I.J. Information Technology and Computer Science, **2024, 1, 43-53**
Published Online on February 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2024.01.05

Analysis of Threats and Cybersecurity in the Oil and Gas Sector within the Context of Critical Infrastructure

Shakir A. Mehdiyev*
Institute of Information Technology, Baku, Azerbaijan
E-mail: shakir.mehtieff@gmail.com
ORCID iD: https://orcid.org/0000-0003-4828-577
*Corresponding author

Mammad A. Hashimov
Institute of Information Technology, Baku, Azerbaijan
E-mail: mamedhashimov@gmail.com
ORCID iD: https://orcid.org/0000-0001-5982-8986

Received: 25 August 2023; Revised: 10 October 2023; Accepted: 01 December 2023; Published: 08 February 2024

Abstract: This article explores the multifaceted challenges inherent in ensuring the cybersecurity of critical infrastructures, i.e., a linchpin of modern society and the economy, spanning pivotal sectors such as energy, transportation, and finance. In the era of accelerating digitalization and escalating dependence on information technology, safeguarding these infrastructures against evolving cyber threats becomes not just crucial but imperative. The examination unfolds by dissecting the vulnerabilities that plague critical infrastructures, probing into the diverse spectrum of threats they confront in the contemporary cybersecurity landscape. Moreover, the article meticulously outlines innovative security strategies designed to fortify these vital systems against malicious intrusions. A distinctive aspect of this work is the nuanced case study presented within the oil and gas sector, strategically chosen to illustrate the vulnerability of critical infrastructures to cyber threats. By examining this sector in detail, the article aims to shed light on industry-specific challenges and potential solutions, thereby enhancing our understanding of cybersecurity dynamics within critical infrastructures. This article contributes a comprehensive analysis of the challenges faced by critical infrastructures in the face of cyber threats, offering contemporary security strategies and leveraging a focused case study to deepen insights into the nuanced vulnerabilities within the oil and gas sector.

Index Terms: Critical Infrastructure, Vulnerability, Cyber Security, Cyber Threats, Cyber-attacks, Oil and Gas Sector.

1. Introduction

Critical Infrastructure (CI) stands as the backbone of modern societies, encompassing vital facilities, systems, and networks crucial for societal function, economic stability, and national defense. Despite its paramount significance, a universally accepted definition of CI remains elusive on the global stage. While the ISO 22301 standard outlines guidelines for managing and mitigating risks associated with potential disruptions, the adaptability of both CI and this standard persists, subject to contextual variations and national disparities [1].

The ISO 22301 standard, a cornerstone in CI resilience, provides a framework for averting and recovering from incidents. However, its implementation varies as nations tailor their approaches based on specific interests, perceived threats, available resources, and legal frameworks. This flexibility spans across diverse sectors, including energy, transportation, telecommunications, finance, healthcare, water, and government services.

As the world becomes increasingly interconnected and digitally dependent, the imperative to shield CI from cyber threats intensifies. This is underscored by the evolving landscape of cyber-attacks on CIs, extensively explored in numerous cybersecurity studies [2-7]. Nations globally respond to this challenge, with the United States, the European Union, China, Japan, South Korea, and others formulating cybersecurity strategies to secure critical systems and infrastructure [8-11].

The article distinguishes the critical role of the oil and gas sector (OGS) within CI, given its pivotal properties and the crucial importance of sustaining the infrastructure subsystems within oil companies. In the face of a dynamic cyber

landscape, oil companies struggle with increasing threats encompassing cyber-attacks, espionage, and fraud, jeopardizing both financial resources and corporate reputations.

Against this background, this article explores a comprehensive analysis of current threats, emerging attack vectors, and prevailing trends in CI cybersecurity that demand immediate attention. Furthermore, it explores contemporary approaches aimed at fortifying the security and sustainability of OGS, shedding light on the ever-evolving strategies required to safeguard critical infrastructure in an era of escalating cyber threats.

The subsequent sections of this article are organized to provide a thorough examination of the subject matter. Section 2 outlines related studies, laying the foundation for an in-depth analysis of security issues and cyber threats. Section 3 explores the security issues inherent in CI management, analyzing complexities, and vulnerabilities, and emphasizing the need for robust security measures. Section 4 examines cyber threats to CI subsystems in the OGS, encouraging for the development of a targeted cybersecurity strategy. Section 5 proposes monitoring and incident detection solutions tailored to the unique security challenges of CI, particularly within OGS. Finally, Sections 6 and 7 conclude the work, summarize key findings, and outlines perspectives for further investigations.

2. Related Works

It should be emphasized that various infrastructures have evolved over the centuries to meet the growing needs of society. In the current era, we rely heavily on them in various aspects of daily life (Fig. 1).

