landscape Outlook Report. https://www.esentire.com/resources/library/esentire-2026-annual-cyber-threat-report

[5] Lakshminarayana, S., Maple, C., Larkins, A., Flack, D., Few, C., David, K.-A., & Srivastava, A. K. (2023). Cybersecurity threats to power grid operations from the demand-side response ecosystem. arXiv. https://doi.org/10.48550/arxiv.2310.18820 [6] Global Security Forum. (2024). Cybersecurity Workforce Report: Bridging the W[orkforce Shortage and Skills Gap. https://gcforum.org/en/research-publications/cybersecurity-workforce-report-bridging-the-workforce-shortage-and-skills-gap/

[7] Verizon. (2024). 2024 data breach investigations report (DBIR). https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

[8] World Economic Forum. (2026). Global Cybersecurity Outlook 2026. https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[9] AON. (2026). Cyber 2026: Evolving Threats Demand Strategic Leadership. https://www.aon.com/en/insights/articles/cyber-2026-evolving-threats-demand-strategic-leadership

[10] NATO Scicence and Technology Organisation. (2025). Cognitive Warefare - NATO Chief Scientist Research Report. NATO Headquarters. Brussels. 2025. https://www.sto.nato.int/document/cognitive-warfare/

[11] ACM Computing surveys. (2016). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. DOI: 10.1145/2897166. https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures

[12] Government of Canada, Canadian Centre for Cyber Security. (2023). The cyber threat from supply chains. https://www.cyber.gc.ca/en/guidance/cyber-threat-supply-chains

[13] Amomo, C.G. (2023). Countering IoT-Based Cyber-Physical Manipulation: A Framework for National Resilience Against Systemic Disruption. International Journal of Scientific Research & Engineering Trends, 9(6), ISSN: 2395-566X, 2023.

[14] Dragos, Inc. (2026). DynoWiper: Analyzing the coordinated strike on Poland's energy grid. Dragos Industrial Cybersecurity. https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

[15] ESET. (2026). DynoWiper update: Technical analysis and attribution. https://www.welivesecurity.com/en/eset-research/dynowiper-update-technical-analysis-attribution/

[16] Walter, M., Vineetha Harish, A., Christison, L. (2025). Visualisation of cyber vulnerabilities in maritime human-autonomy teaming technology. WMU J Marit Affairs 24, 5–31, https://doi.org/10.1007/s13437-025-00362-z

[17] Hong, Y. (2023). Exclusive: Hackers behind cyberattack on Wuhan Earthquake Monitoring Center aim at stealing geological data: top cybersecurity expert. GlobalTimes, https://www.globaltimes.cn/page/202308/1295562.shtml

[18] ACM Computing surveys. (2016). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. DOI: 10.1145/2897166. https://www.researchgate.net/publication/301798786_A_Survey_and_Analysis_of_the_GNSS_Spoofing_Threat_and_Countermeasures

[19] CISA (2025). Joint Guidance: Identifying and Mitigating Living Off the Land Techniques. Cybersecurity and Infrastructure Security Agency, Washington DC, https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf

[20] Claroty. (2025). The Global State of CPS Security 2025: Navigating Risk in an Uncertain Economic Landscape. https://claroty.com/resources/reports/the-global-state-of-cps-security-2025-navigating-risk-in-an-uncertain-economic-landscape

[21] TSA (2024). Security Directive Pipeline-2021-0lC Enhancing Pipeline Cybersecurity. https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01c.pdf

[22] Department of Energy (2022). The API 1164 framework and cybersecurity considerations for pipeline transportation and storage. Technology Advancement and Deployment Task Group, Working Document of the NPC Study – Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation, Topic Paper #4-15, https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-15_FINAL.pdf

[23] Georgescu, A., Gurău, M.M., Bucovetchi, O. and Dinu, A. (2024) *The European Cybersecurity Framework for Critical Energy Infrastructures*, in Barichella, A. and Yada, J. (eds) The Palgrave Handbook of Cybersecurity, Technologies and Energy Transitions. Palgrave Studies in Energy Transitions. Cham: Palgrave Macmillan. Available at: https://doi.org/10.1007/978-3-031-04196-9_9-1

[24] Badea, M., Bucovețchi, O., Gheorghe, A. V., Hnatiuc, M., & Raicu, G. (2025). Maritime Industry Cybersecurity Threats in 2025: Advanced Persistent Threats (APTs), Hacktivism and Vulnerabilities. Logistics, 9(4), 178. https://doi.org/10.3390/logistics9040178

