https://afrjcict.net

COUNTERING CYBER THREATS IN OFFSHORE OPERATIONS OF SMART FIELDS:A SURVEY

Sonny N. Epelle[1] and Bunakiye R. Japheth[2]

[1]Department of Computer Science, Ignatius Ajuru University of Education, Rivers State, Nigeria
[2]Department of Computer Science,Niger Delta University, Bayelsa State, Nigeria
Email: [1]epelleson@gmail.com,[2]bunakiye.japheph@ndu.edu.ng

ABSTRACT

The significance of offshore petroleum in providing the world's energy demands cannot be over overstated. The growing global energy resources demand, along with considerable technological developments, has resulted in a dramatic transfer of petroleum operations from onshore to offshore locations. States and oil companies are looking to the sea for offshore petroleum resources more than ever before. The offshore industry accounts for roughly 30% of overall petroleum output. This figure is likely to rise dramatically due to declining onshore fields and rapidly rising offshore petroleum exploration and development. The digitization of operational procedures in the oil and gas industry has created new potential to increase productivity and reduce costs. This, however, has also exposed the organization to a wide range of new cyber threats. For many years, the upstream sector, particularly offshore oil installations, has been an attractive target for terrorists. Attacks on crude oil and natural gas (O&G) firms have increased in frequency, sophistication, and impact as the industry adopts more linked technologies. As hackers' motivations evolve - from cyberterrorism to industrial espionage to interrupting operations to stealing field data - and firms increasingly relying daily operations on linked technology, dangers and stakes are rising rapidly. As a result, the sector must be protected from ongoing threats. This study therefore aims at looking at ways to Countering Cyber Threats in Offshore Operations of Digital Oil Fields. Organisations can fight sophisticated hackers by anticipating assaults, reacting in real time, and securing assets depending on their worth. They must use the "active defence" approach by taking all steps geared at predicting, detecting, redirecting, and isolating cyberattacks, if they must keep their organization secured.

.

Keywords: Energy Resources Demand, Appealing Targets for Terrorism, Digital oil Fields, Digitization, Cyber Threats, Mitigation

African Journal of Computing & ICT Reference Format

Sonny N. Epelle and Bunakiye R. Japheth(2022),
Countering cyber threats in offshore operations of smart fields: A survey
Afr. J. Comp. & ICT, Vol. 15, No. 1, pp. 22 –28

1. Introduction

The oil and gas system has an impact on every part of the country, and its operation is dependent on a sophisticated network of instrumentation, control, communications, and human and commercial activities. Increased control capabilities have resulted in increased system efficiency. However, as we become more reliant on technology and web-based communication, serious cyber security threats have emerged. With the oil and gas sector fueling practically every part of our daily lives, it's never been more important to protect this vital infrastructure. We can't afford to overlook the impact of cyber-attacks on the operations and systems that support our way of life**.**As a result, this study will take a closer look at the attraction of these vital infrastructures to cyber-attacks and their vulnerabilities, as well as provide solutions for countering cyber threats, particularly in the context of Digital Oil Fields' offshore operations. The aim of this study therefore, is to examine ways of countering cyber threats in offshore operations of Smart fields.Offshore petroleum plays a critical role in meeting the world's energy needs. The increasing global demand for energy resources, coupled with increased technological innovations, has resulted in a significant shift of petroleum operationsfrom onshore to offshore locations[1].More than ever before, states and oilcompanies are looking to the sea for offshore petroleum resources [2]. About 30% of total petroleum output comes from the offshore sector [3]. Due to declining onshore resources and rapidly developing offshore petroleum exploration and development, this number is likely to climb significantly[1, 4].