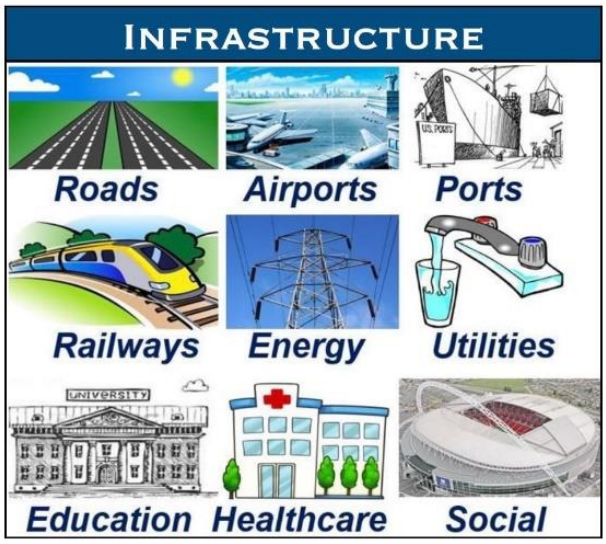

Fig.1. Types of infrastructure (source: market business news)

That is, infrastructure systems are integral components of modern society. However, CIs stand out among many other infrastructure systems due to their relevance to socio-economic needs and the risk of events that can cause serious consequences. Two key factors making CI critical to society are relevance related to socio-economic needs and risk assessment based on the likelihood of occurring events that could have serious consequences. These aspects provide a strategic basis for classifying and prioritizing infrastructure systems that ensure life support and the functioning of society in the face of adverse events and threats (Fig. 2).

Fig.2. Relevance and risk as basic factors of criticality

The relevance of infrastructure is manifested in the fact that its performance and accessibility become important for a large number of people. For example, the transport system, energy grid, water supply, and telecommunications become critical when they are needed for the daily life and work of large numbers of people.

Infrastructure also becomes critical when its condition or ability to meet the needs of society is compromised or threatened. For example, if a transport system cannot accommodate a city's growing population, it becomes a potential threat to the economic activity and livability of that city. Risks of destruction and accidents can lead to the failure to provide important services have a strong impact on the moral and psychological mood of society, and can also cause

social disturbance [12, 13].

CI must also be safe, which depends on many other factors, including engineering, geological, natural, and demographic. Issues of environmental sustainability and efficient resource use have also become important. Ensuring the cybersecurity of information and communication technologies (ICT) has become especially important in the modern world. Cybersecurity, as a multifaceted issue, includes protecting against cyber-attacks, managing data access, ensuring confidentiality and integrity of information, and ensuring the continuity of functioning of ICT systems. These aspects have become an integral part of ensuring the reliability and resilience of modern CI.

CI faces some serious threats that could have extensive consequences. Examples of such threats can be found in relevant articles and publications. Some of them are discussed below.

[14] analyzes scenarios of attacks on electrical networks and the risks they create. These attacks came from extremists, vandals, and cybercriminals. As a result, there are problems with the electricity supply, which can provoke social unrest. The article also mentions that the risk of attacks on the power grid is increasing due to the expansion of the electricity system through the use of renewable energy sources such as wind and solar power, as well as increasing demand for electricity from electric vehicles.

[15] describes a DoS cyber-attack on the power grid infrastructure of Ukraine. This caused power outages for several hours and affected 230,000 people. The article also describes how this affected other vital services.

[16] analyzes terrorist attacks on CI in the United States from 1970 to 2015 and examines various aspects of terrorist attacks, such as location, types of targets, weapons and tactics used, and consequences.

[17] defines healthcare cybersecurity challenges and solutions during the COVID-19 pandemic. The article also describes the most significant cyber-attack methods occurred during the COVID-19 pandemic, such as phishing, ransomware attacks, distributed denial of service attacks, and malware. The most famous examples of cyber-attacks occurred during the COVID-19 pandemic are the attacks on government agencies, hospitals, and pharmaceutical companies, such as the attack on the world's largest pharmaceutical company Pfizer, which produces the COVID-19 vaccine [18].

[19] discusses economic shocks and losses due to infrastructure failure, which is a difficult phenomenon to analyze. The authors highlight those businesses relying on infrastructure (such as electricity, gas, and telecommunications) for a variety of purposes, and information about the location and performance of the physical networks providing these services is difficult to obtain. The authors suggest that to model and understand the pervasive impact of infrastructure failures on business and the economy, a framework taking into account the processes and consequences of physical infrastructure failures in terms of physical capital losses and disruptions in service flows is needed.

Table 1 shows some of the cases of cyber-attacks.

Table 1. Examples of cyber-attacks

№	Cyber-attacked object/country/year	Target	Damage	Ref.
1.	Power grid/ Ukraine / 2015	Cause disruption and damage to the infrastructure and economy	The attack was successful in causing power outages for about half a million homes in one region of Ukraine for about six hours	[15, 20]
2.	Water company / USA / 2016	Manipulate valves that control the flow of chemicals	Stolen customer accounts. Changing the amount of chemicals used.	[21]
3.	Petrochemical Plant / Saudi Arabia / 2017	Sabotage the facility and cause an explosion	It failed.	[22]
4.	Transport system / Sweden / 2017	Crash an IT network system	Removing email systems, websites, and roadmaps	[23]
5.	Credit bureau Equifax / USA / 2017	Identity theft	The personal information of 147 million people was disclosed to compromise and blackmail	[24]
6.	Dept. of Health / USA / 2018	Get money from the company using scammers' methods	The dept. paid hackers $55,000 to regain access to its computer systems	[25]
7.	Telecommunications and financial sectors / Turkey / 2019	Communication networks of national infrastructure sectors	Getting money from a company by fraudulent methods	[26]
8.	Colonial Pipeline / USA / 2021	Get a lot of money	$4.4 million paid. Flights canceled due to fuel cuts	[27]
9.	Government agencies / Costa Rica / 2022	Extortion	A state of emergency declared	[28]
10.	State railway network / Poland / 2023	Public discontent	Emergency train stop	[29]

The basis of carried-out cyber-attacks very often hides elementary extortion of money. But attackers can also seek to achieve economic advantages, cause a public protest, and harm the national security of countries, also receiving financial rewards from interested parties.

