“Cybersecurity in the Oil and Gas (ONG) Sector”

Published: September, 2022

Author: Natali Cordova Siegwart

“Well intended policy can have unintended consequences”
(ONG Sector Representative)

Introduction

It is often said that offshore oil and gas operations are more complex than space exploration because of the challenge of bringing deposits from thousands of feet underground and underwater to the surface.

We will explore cybersecurity in the ONG sector in this paper, and to do so, first we will explain how the sector is organized, after which we can examine how cybersecurity impacts the sector specifically. We will discuss the ONG sector as critical infrastructure and as which is it the companies or the governments responsible for their security. We will analyze Cybersecurity Capability models developed by the US Energy Department as frameworks to help the sector evaluate their cybersecurity readiness.

The research questions that we are working with in the present paper are the following: Is the Oil and Gas sector protected against cyber-attacks? Does being a part of what is considered critical infrastructure give Oil and Gas companies more protection against cyber-attacks? Is enough being done in the ONG sector by the companies and governments to protect it against cyber threats? Are risk assessment cybersecurity capability models effective?

In order to answer the research questions, the paper will be structured with an Introduction, the first chapter providing background information about the ONG sector. The second chapter will analyze Cybersecurity in the ONG sector in general. Chapter Three will explore what securing the ONG sector against cyber threats implies, analyzing the ONG as critical infrastructure and who holds the responsibility (companies or governments) for securing its safety against cyber threats and attacks, also analyzing some examples of government bodies in the world in charge of cybersecurity for critical infrastructure.

Chapter four will explain the risk assessment done in the sector based on Cybersecurity capability models developed by the US Energy Department ONG C2M2 and C2M2. Finally, we come to the conclusions and bibliography.

In the present paper, we have the following hypothesis: cybersecurity capability models ONG C2M2 and C2M2 are insufficient, as part of policies and frameworks to assess the risks. Another hypothesis is that perhaps creating new policies with good intention may have unintended consequences, like the phrase we used at the beginning.

Our last hypothesis for the present paper is; Increasing policy may not have a positive effect, and a step before that is assessing risk and understanding threats, improving cybersecurity capability models is the way forward.

The Oil and Gas (ONG) Sector

Our daily lives are intertwined with petroleum products. They affect every aspect of our lives, from cooking to traveling to electricity. Hydrocarbons are used in nearly every aspect of our daily lives. As the hydrocarbon industry developed in the late 20th century, it would not be inappropriate to say that it was during this time that the oil and gas industry was born. The development of the oil and gas industry began in a meteoric fashion, despite some evidence suggesting hydrocarbons have been used since the last 1500 years ago. In the 16th century, the Industrial Revolution and the need for authentic and fast modes of transportation and logistics during the colonial era of American and European powers were two of many events that contributed to the development of this industry.

Researchers agree that while World War II was a highly destructive war, in which nearly 60 million people died, it was also an important turning point in the development of the hydrocarbon industry. Although it was destructive, it had positive effects on technological development. There were many scientific inventions during the war in the fields of welding

technology, metallurgy, organic chemistry, chemistry, electronics and computation as well as numerous others. As with many other industries, these inventions paved the way for the oil and gas sector to develop and grow. It was after the 1960s that offshore oil and gas began to evolve. In the Thames and Mersey estuaries, the British Navy built the "Thames Sea Forts" as a means of preventing an invasion by the Nazis. Modern offshore platforms are direct descendants of those towers. (Dalvi, 2015)

Fig. 1.1: 1p Thames Sea Forts

(Dalvi, 2015)

In the ONG sector, upstream and downstream are commonly used terms. An upstream activity refers to the exploration and production of crude oil and natural gas, whereas a downstream activity refers to the process of delivering the crude oil and natural gas to the customer.

Upstream: Exploration involves multiple activities, including obtaining land rights, conducting geological surveys, and digging exploratory wells to identify reserves of oil and gas. It is a high-risk activity for companies. In the production process, the natural

resource is extracted from the ground by drilling wells (onshore or offshore), or by fracking. As a result, upstream operations are heavily reliant on electronics and technology. Before exploration wells are dug, surveys are conducted with sophisticated electronic equipment, which will likely inform AI and computer-based models of the area. The drilling and fracking industry has also become increasingly automated and computerized as drilling and fracking equipment has become more advanced, autonomous, and efficient.

A downstream process is the final step in the journey of oil and gas from the ground to the consumer's hands. Traditionally, upstream and midstream activities are responsible for extracting crude oil and natural gas and transferring it to refineries.

Therefore, refinement is the first step in downstream work. As a result of fractional distillation, crude oil is refined into gasoline, naphtha, kerosene, and diesel oil. Because each product has a different boiling point, fractional distillation works.