In the oil and gas industry, digitization of operational procedures has opened up new possibilities for increasing efficiency and lowering costs. In contrast, the company has been exposed to a new set of cyber threats as a result of the convergence of operational and business systems [5].Digital Oil Field (DOF), is all about how oil fields are run. By connecting remote sites in real-time to enable collaborative working, better decisions can be made, health risks can be reduced, Health Safety and Environment (HSE) can be improved, operating costs can be reduced, and output can be increased. DOF would not have been possible without smart field devices, the integration of industry automation systems, the integration of the Industrial Control System (ICS) withcorporatenetworks/systems, and thecapture ofreal-timedata [6]. DOF automation systems are similarin nature to IT systems used in enterprise networks, and they have become vulnerable tosimilarcyber attacks targeted at enterprise systems. Cyber security threats of today has transformed beyond the basic spread of viruses, computer data loss, and data theft,to the nature and ability to alter process plant operations such as increasing pressure in a pipeline, changing field device parameter settings, closing/opening a motorised valve, and causing a Denial of Service (DoS)attack within ICS, increasing/decreasing motor speed, showing a fictional process diagram, and flashing alerts on operators' Human Machine Interfaces (HMI) [6].Modern automation systems, according to AL-Issa [6], are based on industry standards like Windows or TCP/IP. As a result, they were vulnerable to cyber threats comparable to those that impact corporate business networks' systems. The consequences of cyber-attacks on industrial vital infrastructures, on the other hand, are dangerous, hence cyber security defenses and considerations must be built into critical infrastructure cyber security plans. Note that cyber security risks to vital infrastructure and/or the environment may result in loss of life,view, control, operation, production ordamage to critical infrastructure and/orenvironment.The automation technologies and the digital oilfield have made drilling rigs and all onboard equipments considerably more networked than before. The old isolation concept for drilling rigs is no longer sufficient to protect them from cyber-attacks. Remote access to a variety of shore-based facilities is common on rigs, whetherfor real-time operations support orequipment troubleshooting[7].Furthermore, there is a growing trend to locate control centers onshore, with one control center serving many fields, which may introduce vulnerability. Wireless technology is increasingly being used to connect field devices, potentially exposing plant operating systems to risk. [8].

Furthermore, due to the continual need to increase operational efficiency, large oil and gas corporations and drilling contractors are now relying on remote access due to costs involved or a shortage of personnel on board an offshore unit. [9].This has also contributed in making smart fields more vulnerable and appealing to cybercriminals.

The increased sophistication of hackers contributes to the natural dread connected with cyberattacks. If one assault fails, the next one improves on the previous one and becomes more capable of penetrating or exploiting a flaw in the system. Unless offshore oil platforms choose to resort to entirely isolated networks, there is nowayto ensure that a rig will be secure fromcyberterrorism. "We have embraced thegoodness of technology and all that itbrings us – efficiency and safety – butwe haven't addressed the bad" [10].There is a mismatch between theadvantage of connection and the dangerof connectivity on platforms. The oilandgas sector has been slow to recognisethe hazards of inadequate cybersecurityon offshore oil platforms[10]. As aconsequence, the days of a fictitioushacking threat are long gone, and we now live in a dangerous world**.** Hence, the industry is in desperate need of protection from these constant onslaughts. This study therefore aims at Combating Cyber Threats in Offshore Operations of Digital Oil Fields.

2. Related Work

In their study, Progoulakis and Nikitas[11] looked into the notion of security riskassessment for offshore oil and gasinstallations, focusing on the instruments used to detect, assess, and reduce security threats. The paper's examination of statistics of reported security events for offshore oil and gas assets highlighted the need for security risk assessment. A number of security and risk assessment methodologies that are more suited to offshore oil and gasinstallations were given. Thesignificanceof integration of Process Safety Management, Security, and Risk Assessment was emphasized. A qualitative security risk management tool was demonstrated, emphasizing the need for a multidisciplinary approach to the mitigation of security risks.

Infosys [12] discussed the inherent limitations and security challenges that oil and gas organizations face, as well as the approaches that define the way forward for addressing the concerns. They also discussed the key factors that must be considered when defining and designing appropriate security roadmaps for long-term cybersecurity programs

Roy et al [13] analysed and explained the principles of threatanalysis from an "academic" perspective in their work.Other concepts such as impact assessment, desire, intent,capability, opportunity, and planning were discussed. Therewere descriptions of how the inherent threat and theactualrisk were ssessed. A summary of the research imperativesfor threat analysis was provided, as well as approaches tothreat value stabilisation based on neural networks andother mathematical techniques.Gelenbe et al. [15]presented and analysed a distributedand resilient attackdetection and mitigation system fornetwork settings inwhich communicating decision agentsemployed GraphNeural Networks to generateattackalarms.They alsoshowed an attack mitigationsystem thatemployed aReinforcement Learning-drivenSoftwareDefined Networktohandle alarms and Quality-of-Service measures to reroute important traffic away from vulnerable network pathways. The detection and rerouting schemes were demonstrated in the experiments.