Thus, only a small portion of the incidents show what consequences they can have for the economy, society, and national security, and indicate the need for further analysis. This will allow us to better understand the nature and scale of threats, as well as develop effective strategies and measures to strengthen cybersecurity.

3. Safety Challenges in CI

In reliability theory, threats refer to various types of impacts on objects that can lead to their failure or damage. These impacts can be caused by a variety of factors such as environmental conditions, human error, or design flaws. Threats can be classified into different categories such as physical, chemical, biological, and cyber threats [30].

In general, taking into account modern trends, the following threats are relevant for CI:

- Physical attacks
- Environmental factors
- Insider threats
- Pandemics and health emergencies
- Cyber-physical attacks
- Malicious Artificial Intelligence

Each of the above threats has unique goals and exploits specific vulnerabilities. Moreover, each of these threats can have different subtypes, which are defined and described in the following sections and illustrated in Fig. 3.

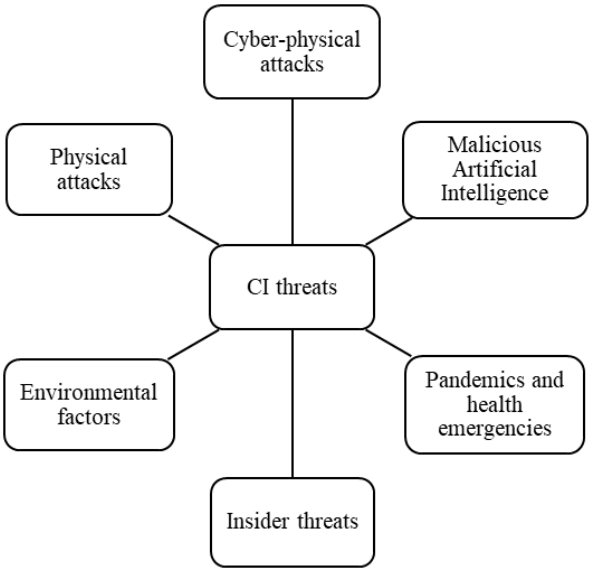

Fig.3. Current threats to CI

These threats are analyzed below:

3.1. Physical Attacks [31]

A. Explosions and Sabotage

One of the most dangerous types of physical attacks is explosions and acts of sabotage aimed at causing damage to the CI. For example, bombs or devices used to destroy power plants, oil pipelines, railroad bridges, and other devices can result in significant property losses and disruption of services.

B. Armed Attacks and Terrorism

CI may be the target of armed attacks by terrorist groups or other hostile forces. For example, an attack on water supply systems, gas pipelines, or transport hubs could disrupt water, energy, or transport services to the population and cause panic and chaos.

C. Systematic Damage

Physical attacks can also be systematic, aimed at gradually damaging or degrading infrastructure components. For example, the detonation of underground communication cables or damage to structural elements of bridges and dams can cause their gradual destruction and lead to disruption of the systems associated with them.

3.2. Environmental Factors [32]

Natural disasters in the environment can have significant consequences for CI. For example, changing rainfall patterns can be a factor influencing on water supplies. Excessive rainfall, flooding, or tornadoes can cause flooding which

is significant damage to transportation infrastructure, including roads and bridges. The changes or fluctuations in minimum and maximum temperatures has a major impact on energy production and distribution, resulting in enormous stress on energy systems. Natural disasters, such as major earthquakes, have a significant impact on CI, causing restrictions on the normal functioning of society. Therefore, the development of strategies and measures to strengthen and adapt CI to environmental factors is an important task to ensure its sustainability and continuous functioning.

3.3. Insider Threats [33, 34]

These threats involve individuals who have authorized access to systems and can use their privileges to cause harm or compromise security. Dissatisfied employees are known to abuse their access rights to deliberately disrupt or damage CI systems. Additionally, contractors or third-party service providers with temporary access to CI systems can, if not properly monitored or controlled, use their access to steal data, inject malicious code, or compromise the integrity of the infrastructure. In some cases, external actors use bribery or blackmail to coerce a responsible employee into compromising CI security.

To minimize the risk of insider threats, preventive security measures are necessary:

- reliable access control;
- ensuring strict oversight and accountability;
- employee monitoring;
- creating a safety culture;
- encouraging ethical behavior.

3.4. Pandemics and Health Emergencies [35, 36]

They pose a serious threat to CI due to their ability to disrupt operations, drain resources, and reduce labor availability. Here are some key points regarding these threats:

- Disruptions to Essential Services - During a pandemic or health emergency, CI sectors such as healthcare, transportation, energy, and telecommunications may experience significant disruption. High levels of absenteeism, increased demand for services, or supply chain disruptions could strain the capacity of these sectors, potentially impacting their ability to provide essential services.
- Impact on the workforce - Pandemics can lead to widespread illness among the workforce, affecting key personnel responsible for maintaining and operating CI systems. Quarantine measures, travel restrictions, and the need for social distancing may further impact labor availability and prevent the efficient achievement of operational goals.
- Increase in cyber threats - During health emergencies, the risk of cyber threats targeting CIs upsurges. Attackers can exploit the chaotic situation to launch cyber-attacks aimed at disrupting operations, stealing sensitive data, or spreading misinformation

3.5. Cyber-physical Attacks [37-39]

Attackers can use cyber-attacks to manipulate physical systems and CI components. This may include unauthorized access to information resources, which may result in malfunction or even damage to physical objects. At the same time, there may be attempts to physically enter the premises where servers and equipment are located to install malicious software, insert devices to steal data or change the operation of systems.