All the components of crude oil are heated at the bottom of the distillation chamber until they turn into gasses, which rise upwards. After they rise up the chamber, they cool, and an apparatus is placed to catch the different products as they condense from a vapor into a liquid.

Natural gas processing involves multiple chemical reactions that result in multiple end products such as ethane, propane, and butane, all of which are complex. After refinement and processing of both products, they are packaged in various ways and delivered to consumers.

As part of the production of oil and gas products, midstream works or field processing are often mentioned – these processes connect upstream and downstream processes. Following the completion of upstream operations – exploration and extraction of raw materials from the ground – midstream operations deal with processing, storing, and transporting those materials to further refinement sites.

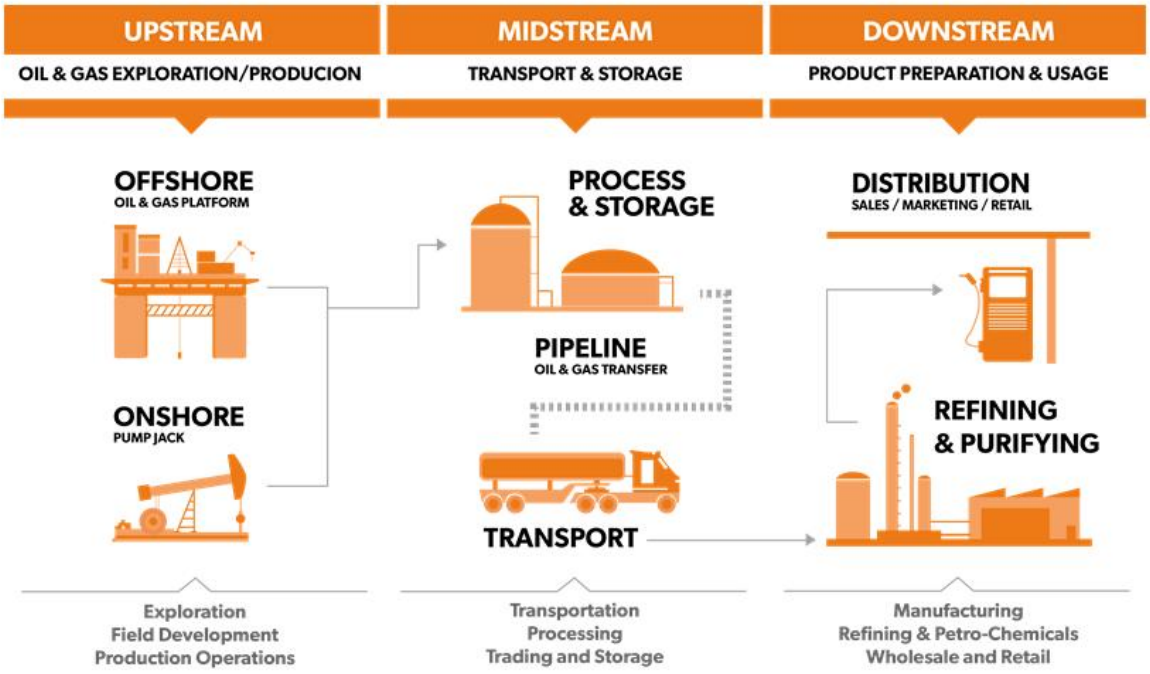


Illustration and simple explanation of the sector made by a private company: https://www.elandcables.com/the-cable-lab/faqs/faq-what-are-upstream-and-downstream-works-in-the-oil-gas-industry

Some past and present challenges the ONG sector is facing:

Global politics and economics were affected for years by two oil price shocks that occurred during the 1970s as a result of geopolitical events. On the demand side, major oil and gas producers faced declining consumption, as consumers turned to alternative energy sources, energy efficiency improved, and non-OPEC oil supplies increased.

A similar but more intense crisis in the 2000s led to a profound change in the structure of oil and gas markets. The oil and gas industry face two major challenges: energy substitution and resource scarcity. The substitution of coal and renewable energy threatens to reduce the demand for oil and gas, but resource scarcity is expected to promote the development of unconventional hydrocarbons such as shale oil and gas.

In the 2000s, oil consumption did not decrease as it did in the 1970s. Moreover, the recent fall in oil and gas prices created a fiscal challenge for conventional producers, such as OPEC countries, and non-OPEC countries like Russia and Mexico, whose governments depend on export revenues.