Suganthi and Usha [16] offered a detailed overview of the taxonomy, as well as a description and arrangement of current research findings on intrusion detection systems in IoT devices. Thanks to this study, the researchers were able to uncover security problems resulting from information sharing technologies in the Internet of Things, as well as learn about numerous security threats and mitigation strategies. Christopher et al. [17] proposed two methods for identifying botnetactivityin consumer IoT devices andnetworks in their article. To begin, a detection model was built using Term Frequency-Inverse Document Frequency(tf-idf), which analyses network traffic for semantic structure and highlights semantic similarities between collected data and a known assault dataset. The detection of Mirai attack vectors incollected network data was determined using a similarityscore. Second, a detection model based on a RecurrentNeural Network with Bidirectional Long Short-TermMemory was created using an unique Deep Learningapplication (BLSTM-RNN). The model was tested foraccuracy and loss after detecting four attack vectors usedby the Mirai botnet. Both techniques generate great outcomes, according to the article, and further research in this area seems promising.

MacKinnon et al. [18], looked at the differences between cyber terrorist and cybercriminal incidents, as well as the societal and technological changes that made such events more likely and devastating. The researchers then looked at three major components ofcyber-terrorist attacks: cyber-attacks onphysical systems, malware designedspecifically for suchattacks, and insiderthreats that enable or support suchoperations. They then looked at the countermeasures that organisations and individuals could use to address suchthreats, emphasising the humancomponent of such systemsbyemphasising the importance of standards-based policiesand protocols, goodsecurity hygiene, and system usertrainingat all levels. Physical system upgrades and software tools for detecting and isolating cyber threats were also discussed. Finally, they discussed the expected continued growth of cyber terrorist acts, as well as the threat they pose to critical infrastructure and systems on which we are increasingly reliant, both socially and technologically.

3. Motivation and Open Problems

3.1 Offshore Platforms as Targets for Attacks

Despite changing opinions towards oil and a growing thirst for clean energy, offshore natural gas production has increased by more than 50 percent since 2000 [19]. Offshore production accounts for more than a quarter of today's oil and gas supply [20]. Offshore oil platforms, on the other hand, have always been a valuable target for both physical and cyberattacks [21]. Terrorists put a high value on these assets because of their role in producing energy and money for many nations, as well as the great destruction that an attack on them may do. If an offshore oil rig is attacked, the results can be severe. An act of terrorism carried out on a platform may interrupt a country's regular supply of electricity, deprive it of a crucial source of money, generate substantial and long-term environmental impact, and result in considerable loss of life [10].

Offshore oil platforms are also high-value targets forterrorists owing to theirextreme susceptibility to physicalandcyber assaults, as well as the incredible difficulty of defending them and the possibleconsequences of strikes [10]. Physical assaults on offshore platforms continue to be a hazard, but cyber-attacksare a tactic of attack that platforms areequally, if not more, susceptible to. Because of the linkage of the platform to the coast, drilling rigs that

were historically geographically separated are no longer asisolated as theindustry thinks.

3.2 Digitization Magnifies the Challenges

A complex ecosystem of computing, networking, andphysical operational processes dispersed throughout theglobe, in addition to the upstream sector's "criticalinfrastructure" designation, renders the industry especiallysusceptible to cyber-attacks. In other words, the industryhas a vast attack surface and various assault vectors [5, diagram 1]. For example, a large oil and gas companyemploys half a million processors solely for reservoirsimulation; generates, transmits, and stores petabytes ofsensitive and competitive field data; and manages andshares thousands of drilling and production controlsystemsacross geographies, fields, vendors, service providers, andpartners

.