3.6. Malicious Artificial Intelligence [40]

This term emphasizes the role of AI as a tool in the hands of attackers. It is already being used for password guessing, CAPTCHA-breaking, and voice cloning, and there are many more malicious innovations in the works. Advances in AI indicate that the likelihood of its use in cyber-attacks on CI has increased. Automating the processes of finding vulnerabilities and executing attacks using AI can lead to massive and coordinated attacks that can cause significant damage to CI. Additionally, AI systems can adapt to defensive measures and learn from experience, making them more difficult to detect and combat rather than traditional security methods.

Attackers can also use AI to disguise attacks and create new methods to bypass security measures. AI’s ability to analyze large amounts of data, including social media and other open sources, can be used to create fake profiles, spread misinformation, and improve social engineering techniques.

All of these threats highlight the need for in-depth research and development of new cybersecurity techniques specifically tailored to combat AI-based attacks.

4. Cyber Threat Analysis for Critical Infrastructure Subsystems in the Oil and Gas Sector

It is important to emphasize that oil and natural gas are of strategic importance in the economies of the world, from raw material extraction to energy, industrial production, transportation, and much more. The impact of the OGS on these areas can be described as critical, since it provides the energy and raw materials base necessary for the sustainable

functioning of the economy and meeting the vital needs of society. In this regard, issues related to ensuring the sustainability and security of the infrastructure of companies engaged in the exploration, production, transportation, processing, manufacturing of finished products from raw materials, electricity generation, and much more become key priorities. These issues cover a wide range of aspects, including creating regulations, developing preventive measures, and responding to potential threats and cyber-attacks.

Therefore, we will take a closer look at the risks and cyber threats in this area.

The OGS is a complex and multi-level system, in which many subsystems and functional areas interact with each other to ensure stable and efficient operation. It is known that here, the processes are carried out sequentially in three segments, which are usually called Upstream, Midstream and Downstream [41, 42]. These three segments cover oil and gas production, from exploration and drilling platforms to oil wells; transportation of raw materials through pipelines to oil refineries; the processing of raw materials into the final product and delivering it to consumers. Thus, this three-segment model provides an integrated and efficient approach to the production and distribution of petroleum products, playing an important role in the global energy and economics.

In contrast to the previously known model, this article proposes the concept of the OGS infrastructure in the form of an integrated system (IS). The proposed model consists of numerous subsystems, each of which specializes in performing specific functions. This approach provides deep insight into the internal structure of an industry and its interrelationships. The architecture of the proposed model, presented in Fig. 4, serves as the basis for a detailed analysis of cybersecurity in the OGS. This approach allows not only to anticipate possible attacks, but also to actively prevent and counter them, ensuring the stable functioning of the OGS in the context of an ever-changing cyber threat landscape.

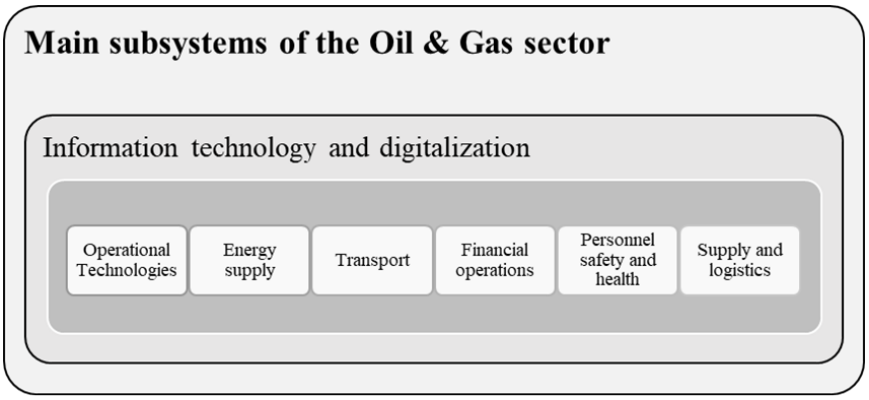

Fig.4. Integrated architecture of oil and gas sector infrastructure and its subsystems

Operational Technology (OT): Operational Technology includes the processes of exploration, production, refining, and distribution of oil and gas.

Power supply: Power supply provides the necessary energy for the operation of all systems and equipment in the OGS. This may include electricity, gas, heat, and other forms of energy needed to ensure continued operations.

Transport: The transportation subsystem includes vehicles for transporting oil, gas, and petroleum products from fields to processing and distribution points, as well as for delivering products to consumers. This may include pipelines, ships, railways, vehicles, and other forms of transport.

Financial Operations: The financial subsystem is responsible for financial management and accounting in an oil and gas company. This includes budgeting, investment management, expense and income accounting, and financial analysis.

Personnel Safety and Health: Occupational safety and health are critical in the oil and gas industry due to the high risk associated with working in oil fields and operating areas. This subsystem includes safety measures, personnel training, medical care, and other aspects related to the health and safety of employees.

Supply and Logistics: This subsystem is responsible for inventory management and logistics in the oil and gas industry, including the management of raw materials and components, as well as supply chain management and logistics to maintain continuous production.

Information Technology and Digitalization: IT and digital technologies are becoming increasingly important in the OGS for data management, process automation, and optimization of operations. This includes data management systems, monitoring and analytics, and cybersecurity.