National oil companies (NOCs) and international oil companies (IOCs) are expected to be more competitive as a result of these fiscal challenges, requiring structural changes in industry governance. A rise in state capitalism is expected in the next decades not only in major oil and gas producing countries, but also in the global energy industry, as NOCs continue to dominate the industry. The increasing interference of the corresponding governments will likely lead to an increase in state capitalism. (Ediger, 2018)

Some researchers agree that in recent years, the petroleum industry has faced several complex challenges in terms of sustainability. The oil industry should invest pro rata to the increasing demand for energy in the world, on the other hand, as a result of the more competitive activities in these sectors, this industry needs to reduce the total cost of production of hydrocarbon resources while adhering to environmental laws and social obligations at the same time. Price fluctuations, complexity of drilling and production processes, growing demand for oil and gas in most regions, and handling increasingly large data sets are some of the significant challenges facing the oil and gas industry. (Mojarad, 2018)

General Aspects of Cybersecurity in the ONG Sector

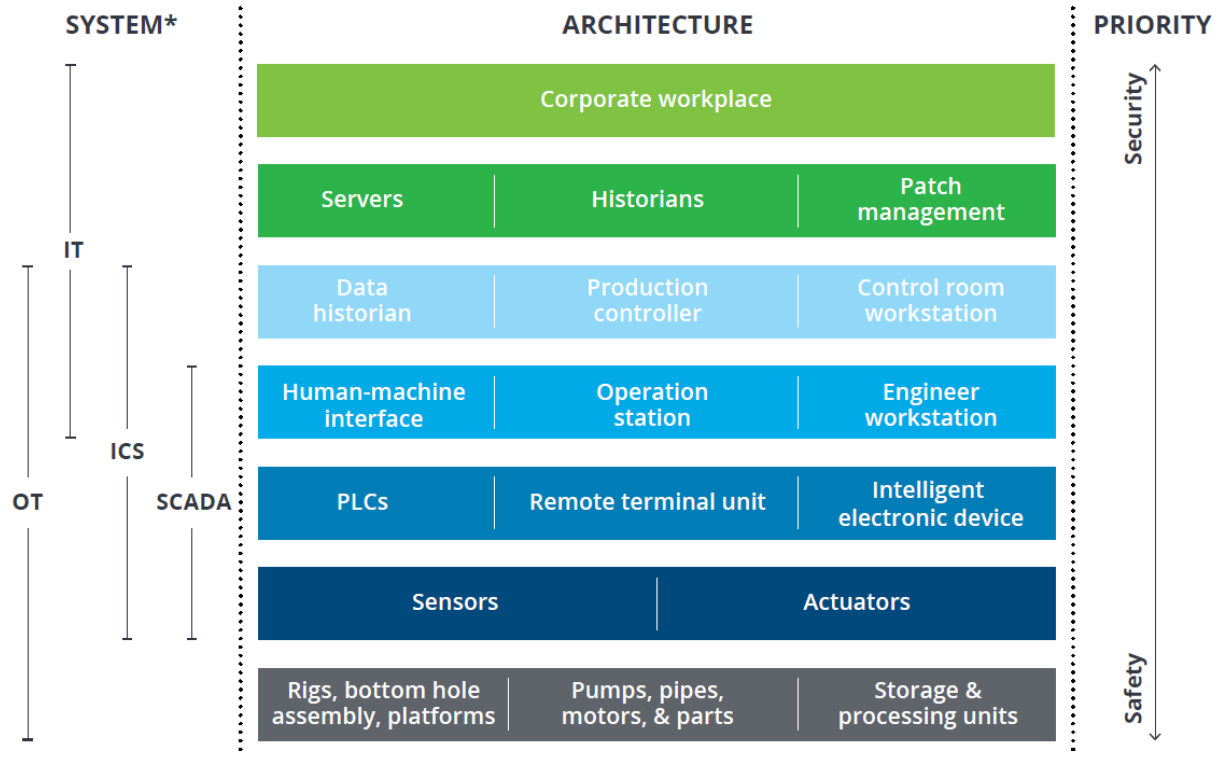
In addition to sophisticated equipment, tools, assets, and specialized interdisciplinary knowledge, the oil and gas industry is an important part of the nation's critical infrastructure. The oil and gas industry is experiencing an increase in digital transformation in order to improve productivity and efficiency. This, in turn, increases cyber vulnerabilities and threats. Therefore, cyber risk management has become an essential part of the process of digital transformation of the petroleum sector. However,

despite concerns about cyber threats for oil and gas projects, research on integrating technical and non-technical cyber risk management models is scant. (Imran, 2021)

It is only natural that the ONG business carries different levels of risk and requires different strategies. Development drilling and production have the highest cyber risk profiles among upstream operations; seismic imaging has a relatively low risk profile, but it may face an increase in risk in the future as it digitizes, stores, and feeds seismic data into other disciplines.