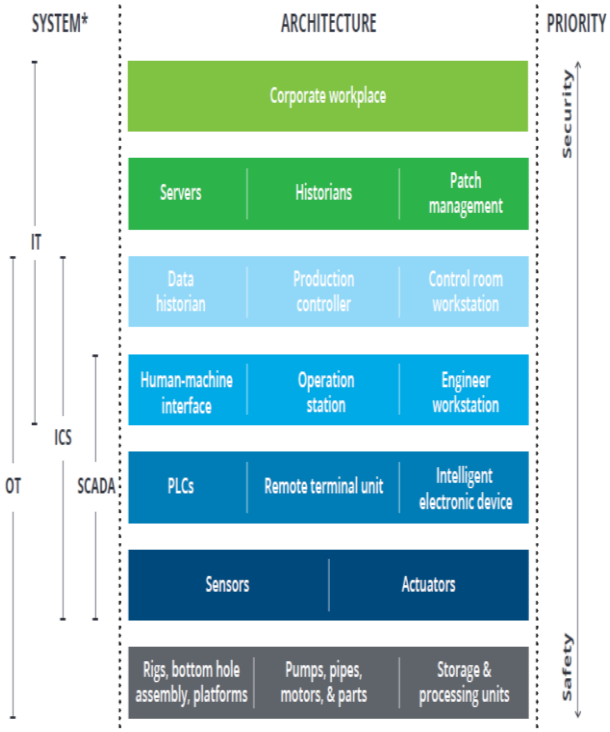

Figure 1: Typical Oil and Gas Company Cyber Concerns Architecture [22]

4. Understanding the risks

Complex ecosystems, fragmented ownership, latency issues, inconsistent cyber standards, irregular patching, and legacy issues are just a few of the cyber vulnerability challenges. The disparity in priority between the operations and information technology departments of businesses aggravate thesevulnerabilities. Sensors and programmable logic controllers, which are near to drilling and well site activities, are intended to execute duties with a crucial characteristic of 24X7 availability, followed by integrity and secrecy. IT systems,on the other hand, such as enterprise resource planning, have a reversible priority order for confidentiality, integrity, and availability. Engineers in drilling and production control rooms are worried that tight IT security measures may bring unacceptable delay into time-critical control systems, compromising decision making and operational reaction [22].

Security threats are also introduced by the technical setup of Industrial Control System (ICS). ICS software decisions are typically taken at the field or unit level rather than by corporate IT, resulting in solutions from a variety of solution providers, based on a variety of technologies, and with a variety of IT security requirements. The multi-decade life cycle of wells and ICS systems, as well as continuing asset sales and acquisitions, add to the complexity, making it difficult to account for, standardise, update, and refit these systems on a regular basis. For example, more than 1,350 oil and gas fields throughout the globe have been producing for more than 25 years, employing methods and equipment from diverse periods. [23]

In addition to the numerous benefits, increased digitization andinterconnection of operations has increased cyber risks.Connected technology, in the form of digital oil fields orsmart fields, has opened up an altogether new set ofattack vectors for hackers by combining upstreamactivitiesin real time. Shell, for example, recently drilled a well inVacaMuerta, Argentina, and controlled the drilling paceand pressure from a distant operations centre in Canada. [24]

What makes Internet of Things (IoT) technology bothpowerful and dangerous is its capacity to produce, transmit, collect, analyse, and act on data. Sensor technologies, wirelesscommunications networks, and a range of analytical andautomated tools allow the IoT phases, all of which are very susceptible to security breaches in outdated ICS systems and complicated upstream ecosystems. Protecting previously produced value while keeping ahead of future IoT adoption is a twofold cyber problem for the upstream oil and gas sector. [22]

Not all flaws in technology are the result of the technology itself. Internal actors wanting to undermine production, rivals looking to create brand harm, and external parties looking to shut down operations, such as activist organisations, are all potential sources of cyber risks. [5] It might also happen accidentally as a result of a lack of security awareness. Employees bringing infected portable media into the workplace, for example, might unwittingly expose systems to cyber-attacks due to a lack of security knowledge inside the firm. Furthermore, many operations staff just assume that their systems are unlikely to be attacked, thus they resist changing their routines and implementing new security policies. Another obsolete idea is that process failures are caused mostly by weather, human mistake, and equipment exhaustion, rather

than purposeful system manipulation by people who want to hurt others. [5]

The repercussions of a cyber breach, whether planned or inadvertent, may be severe, ranging from the compromise of sensitive data to system failure or shutdown. Reduced revenue, reputational damage, environmental disaster, legal penalties, and, in the worst-case scenario, death are all possible outcomes. [5]

5. Mitigating Cyber security Risk

Employees, regardless of size, are one of the most critical cybersecurity hazards in any firm. "Insiders carried out 60% of all assaults," according to a Harvard Business Review (HBR) study[14]. Three-quarters of the assaults were carried out with malevolent intent, while the other one-quarter were carried out by unintentional actors. [25]. Insiders who carry out malicious-intent assaults may be difficult to stop since the perpetrators generally know their way around the systems and can get beyond most of the perimeter protections, thanks to their valid access credentials. On the other hand, "inadvertent actor" assaults may be averted by training personnel about typical cybersecurity threats. Employees unknowingly participate as a vector of attack in many assaults because they do anything that compromises their user account credentials or workstation.