The interaction of IT with each of these subsystems creates risks of cyber-attacks and requires increased attention to cybersecurity. Table 2 illustrates the risks of cyber-attacks on each subsystem and what consequences they can lead to in the overall structure of the OGS.

Table 2.

OGS critical infrastructure subsystems	Type of attack	Consequences
Operational Technology	Cyber-attacks on control and monitoring systems of oil and gas wells, raw material storage tanks, pipelines, and compressor stations, changes in product quality data	Unavailability or malfunction of equipment can lead to the shutdown of production processes and significant financial losses. Changing process parameters: which can lead to a decrease in product quality or even accidents
Power supply	Cyber-attacks on the power grid causing disruptions, overload, or damage to equipment	Power outage, loss of service, equipment damage, risk of fire or explosion
Subsystem for transportation of raw materials and finished products	Cyber-attacks on the navigation, communication, or security systems of vehicles such as tankers, pipelines, and fuel tankers, causing changes in routes, speed, or position, falsification of data or signals, or takeover of control	Crashes, collisions, loss of cargo, environmental damage
Personnel safety and health subsystem	Cyber-attacks on the storage and processing of medical data, medical equipment or implant management systems, remote diagnostic or treatment systems, causing theft, alteration or destruction of data, failure of equipment or implants, exposure of patients to unwanted influences, or murder	Creation of dangerous situations at oil and gas industry facilities, which can lead to breakdowns, accidents, and injuries to workers
Financial Operations	Cyber-attack on banking, payment, or financial market systems causing theft of funds or data, falsification of transactions or records, denial of service attacks, financial espionage	Loss of financial gain, obtaining confidential information, disruption of financial stability, or even the settlement of competitive advantages, disruption, economic instability
Supply and Logistics	Attackers can use phishing emails to gain access to supply chain management systems or steal sensitive information; Man-in-the-Middle (MITM) Attacks: In logistics, this could compromise the security of communication between suppliers, customers, and partners	Disruptions to the movement of goods, theft of sensitive information, and financial losses
Information Technology and Digitalization	Cyber-attacks target the very infrastructure and technologies that underpin OGS. Some common types of cyber-attacks that target IT and digitalization systems include Malware Attacks, Phishing, Zero-Day Exploits, DDoS, IoT Vulnerabilities, etc.	Cyber-attacks on information technology (IT) and digitalization systems in the oil and gas sector can have far-reaching and serious consequences due to the critical nature of this industry. Some potential consequences include Disruption of Operations, Safety Risks, Loss of Sensitive Data, Geopolitical Implications, etc.

As already noted, the oil and gas industry is one of the most powerful sectors of the world economy, having a great impact on most industries and consumers. Oil and gas are produced both onshore and offshore.

Offshore oil and gas production is the process of extracting crude oil and natural gas from subsea reservoirs, often located on the continental shelf or in deep-sea regions [43]. Since maritime conditions can be extremely unpredictable and harsh, ensuring the smooth operation and safety of maritime infrastructure becomes a priority. Protecting critical maritime infrastructure has become a top political priority following the September 2022 attacks on Nord Stream pipelines in the Baltic Sea [44]. Underwater control and remote monitoring are one of the most important processes in marine operations of the underwater control system [45]. Attacks on underwater control systems can occur in a variety of directions, and their nature may vary depending on the attacker's goals. Below are some possible attack vectors:

4.1. Interception and Manipulation of Commands and Sensor Readings [46]

Malicious actors may attempt to intercept and manipulate commands sent to the control system or sensor readings to disrupt operations and distort information. For instance, they could intercept and tamper with commands related to production parameters like pressure or temperature control. Such actions can lead to process instability and pose potential risks to the platform and personnel.

4.2. Fabrication of False Sensor Data [47]

By compromising sensors or manipulating data transmission, attackers can introduce fabricated or falsified data into the control system. This can result in incorrect decisions and responses to hazardous situations, as the system will be relying on inaccurate or distorted information.

4.3. Power Management Attacks

Sensors can be targeted by attacks that aim to manipulate their power consumption and power supply. For example, an Energy Depletion attack, where an attacker forces sensor nodes to operate in a high-power consumption mode, consequently reducing their lifespan and reliability [48].

4.4. Denial of Service (DoS) Attack [49]

An underwater control system can be subjected to a DoS attack, where attackers overload the system or its components by generating a substantial amount of traffic or sending numerous invalid requests. This can lead to

temporary or permanent system failure, posing significant risks to the security and performance of the platform.

4.5. Physical Intrusion [50]

Attacks can be realized through the physical infiltration of an offshore platform. Attackers may employ various tactics, such as impersonating an employee or infiltrating a service provider, to gain physical access to the underwater control systems.

4.6. Compromising of Service Providers [51]

Service providers involved in underwater monitoring systems can be specifically targeted by attackers with the intent of gaining unauthorized access to their networks or systems. By compromising a service provider, attackers can exploit their connection to subsea control systems, potentially granting them an advantageous position to infiltrate and manipulate the control systems.

4.7. Malware Attacks [52]

Malicious software, such as trojans or viruses, can be utilized by attackers to infect underwater control systems. These malicious programs are designed to alter system configurations in unauthorized ways. Attackers may introduce or activate malware on computers or devices responsible for controlling the system, enabling them to manipulate critical settings. For example, malware can modify control systems governing production parameters on oil or gas platforms. This may involve tampering with safety limits, falsifying data, rescheduling operations, and so forth. Such unauthorized changes can lead to hazardous working conditions and result in severe consequences, including accidents, decreased productivity, or even life-threatening situations.