Research suggests that: vigilant, resilient risk management programs can mitigate cyber risks and incorporate them into all operations. Safety, reliability, and value creation are three of the operational imperatives of an upstream company. In order to protect the connected barrels, a complex ecosystem of computation, networking, and physical operational processes spread around the world makes the industry highly vulnerable to cyber-attacks; therefore, the industry has a large attack surface and a multitude of attack vectors. As an example, a large oil and gas company uses half a million processors just to simulate reservoirs; generates, transmits, and stores petabytes of competitive field data; and operates and shares thousands of drillings and production control systems across geographies, fields, vendors, service providers, and partners. (Mittal-2017)

Figure 1. Typical IT/OT architecture and cyber concerns of an O&G company



CYBER CONCERNS

- **Complex ecosystem**: Joint operations take place across regions and employ multiple vendors with different security guidelines.
- **Fragmented ownership**: IT and OT were developed with distinct missions, thus cyber ownership and responsibility are fragmented across the organization.
- **Latency concern**: Firewalls could introduce unacceptable latency into time-critical ICS systems that face operational constraints.
- **Inconsistent cyber standards**: A mix of proprietary and off-the-shelf technologies complicates the problem.
- **Irregular patching**: Security patching of many systems is irregular and vendor specific as these systems are in remote, unmanned areas.
- **Legacy concerns**: Many systems have long life cycles (10+ years) that were not built for cybersecurity. Retrofitting or upgrading is costly and impacts operations.

**Acronyms: ICS: Industrial control systems; SCADA: Supervisory control and data acquisition*

Source: Deloitte analysis.

Deloitte University Press | dupress.deloitte.com

(Mittal-2017, pg4)

Operational technology (OT) departments and information technology (IT) departments have contrasting priorities, which adds to this vulnerability. As a rule, confidentiality,

integrity, and availability are ranked in reverse order for systems near drilling and well site operations. The conflict between safety and security plays out in drilling and production control rooms where engineers worry that IT security measures may introduce unacceptable latency into time-critical controls, impacting decision-making and operational efficiency.

Researchers suggest that there is inherent security challenges associated with the technical set-up of the ICS (Industrial Control System). ICS software decisions are often not made centrally by corporate IT, but rather at the field or unit level, resulting in products from different providers, using different technologies, and complying with different security standards. The decade-plus life cycle of wells and ICS systems and ongoing asset sales and purchases

Due to their diversity, these systems are difficult to account for, standardize, upgrade, and retrofit frequently, adding to the diversity problem. For example, over 1,350 oil and gas fields around the world have been producing for more than 25 years, using a variety of equipment and systems.

Increasing digitization and interconnectedness of operations have increased cyber risks. With the advent of digital oil fields and smart fields, hackers have been able to develop entirely new attack vectors by connecting upstream operations in real time, creating an entirely new landscape of attack vectors.

From a remote operating center in Canada, Shell recently designed and controlled the drilling speed and pressure in Vaca Muerta, Argentina. A key factor in the power and vulnerability of Internet of Things (IoT) technology is its ability to create, communicate, aggregate, analyze, and act upon data. (Mittal-2017)

The industry is a highly visible target for disruptions, interceptions of sensitive data, and economic damage. A number of attacks against this industry have demonstrated the importance of risk management and risk-based security policies.

Aside from the challenges associated with maintaining the ONG sector's infrastructure, it faces extreme conditions, remote locations, difficulties operating in harsh environments,

and complex socio-political factors that make finding, transporting, refining, and distributing oil and natural gas difficult. It is therefore important for major Independent Oil Companies (IOCs) to develop standards and management systems to address these risks.

A company's management system determines how it identifies and mitigates health and safety risks throughout its operations. Aside from the traditional operational and physical risks, the oil and gas industry also face cyberattacks that threaten other companies, organizations, and government agencies worldwide.

It is reported that cyber-attacks are on the rise. Some of the biggest attacks on the ONG have been the following:

The Cutting Sword of Justice, a hacker group, claimed responsibility for the **Saudi Aramco** attack of 2012**.** The Saudi Aramco attack, targeted at stopping Saudi Arabia's largest exporter's oil and gas production, damaged the hard drives of 30,000 computers and highlighted the industry's vulnerability. It was the first cyberattack that actually damaged computers on a large scale.

Referring to the Aramco hack, the computer security research community dubbed the virus reputed to have spread across Aramco's network Shamoon. The SHAMOON-Aramco incident came after years of warning about the risk of cyber-attacks against critical infrastructure. Saudi Arabia and the United States have shared a common concern over the protection of Saudi petroleum infrastructure from military and terrorist attacks for decades. Iranians pose a significant threat to oil production facilities in Saudi Arabia's Eastern Province. It would have immediate effects on oil supplies and prices, with knock-on effects for the global economy, even if these production facilities were interrupted in part. In spite of the Shammon attack not causing any physical damage to critical infrastructure in the Middle East, it has had a secondary impact on risk assessment for critical service providers worldwide. (Bronk-2013)

RasGas Company Limited was attacked with an improved version of the Aramco virus two weeks later. This second attack demonstrated the speed with which motivated

attackers can respond and adapt; these highlights, not only the need for the oil and gas industry to respond quickly and adapt to events, but also the need to anticipate them through a risk-based security program that identifies and eliminates risks as often and as practically as possible, and prepares for any remaining risks. (Holcomb, 2016)