Employees that are taught about typical cybersecurity dangers may prevent many of these scenarios. Employees who areaware of phishing efforts and realise that certain securityinformation is never sought in an email are less likely tohand up their credentials to a hacker. Employees are less likely to connect compromised devices to their network if a firm has a clear policy in place for utilising personal devices at work that they are aware of. Educating staff on certain email capabilities may help them prevent accidentally sending emails to the incorrect individuals. A staff with basic cybersecurity training is less likely to leak data or provide hackers unlimited access to their systems.Another important element to consider is the inclusion of a framework to improve cyber security in the energy industry. The National Institute Standards and Technology's (NIST) Framework forImproving Critical Infrastructure Cybersecurity (CSF) helpsfirms evaluate their cybersecurity risks(threats,vulnerabilities, and consequences) and how to reduce those risks using tailored methodologies. The Framework's volunteer user base has expanded significantly throughout the nation and beyond the globe. It was created with the intention of benefiting private-sector owners and operators of essential infrastructurein the United States. The Framework integrates industrystandards and best practises to help businesses managecybersecurity risk. It creates a common language thatallows personnel at all levels of a business – and at allpoints in the supply chain – to have a sharedunderstanding of their cybersecurity concerns. In response to President Obama's executive order on defending privately-owned vital infrastructure, NIST published this study in 2014 as a consequence of the rising security, economic, public safety, and health risks posed by cyber security threats. The purpose is to improve the defence of critical infrastructure, which is crucial to the nation's security but is out of government control. "Regardless of an organization's size, threat exposure, orcybersecurity skill today, this strategy is required" [26].

The core functions of the NIST cyber security framework are: identify, protect, detect, react, and recover. [32, Fig 2]

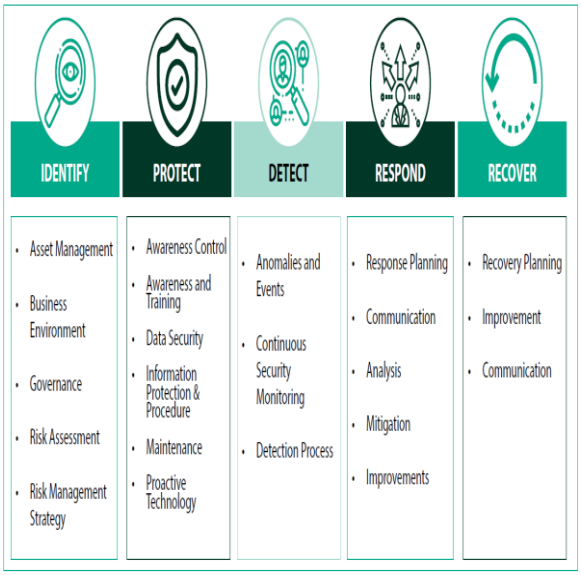

Figure 2: Cyber Security Framework NIST [12]

Understanding the organization's aim and business requirements, as well as acquiring current landscape information to manage cybersecurity risk to systems, assets, data, and capabilities, are all part of the identification process. The identification function's operations are critical to the creation of a secure environment. Protect actions assist an organization in deterring cyber intrusion and harmful activities by establishing and implementing security policies to assure the availability and continuation of critical infrastructure services. Organizations should have a mechanism in place to detect and deter any intrusions, as there are possibilities that intrusions will continue to occur after controls and technology solutions have been implemented. It is nearly impossible to achieve a system with no points of entry. Respondis a critical step in which processes and activities within the team and organization are clearly identified, planned, and communicated. Recovery involves developing and implementing procedures for recovering from cyber incidents.To respond to all cyber incidents, these processes and procedures are developed and implemented. This allows the organization to reduce the impact of a cyber-security incident to a bare minimum. Because of the speed and intelligence of many of today's cyberattacks, cyber breaches may still occur; as a result, organizations should anticipate attacks and develop solutions to respond to them in real time.