The above example highlights the vital importance of studying cyber threats at different levels of the OGS. By comprehensively researching potential vulnerabilities, developing robust defense strategies, and raising awareness of cybersecurity, the industry can better defend against attacks that can disrupt operations, put personnel at risk, and lead to significant financial and environmental impacts. Proactive action and a comprehensive understanding of cyber threats are essential to mitigate risks and maintain the reliability and security of oil and gas infrastructure.

5. Solutions for Incident Monitoring and Detection

An effective system for monitoring and detecting incidents is a crucial component in ensuring the cybersecurity of CI in OGS. To identify potential incidents and promptly respond to them, it is necessary to use various methods and tools [53]. One such method is network traffic monitoring. By monitoring the network traffic carried within the information infrastructure, suspicious activity, anomalies, and unauthorized access attempts can be detected. Special tools are used for this, including intrusion detection systems (IDS) and anomaly detection systems. IDS are based on analyzing network packets and comparing them with known attack signatures. Anomaly detection systems build models of the normal performance of the system and highlight anomalous events and deviations from this model. In addition to network traffic monitoring, it is also important to analyze and aggregate events and event logs in the information infrastructure. This enables identification of suspicious or unusual events that may indicate security breaches. The use of information security management systems or other log analysis tools allows to efficiently process a large amount of data, and identify and analyze events associated with potential security incidents. This includes detecting suspicious activity, unusual user behavior, unauthorized access attempts, and other anomalies.

Prompt response to identified incidents is also important to an effective monitoring and detection system. To this end, it is necessary to establish clear procedures and response mechanisms, which may include automatic blocking of suspicious activities, notification of responsible persons or security services, analysis and diagnosis of the incident, as well as system recovery after the incident.

It is important to note that cybersecurity solutions in the OGS must be comprehensive and integrated. They should include not only monitoring and detection of incidents, but also preventive measures, such as the use of modern authentication and encryption mechanisms, regular software updates and patching, training of personnel on cybersecurity issues, etc. Proper implementation of these solutions may prevent serious security breaches and ensure critical OGS assets to be protected.

6. Conclusions

Research related to CI sustainability covers a wide range of areas, reflecting the complex and interdisciplinary nature of this issue. With an increasing number of CIs relying on modern information technology, cybersecurity has become more critical than ever. In this context, cybersecurity research becomes particularly important and it focuses on developing robust measures to protect against a variety of cyber threats. The field of cybersecurity includes a wide range of aspects such as methods for detecting, preventing, and responding to cyber-attacks. Research in this area aims at creating innovative tools and methodologies that will effectively detect and block threats, as well as restore systems after incidents. This includes developing machine learning algorithms to analyze large volumes of data, AI technologies to predict potential attacks, and creating defenses capable to adapt to new and improved cybercriminal techniques. Particular

attention should be paid to critical assets and systems, such as OGS, which face growing and sophisticated cyber threats. These systems often provide key services and support vital functions of society, and their vulnerability to cyber-attacks can have serious consequences. To protect OGS from cyber-attacks and malware, it is necessary to take a comprehensive approach. This approach includes measures to monitor and detect incidents; development of monitoring and early detection systems; incident response; ensuring the integrity and reliability of systems; applying safe software development practices; regular updates and fixes; and antivirus software and integrity controls to create reliable and secure systems at OGS. Studies in cybersecurity and CI resilience helps protect systems from cyber threats and improves society's ability to adapt to new challenges and threats in the digital age. It is important to continue to invest in this area and support collaboration between the scientific and engineering communities to ensure the safety and sustainability of CIs. In addressing the pressing issues outlined above, this article made several noteworthy contributions. An in-depth analysis of OGS within CI served as a novel contribution to the broader discourse on CI cybersecurity. A comprehensive examination of current threats and trends provided valuable insights to existing knowledge. The presented article did not merely highlight challenges but also put forth contemporary approaches aimed at fortifying the security and sustainability of OGS. The emphasis on tailored monitoring and incident detection solutions for CI, especially within OGS, represented a novel contribution to this field.

7. Future Investigations and Discussion

This article explored some of the key aspects of cybersecurity for CIs, with a focus on OGS. However, there are still many challenges and opportunities for further research in this field. Some of the possible directions for future investigations are:

Advanced threat landscape: how to anticipate and understand the evolving cyber threats that target CIs, especially OGS, and how to develop proactive measures to counter them.

Technological advancements: how to leverage emerging technologies, such as blockchain and quantum computing, to enhance the resilience of CIs against increasingly sophisticated cyber threats.

Human factors: how to address the human element in cybersecurity, exploring user behaviors, training protocols, and awareness campaigns to mitigate vulnerabilities arising from human actions.

International collaboration: how to foster international collaboration in addressing cyber threats to CIs, exploring frameworks for global cooperation and coordination.

Briefly, future investigations should build upon the foundations laid in this article, delving deeper into the emerging challenges and adopting innovative strategies to strengthen the security and sustainability of CIs, particularly in the context of OGS.

Acknowledgment

This work is supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

References

[1] ISO 22301. Available at: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf

[2] J. A. Lewis, "Cybersecurity and critical infrastructure protection," Center for Strategic and International Studies, vol. 9, 2006. Available at: http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf

[3] L.C. Herera, and O. Maennel, "A comprehensive instrument for identifying critical information infrastructure services," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 50-61, June 2019.