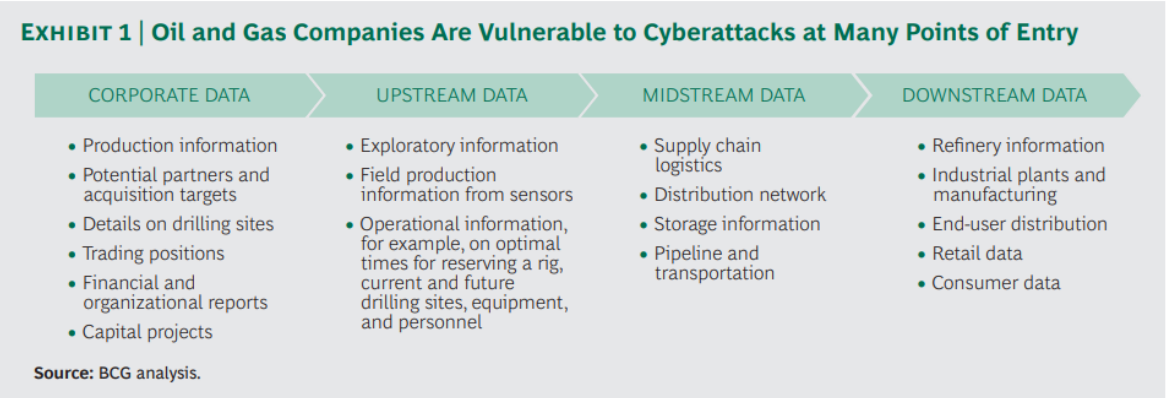
The **Colonial Pipeline,** a private company that controls a major piece of US energy infrastructure and supplies nearly half of East Coast liquid fuel, was attacked with ransomware in May 2021. This attack demonstrates the vulnerabilities of OT and connectivity, according to the FBI. It was attributed to a Russian cybercrime gang. As the ransomware attack did not directly target the OT but the IT, the OT was shut down to prevent the risk of the attack and to ensure the safety of the OT. (Watney,2022)

According to Global Data's last report, the ONG industry is becoming more digitalized, making it more vulnerable to cyberattacks. They advise companies to strengthen their cybersecurity strategies in line with their digitalization plans. From the Colonial Pipeline attack (05-2021), researchers agree that the sector became more aware of its vulnerabilities. As a result, more spending was made on cybersecurity. Global Data estimates that by 2025, cybersecurity revenues in the energy sector will reach US$10 billion. Cybersecurity risks are still not taken seriously enough despite increased cybersecurity spending. The digitalization wave creates new access points for hackers. Only 20% of the largest oil and gas companies had a CISO (Chief Information Security Officer) on their board, suggesting that cybersecurity is not a priority. (Global Data Report, 2022)

Oil and gas companies will need to become increasingly proactive in addressing cyber-threats. It is predicted that cyber-threats will become the biggest threat in the future for them. As well as oil and gas facilities in high-risk areas, there are also facilities in low-risk areas that are at risk of cyber-attacks. As cyber-threats become deadlier, they will aim to cause explosions inside facilities, putting employees' safety at risk. If this threat is not addressed, severe consequences can result, as well as a significant loss of revenue, be it from the recovery process or from the halting of various operations. In order to minimize cyber threats' impact, ONG companies must develop effective management strategies.

In order to manage risk better, companies will need to analyze cyber-attacks in the oil and gas industry in greater detail in order to better understand and explain them. (McEwan,2020)

Oil and Gas Companies are vulnerable to cyberattacks at different points of entry in their supply chains as illustrated below.



(Rick, 2016)

In the past, oil and gas companies considered the traditional upstream systems to be relatively safe, as they were, in most cases, isolated. In addition to the ever-increasing demand for real-time data and analytics, the growing use of connected industrial systems and networking technology has created new risks for the industry. As compared with corporate and retail segments in the industry, the upstream segment is relatively unprotected against asymmetrical threats. Using nonstandard equipment and potentially insecure technologies and relying heavily on oilfield-services companies further increases the risk associated with the upstream segment. Illustration below shows why the upstream is particularly more vulnerable. (Rick, 2016)