6. Conclusions

In the oil and gas business, digitization of operational procedures has opened up new possibilities for increasing efficiency and lowering costs. However, this has exposed the company to a whole new set of cyber threats. For many years, the upstream sector, particularly offshore oil installations, has been a tempting target for terrorists. Cyber attackers have attacked the crude oil and natural gas (O&G) sectors as the industry embraces more networked technology, with assaults rising in frequency, complexity, and impact. Nonetheless, as hackers' goals evolve - from cyberterrorism to industrialespionage to interrupting operations to collecting field dataand firms increasingly depend on linked technology for day-to-day operations, dangers and stakes are constantly growing. As a result, the sector must be protected from these ongoing threats.Businesses can fight sophisticated hackers by anticipating assaults, reacting in real time, and securing assets depending on their worth. Despite all of the resources spent tostrengtheningcybersecurity, threat levels continue to climbfaster thanprotection capabilities. With the exception of potentially unlawful acts such as hacking back, organisations must take all steps geared at predicting, detecting, redirecting, and isolating cyberattacks. That is, they use an "active defence" approach. Their firewalls should be expected to be penetrated. They should anticipate their encryption keys to be hacked, and that hackers would remain one step ahead of them when it comes to infecting their infrastructure with malware. Organizations must predict assaults before they happen, detect alarms in order to limit attacks, and secure vital assets in a multi-tiered strategy

References

[1] International Energy Agency (IEA), World Energy Outlook (2008, Nov. 30) Accessed on February 8, 2021. [Online]. Available: https://www.iea.org/reports/world-energy-outlook-2008

[2]M. Murphy, "Contemporary Piracy and Maritime Terrorism" Adelphi Papers 47(338) 1, 75.Routledge, London, 2007. https://doi.org/10.4324/9780203759318

[3] International Energy Agency (IEA), World Energy Outlook (2010, Nov. 30) Accessed on February 8, 2021, [Online]. Available: World Energy Outlook 2010 (windows.net)

[4] L. Cordner, "Managing regional risk: offshore oil and gas safety and security in the Asia-Pacific region,"*Australian Journal of Maritime & Ocean Affairs*, 3(1), 15–24. 2011. doi:10.1080/18366503.2011.1081567

[5] P. Zonneveld, An integrated approach to combat cyber risk securing industrial operations in oil and gas, 2017, Accessed on February 8, 2021. [Online] Available:https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Energy-and-Resources/intergrated-approach-combat-cyber-risk-oil-gas.pdf

[6] A. AL-Issa, "Abu Dhabi Marine Operating Company (ADMA-OPCO), Protecting The Digital Oil Fields from Emerging Cyber Threats," Abu Dhabi International Petroleum Exhibition & Conference, Abu Dhabi, UAE, 11-14 November 2012, https://doi.org/10.2118/162304-MS

[7] L. Hsieh, "Industry recognizing need for better cyber defenses as hackers become more sophisticated and drilling equipment becomes more interconnected," *Drilling Contractor*, September 8, 2015, Accessed on August 18, 2021. [Online] Available:www.drillingcontractor.org/drilling-cybersecurity-36727.

[8] F. Lobo, "Upstream Oil & Gas Cyber Risk: Insurance Technical Review,
A Joint Rig Committee Report, "First Report, May 2018, Accessed on February 8, 2021.
[Online] Available: JRC-UpstreamCyberRiskReport1.pdf (d2mqw5602n62j3.cloudfront.net)

[9] L. Soares, and R. Souza, "Cyber Risks in the Oil & Gas Industry," In Proceedings of the Rio Oil and Gas Expo and Conference, Rio de Janeiro, Brazil, 15–18 September 2014. Accessed on February 8, 2021. [Online] Available:https://www.researchgate.net/publication/341651683_Cyber_Risks_in_the_Oil_Gas_Industry

[10] J. Crandal, "Cybersecurity and Offshore Oil: The Next Big Threat, "Oil and Gas, Natural Resources, and Energy Journal, vol 4(6); 703 – 735, 2019, Accessed on February 8, 2021.Online] Available: https://digitalcommons.law.ou.edu/onej/vol4/iss6/2