[4] C. Wilson, "Cyber threats to critical information infrastructure," *In Cyberterrorism: Understanding, Assessment, and Response*, T. Chen, L., Jarvis, S., Macdonald, S. (eds). Springer, New York, NY. pp. 123-136, 2014.

[5] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212-223, Sep. 2018.

[6] H. Brechbühl, R. Bruce, S. Dynes, and M. E. Johnson, "Protecting Critical Information Infrastructure: Developing Cybersecurity Policy," *Information Technology for Development*, vol. 16, is. 1, pp.83-91, 2010.

[7] A. A. Süzen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem," *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.12, No.1, pp.1-12, 2020. DOI: 10.5815/ijcnis.2020.01.01.

[8] *National Cybersecurity Program*. The White House, Washington, 2023, 35 p.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council. Official Journal of the European Union. Available at: http://data.europa.eu/eli/dir/2022/2555/oj

[10] L. Balke, "China's New Cybersecurity Law and U.S-China Cybersecurity Issues," *The Santa Clara Law Review*, vol. 58, is. 1, pp.137-163.

[11] B. Bartlett, "Government as facilitator: how Japan is building its cybersecurity market," *Journal of Cyber Policy*, vol. 3, is. 3, pp. 327-343, 2018.

[12] Y. J. Lee, "Social vulnerability indicators as a sustainable planning tool," *Environmental Impact Assessment Review*, vol. 44, pp. 31-42, 2014.

[13] S. Laska, Shirley, and B. H. Morrow, "Social Vulnerabilities and Hurricane Katrina: An Unnatural Disaster in New Orleans," *Marine Technology Society Journal*, vol. 40, no. 4, pp. 16-26, 2006.
[14] C. Morehouse, "Physical attacks on power grid surge to a new peak," 2022. Available at: https://www.politico.com/news/2022/12/26/physical-attacks-electrical-grid-peak-00075216
[15] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, I. Traore, "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook," *Energies*, Vol. 15, Issue. 19, pp. 2-32, 2022.
[16] "Terrorist Attacks Targeting Critical Infrastructure in the United States, 1970–2015." Available at: https://www.start.umd.edu/pubs/DHS_I&A_GTD_Targeting%20Critical%20Infrastructure%20in%20the%20US_June2016.pdf
[17] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health care cybersecurity challenges and solutions under the climate of COVID-19: Scoping review*," Journal of Medical Internet Research*, vol. 23, is. 4, e21747, 2021.
[18] A. Millar, "Five pharma cybersecurity breaches to know and learn from". Sept. 2021. https://www.pharmaceutical-technology.com/features/pharma-cyber-attacks/?cf-view
[19] E. Koks, R. Pant, S. Thacker, and J. W. Hall, "Understanding business disruption and economic losses due to electricity failures and flooding," *International Journal of Disaster Risk Science*, vol. 10, pp. 421-438, 2019
[20] "Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done". Available at: https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802
[21] "Water Treatment Plant Hit by Cyber-attack". Available at: https://www.infosecurity-magazine.com/news/water-treatment-plant-hit-by/
[22] "Saudi Arabia Investigating Critical Infrastructure Cyberattack". Available at: https://www.securitymagazine.com/articles/88818-saudi-arabia-investigating-critical-infrastructure-cyberattack
[23] B. Barth, "DDoS attacks delay trains, and stymie transportation services in Sweden," 2017. Available at: https://www.scmagazine.com/news/ddos-attacks-delay-trains-stymie-transportation-services-in-sweden
[24] "Equifax Data Breach Settlement". Available at: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement
[25] B. Lovelace Jr., "Hospital CEO forced to pay hackers in bitcoin now teaches others how to prepare for the worst," Available at: https://www.cnbc.com/2018/04/06/hosptial-ceo-forced-to-pay-hackers-in-bitcoin-now-teaches-others.html
[26] "Cyber-attacks blamed for Sunday's internet disruption across Turkey". Available at: https://www.dailysabah.com/turkey/2019/10/28/cyber-attacks-blamed-for-sundays-internet-disruption-across-turkey
[27] Sanger, D. E., and N. Perloth. "Colonial Pipeline hack reveals weaknesses in US cybersecurity." *New York Times* 14, 2021.
[28] J. Córdoba, C. Sherman, "Cyberattack causes chaos in Costa Rica government systems," Available at: https://apnews.com/article/russia-ukraine-technology-business-gangs-costa-rica-9b2fe3c5a1fba7aa7010eade96a086ea
[29] "Poland investigates hacking attack on state railway network." Available at: https://www.reuters.com/world/europe/poland-investigates-hacking-attack-state-railway-network-2023-08-26/
[30] P. Gardoni, *Risk and reliability analysis.* Springer International Publishing, pp. 3-24, 2017
[31] J. Moteff, P. Parfomak, *Critical infrastructure and key assets: definition and identification*. Washington: Congressional Research Service, Library of Congress, October 2004.
[32] I. Pal, A. Kumar, and A. Mukhopadhyay, "Risks to Coastal Critical Infrastructure from Climate Change," *Annual Review of Environment and Resources*, Vol. 48, 2023.
[33] S. Walker-Roberts, M. Hammoudeh, and A. Dehghantanha, "A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure," *IEEE Access*, 6, 25167-25177, 2018.
[34] I. Ghafir, J. Saleem, M. Hammoudeh, et al. "Security threats to critical infrastructure: the human factor," *The Journal of Supercomputing*, 74, 4986-5002, 2018.
[35] "Protecting critical infrastructure from a cyber pandemic." Available at: https://www.weforum.org/agenda/2021/10/protecting-critical-infrastructure-from-cyber-pandemic/
[36] A. Clark-Ginsberg, I. A. Rueda, J. Monken, J. Liu, and H. Chen, "Maintaining critical infrastructure resilience to natural hazards during the COVID-19 pandemic: hurricane preparations by US energy companies," *Journal of infrastructure preservation and resilience*, 1:10, pp. 1-6, 2020. DOI: 10.1186/s43065-020-00010-1.
[37] M. Heinrich, A. Gölz, T. Arul, and S. Katzenbeisser, "Rule-based anomaly detection for railway signaling networks," *International Journal of Critical Infrastructure Protection*, 100603, 2023.
[38] N. Mtukushe, A. K. Onaolapo, A. Aluko, and D. G. Dorrell, "Review of cyberattack implementation, detection, and mitigation methods in cyber-physical systems," *Energies*, 16(13), 5206, 2023.
[39] Z. Yu, H. Gao, X. Cong, N. Wu, and H. H. Song, "A Survey on Cyber-Physical Systems Security," *IEEE Internet of Things Journal*, 2023.
[40] R. Morrison, "How AI will extend the scale and sophistication of cybercrime," 2023. Available at: https://techmonitor.ai/partner-content/ai-cybercrime
[41] Tahmasib Kh. Fataliyev, Shakir A. Mehdiyev, "Analysis and New Approaches to the Solution of Problems of Operation of Oil and Gas Complex as Cyber-Physical System", International Journal of Information Technology and Computer Science, Vol.10, No.11, pp.67-76, 2018.
[42] H. Alfarsi, "Oil and Gas: Upstream, Midstream, and Downstream," 2018. Available at https://www.profolus.com/topics/oil-and-gas-upstream-midstream-and-downstream/
[43] Azeri-Chirag-Deepwater Gunashli. Available at: https://www.bp.com/en_az/azerbaijan/home/who-we-are/operationsprojects/acg2.html
[44] C. Bueger, and T. Liebetrau, "Critical maritime infrastructure protection: What's the trouble?" *Marine Policy*, 155, 105772, 2023.
[45] A. S. Mohammed, P. Reinecke, P. Burnap, O. Rana, and E. Anthi, "Cybersecurity challenges in the offshore oil and gas industry: an Industrial Cyber-Physical Systems (ICPS) perspective," *ACM Transactions on Cyber-Physical Systems (TCPS)*, vol. 6, is. 3, pp. 1-27, 2022.
[46] R. Su, "Supervisor synthesis to thwart cyber-attack with bounded sensor reading alterations," *Automatica*, vol. 94, pp. 35-44, 2018.
[47] A. Vempaty, L. Tong, and P. K. Varshney, "Distributed inference with Byzantine data: State-of-the-art review on data