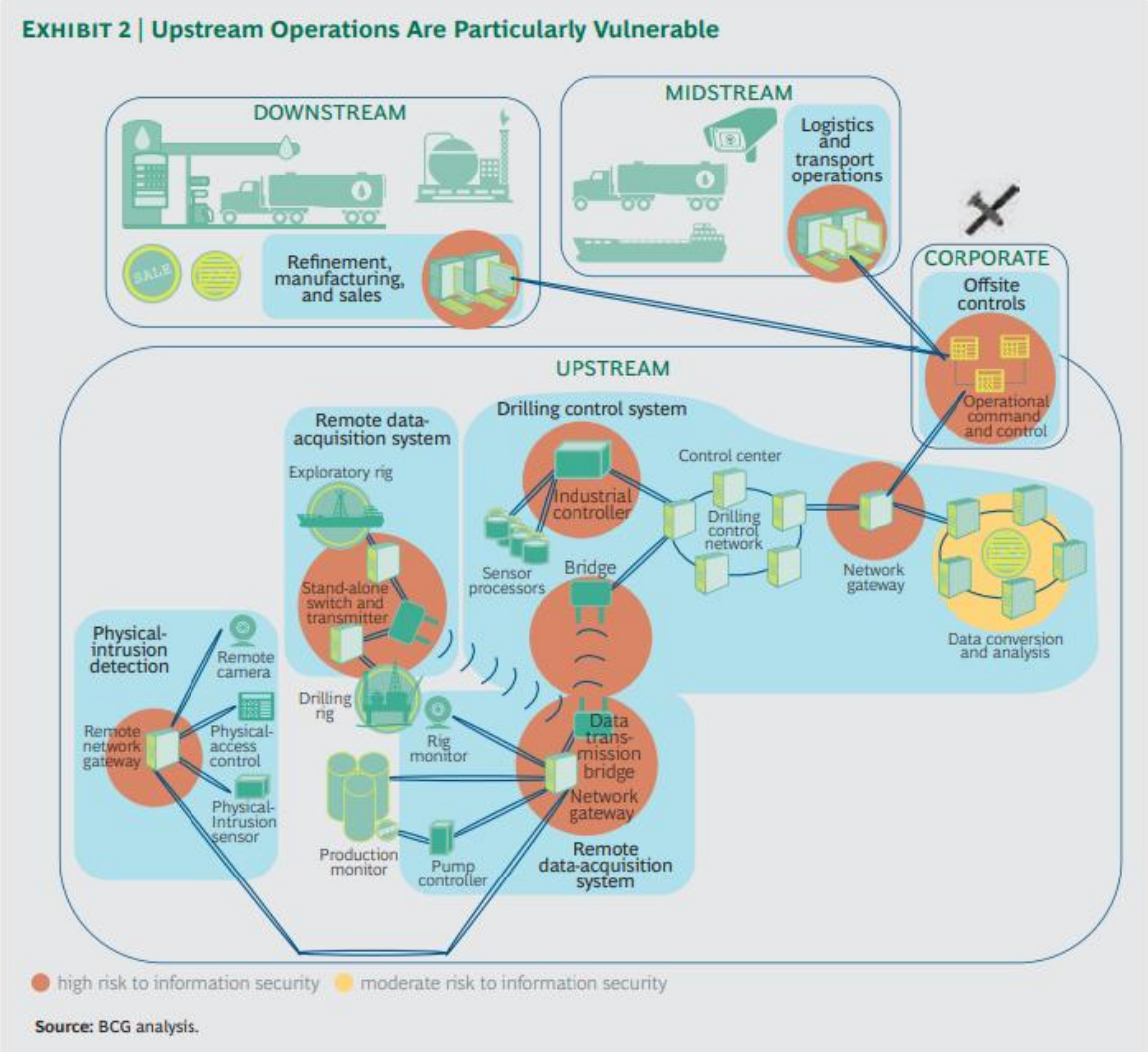


EXHIBIT 2 | Upstream Operations Are Particularly Vulnerable
DOWNSTREAM
MIDSTREAM
Logistics and transport operations
CORPORATE
Offsite controls
Refinement, manufacturing, and sales
UPSTREAM
Remote data-acquisition system
Drilling control system
Exploratory rig
Industrial controller
Control center
Drilling control network
Network gateway
Operational command and control
Sensor processors
Bridge
Stand-alone switch and transmitter
Data conversion and analysis
Physical-intrusion detection
Remote camera
Drilling rig
Rig monitor
Remote network gateway
Physical-access control
Data trans-mission bridge
Network gateway
Physical-Intrusion sensor
Production monitor
Pump controller
Remote data-acquisition system
high risk to information security
moderate risk to information security
Source: BCG analysis.

(Rick, 2016

Securing the ONG sector against Cyber Threats

Responsibility of securing the ONG sector against Cybersecurity risks. –

Because ONG Companies are considered critical national infrastructure, their protection is not only the responsibility of the company's NOC (National Oil Companies) or IOC (Independent Oil Companies), but also the government.

This shared responsibility of securing the ONG sector must, among other things, consider the following: adequate budgeting for both IT and OT network security, as well as data security. In order to maintain continuous operation for critical assets where continuous operation is required, cybersecurity must be extended across the entire organization because of the complexity of the sector and its systems.