[25] Raman, G., AlShebli, B., Waniek, M., Rahwan, T., Peng, JC-H. (2020) *How weaponizing disinformation can bring down a city's power grid*. PLoS ONE 15(8): e0236517. https://doi.org/10.1371/journal.pone.0236517

[26] Kovanan, T., Nuojua, V., Lehto, M. (2019). Cyber Threat Landscape in Energy Sector Cyber Threat Landscape in Energy Sector. pp. - 353-

361. 13th International Conference on Cyber Warfare and Security, ICCWS2018, 8 - 9th March 2018, National Defense University, Washington DC, USA

[27] Republic of Poland, Ministry of Digital Affairs, CERT Polska, Energy Sector Incident Report – 29 December. https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[28] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

[29] Sambucci, L., Paraschiv, E.A. (2024). The Accelerated Integration of Artificial Intelligence Systems and Its Potential to Expand the Vulnerability of Critical Infrastructure. Romanian Journal of Information Technology and Automatic Control 34 (3): 131–148.

[30] Iancu, N., Gurău, M-M, Raicu, G., Cîmpineanu, M-J. (2025). *Building Europe's Civilian-Defence Cyber Resilience Through Expanding and Consolidating Networks: The ECYBRIDGE Experience*. International Journal of Cyber Diplomacy 6: 19–37. https://doi.org/10.54852/ijcd.v6y202502

[31] Hadji-Janev, M. (2021). *Hyper Threats to Critical Information Infrastructure: Bringing the AI in the Game*. International Journal of Cyber Diplomacy 2. https://ijcd.ici.ro/2021/hyper-threats-to-critical-information-infrastracture-bringing-the-ai-in-the-game/

[32] Dinu, A., Vasile, P-C, Georgescu, A. (2024). *AI-Driven Solutions for Cybersecurity: Comparative Analysis and Ethical Aspects*. Romanian Journal of Information Technology and Automatic Control 34 (3): 35–48

Cadru de evaluare a riscurilor cibernetice orientat spre inginerie pentru infrastructurile energetice critice: aplicare la sistemele offshore și de conducte din regiunea Mării Negre

Rezumat: Infrastructurile Energetice Critice (IEC) sunt sisteme ciber-fizice complexe care integrează componente de tehnologie operațională (OT) și tehnologia informației (IT), a căror perturbare poate genera consecințe grave la nivel operațional, de siguranță, de mediu și economice. Această lucrare dezvoltă un cadru structurat pentru evaluarea riscurilor cibernetice la adresa IEC, fundamentat pe principiile securității sistemelor de control industrial și aliniat la standardele internaționale precum IEC 62443 și NIST Cybersecurity Framework 2.0. Studiul este fundamentat pe incidente cibernetice recente (2023–2026) pe care le organizează într-o taxonomie a amenințărilor și vulnerabilităților. Ulterior, cadrul este aplicat la două tipuri de infrastructuri critice reprezentative pentru regiunea Mării Negre: platforme petroliere și de gaze offshore și sisteme SCADA pentru conducte transfrontaliere. Analiza identifică căi critice de propagare a atacurilor între straturile IT și OT, evidențiază vulnerabilități în integrarea lanțului de aprovizionare și în mecanismele de acces la distanță și propune măsuri de reziliență fundamentate tehnic. Lucrarea depășește analiza geopolitică descriptivă, oferind un model analitic structurat și recomandări operaționale aplicabile în practica inginerească din sectorul energetic.

Alexandru GEORGESCU, PhD, Established Researcher R3, The National Institute for Research and Development in Informatics – ICI Bucharest, alexandru.georgescu@ici.ro, +40 753 222 040, 8-10 Maresal Averescu Avenue, Bucharest, Romania

Carmen Elena CIRNU, PhD, Scientific Director, The National Institute for Research and Development in Informatics – ICI Bucharest, carmen.cirnu@ici.ro, +40 753 222 040, 8-10 Maresal Averescu Avenue, Bucharest, Romania

Andreea DINU, M.Sc., Head of Office, The National Institute for Research and Development in Informatics – ICI Bucharest, andreea.dinu@ici.ro, +40 753 222 040, 8-10 Maresal Averescu Avenue, Bucharest, Romania

Tina ANDOLJŠEK, LL.M., PhD Candidate, National University of Science and Technology Politehnica Bucharest, andoljsek.tina1@gmail.com, +40 214 029 465, 313 Splaiul Independenţei, Bucharest, Romania