falsification attacks," *IEEE Signal Processing Magazine*, vol. 30, is. 5, pp. 65-75, 2013.
[48] V. L. Nguyen, P. C. Lin, and R. H. Hwang, "Energy depletion attacks in low power wireless networks," *IEEE Access*, vol. 7, pp. 51915-51932, 2019.
[49] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," *IEEE Internet Computing*, vol. 10, is. 1, pp. 82-89, 2006.
[50] D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms, and challenges in wireless sensor networks," *arXiv preprint*: 0909.0576, 2009.
[51] "Protecting Against Cyber Threats to Managed Service Providers and their Customers". Available at: https://media.defense.gov/2022/May/11/2002994383/-1/-1/1/CSA_Protecting_Against_Cyber_Threats_to_MSPs_and_their_Customers_05112022.PDF
[52] R. Brewer, "Ransomware attacks: detection, prevention, and cure," *Network Security*, no. 9, pp. 5-9, 2016.
[53] O. Harazeem, T. A. Abdulganiyu, and Y.K. Saheed, "A systematic literature review for network intrusion detection system (IDS)," *International Journal of Information Security*, vol. 22, is. 5, 1125-1162, 2023.

Authors' Profiles

Shakir A. Mehdiyev has over 40 years of experience. He graduated from the Automation and Computer Engineering faculty of Azerbaijan Technical University in 1979. His primary research interests include various areas in e-science, computer networks, and maintenance. He is head of the department at the Institute of Information Technology, Baku, Azerbaijan. He is the author of about 30 scientific papers and 7 patents.

His ORCID ID: https://orcid.org/0000-0003-4828-577.

Dr. Mammad A. Hashimov received his Master's degree in automation and control from Azerbaijan Technical University. He received his PhD degree in 2016 from the Supreme Attestation Commission under the President of the Republic of Azerbaijan. He is a scientific researcher at the Institute of Information Technology, Baku, Azerbaijan. His primary research interests include various areas in the Internet of Things, cloud computing, data processing, computer networks, and virtual computing, particularly in the area of cloud technology applications. He is the author of 30 journal scientific papers and 20 proceedings.

His ORCID ID: https://orcid.org/0000-0001-5982-8986.

How to cite this paper: Shakir A. Mehdiyev, Mammad A. Hashimov, "Analysis of Threats and Cybersecurity in the Oil and Gas Sector within the Context of Critical Infrastructure", International Journal of Information Technology and Computer Science(IJITCS), Vol.16, No.1, pp.43-53, 2024. DOI:10.5815/ijitcs.2024.01.05