As well as designing comprehensive security policies, training is required to implement them, audits are required to ensure compliance, and monitoring systems are required to detect changes. Since OT systems place a high priority on reliability and stability, some risks will remain in place. Therefore, policies need to address their mitigation and management based on the likelihood and potential impact of these risks.

ONG as Critical Infrastructure. -

Critical infrastructure is a national security vulnerability. Any cyberattack against an organization that provides critical infrastructure products or services poses a potential significant risk. The US Department of Homeland Security (DHS) states that critical infrastructures provide essential services to support American society and serve as a backbone for the US economy, security, and health. The DHS considers 16 sectors to be part of the critical infrastructure, including chemicals, communications, defense, emergency services, energy, food and agriculture, government, healthcare, manufacturing, and transportation. Organizations and networks operated by these industries could be incapacitated or destroyed, resulting in monstrous impacts on other business and government Cybersecurity systems, economic security, national security, and public health. (Lamb, 2018)

Because the modern world relies heavily on oil, oil and gas industry security is crucial for national and global security and The ONG Sector is considered as critical infrastructure.

In addition to the risks faced by most organizations, oil and gas companies face additional risks as critical infrastructure becomes more interconnected and interdependent. The compromise of a critical infrastructure asset can also result in a domino effect that affects others, leading to cascading consequences across the economy. The sophistication of cyberattacks has increased over the years. (Watney- 2022)

Industrial Control Systems (ICS) are becoming increasingly dependent on the Internet of Things (IoT) connections, especially for Critical Infrastructures (CI). It is becoming increasingly common for cybercriminals to target Operational Technology (OT) environments, including water systems, energy plants, transportation, communication, critical manufacturing, etc. As cyber-attacks against critical infrastructure (ICS) can result in physical disruption and human death, Critical Infrastructure Protection (CIP) has become an increasingly relevant topic in the global industrial environment. In CI, each country approaches cyber threats differently, and the growing number of disruptions has led to huge investments in cybersecurity. Many businesses fail to secure their networks adequately: there are many proposed methods to secure vulnerable networks, including Blockchain technology and mechanical analogy components that are un-hackable. With innovation comes a new concept of cybersecurity, as protecting CI becomes more difficult from both IT and OT perspectives. In light of the global trend that indicates that Critical Energy Infrastructures will be a major target of cyberattacks, it is essential to both enhance their protection and raise awareness about the general lack of preparation regarding the development of an effective cybersecurity strategy for critical energy infrastructures. (Pleta-2020)

Critical infrastructure cybersecurity government bodies around the world

Here are some examples of government bodies that oversee cybersecurity in critical infrastructure:

European Union (EU)

ENISA (‘European Union Agency for Network and Information Security’) is the EU agency that oversees cybersecurity, and the EU takes cybersecurity seriously by implementing numerous initiatives. In addition to providing support to member states, EU institutions, and businesses, ENISA strengthens its role in the implementation of the NIS (Network Information Security) Directive. A permanent mandate has been granted to ENISA, which now has the power to enhance both operational cooperation and crisis management across the EU.

Although ENISA was founded in 2004, it has been playing an increasingly important role in European cybersecurity policy over the last few years, but it is not a recent actor in the European governance system. Previously considered an advisory body to European governance, the agency now influences key cybersecurity policies at the national level. The evolution of ENISA, from advisor to operational actor, wasn't a linear process, and it faced numerous challenges and conflicts throughout its lifecycle. There was only one thing at the core of ENISA's mandate that caused these confrontations: whereas the European institutions called harmonization of the single digital market a matter of national security, the Member States considered it a matter of national security. Indeed, ENISA's governance influences policies such as the protection of critical infrastructures throughout the Union as well as the establishment of common certifications regarding ICT products and services. Thus, ENISA's mandate includes both economic and security aspects. (Brun,2018)

United States of America (US)

As 16 critical infrastructure sectors touch numerous aspects of American society, cybersecurity of critical infrastructures is an essential topic within national and international security. Due to the lack of adequate cybersecurity controls within critical infrastructure sectors, the country is vulnerable to an attack that could impact national

security, public health, safety, and economic security. As a result of the importance of this matter, the Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience outlines a national strategy for strengthening and maintaining critical infrastructure that is secure, functional, and resilient. As the United States' risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) is part of the Department of Homeland Security (DHS). A Knowledge Unit (KU) has been approved by other organizations, including the National Security Agency (NSA), to address cybersecurity for critical infrastructures. (Dawson,2021)

To enhance critical infrastructure security and resilience, these government institutions coordinate efforts with public and private sector partners. An executive order issued by the government in 2021 aimed at modernizing the nation's cybersecurity: Companies doing business with the federal government must comply with certain standards, which improves the security of government software.