[11] I. Progoulakis and N. Nikitakos, "Risk Assessment Framework for the Security of Offshore Oil and Gas Assets," IAME 2019 Conference, June 25 – 28, Athens, Greece. Accessed on February 8, 2021. [Online] Available: https://www.researchgate.net/publication/334226724_Risk_Assessment_Framework_for_the_Security_of_Offshore_Oil_and_Gas_Assets

[12] Infosys, "Industrial Cybersecurity Risks – Oil and Gas Operations: Challenges and roadmap for a secure ecosystem," 2020, Accessed on February 8, 2021. [Online] Available: httpss://www.infosys.com/services/cyber-security/documents/oil-gas-operations.pdf

[13] J. Roy, S Paradis and M. Allouche, "Threat evaluation for impact assessment in situation analysis systems," 2002, SPIE Proceedings, Vol. 4729, Signal Processing, Sensor Fusion, and Target Recognition XI. doi:10.1117/12.477618

[14]M. Van Zadelhoff , "The Biggest Cybersecurity Threats Are Inside Your Company" (2016) Accessed on August 18, 2021, [Online]. Available: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company

[15] E. Gelenbe, P. Fröhlich, M. P. Nowak, and S. Papadopoulos, "IoT Network Attack Detection and Mitigation**,"**2020, 9th Mediterranean Conference on Embedded Computing (MECO)8-11 June 2020, Budva, Montenegro, **IEEE.** DOI: 10.1109/MECO49872.2020

[16] Suganthi and D.Usha, "A Survey of Intrusion Detection System in Iot Devices.,"International Journal of Advanced Research 6(6):23-30, 2018,DOI:10.21474/IJAR01/7183

[17] C. D. McDermott, W. Haynes, Andrei V. Petrovksi, "Threat Detection and Analysis in the Internet of Things using Deep Packet Inspection," Intl. Journal on Cyber Situational Awareness, Vol. 3, No. 1, 2018, pp 1 – 23. DOI:10.22619/IJCSA.2018.100120

[18] L. MacKinnon, L. Bacon, D. Gan, G. Loukas, D. Chadwick, D. Frangiskatos, "*Cyber Security Countermeasures to Combat Cyber Terrorism*", In book: Strategic Intelligence Management (pp.234-257), 2013, [Online]. DOI:10.1016/B978-0-12-407191-9.00020-X

[19] J. M. Broder, "BP Shortcuts Led to Gulf Oil Spill", Report Says, N.Y. TIMES (Sept. 14, 2011), Accessed on August 25, 2021, [Online]. https://www.nytimes.com/2011/09/15/science/earth/15spill.html.

[20] International Energy Agency, (2018, May), "The Future of Offshore Energy*"*, WORLD ENERGY OUTLOOKOFFSHORE, Accessed on August 25, 2021. [Online] Available: https://www.iea.org/weo/offshore/.

[21] A. Harel, "Preventing Terrorist Attacks on Offshore Platforms: Do States Have Sufficient Legal Tools?" 4 HARV. NAT'L SEC. J. 131, 133-134 (2012). Accessed on August 25, 2021. [Online]. Available:https://harvardnsj.org/2013/01/preventing-terrorist-attacks-on-offshore-platforms-do-states-have-sufficient-legal-tools/

[22] A. Mittal, A. Slaughter, P. Zonneveld, "Protecting the connected Barrels, Cybersecurity for Upstream Oil and Gas", A report by Deloitte Center for Energy Solutions, 2017. Accessed on February 8, 2021 [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/energy-resources/DUP_Protecting-the-connected-barrels.pdf

[23] Global Data, "Oil & gas database," Accessed on April 23, 2021[Online]. Available: https://energy.globaldata.com/research-areas/oil-and-gas

[24] Economist, (2017, Apr.) "Oil struggles to enter the digital age," Accessed on August 18, 2021, [Online]. Available: www.economist.com/news/ business/21720338-talk-digital-oil-rig-may-be-bit-premature-oil-struggles-enter-digital-age

[25] E. Dosal, (2018, Apr) "How to Mitigate Cyber security Risk is a cost effective manner", Compuquip Cybersecurity, Accessed on February 8, 2021, [Online]. Available:https://www.compuquip.com/blog/mitigate-cybersecurity-risks-cost-effective.

[26] NIST, "Framework for Improving Critical Infrastructure Cybersecurity", Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://doi.org/10.6028/NIST.CSWP.04162018