Cybersecurity breaches that could affect US networks must be reported to the government by IT service providers, and certain contractual barriers must be removed to prevent providers from reporting them. The establishment of a “Cybersecurity Safety Review Board” which comprises public- and private-sector officials, which can convene after cyberattacks to analyze the situation and make recommendations. What is mentioned above are only a few steps that the US has taken to tackle the problem oy cybersecurity threats to the critical infrastructure. (Watney, 2022)

Cyber Risk assessment in the ONG Sector, Cybersecurity Capability Models. -

To effectively manage risk, organizations must understand the risk of an event and the potential repercussions of it. The goal of risk management is to identify, assess, and respond to risks on an ongoing basis. Using this information, organizations can determine the level of risk acceptable for achieving their organizational goals and express their risk tolerance accordingly. In order to make informed cybersecurity expenditure decisions, organizations must understand their risk tolerance. Depending on the potential impact on

critical services, organizations may handle risk in a variety of ways, including mitigating, transferring, avoiding, or accepting it. (Cybersecurity, 2018)

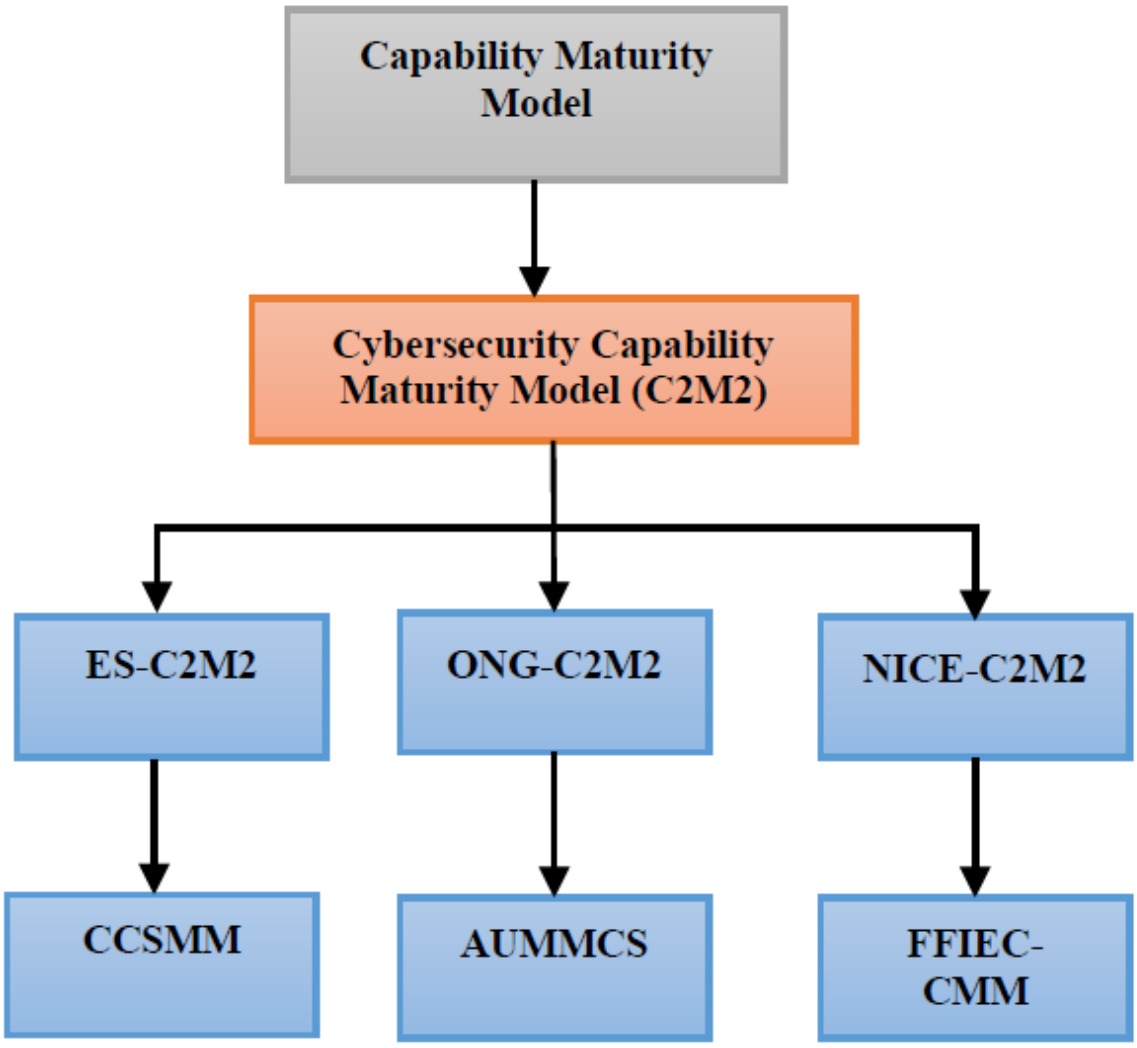
Organizations can inform and prioritize cybersecurity decisions with the help of frameworks in general through risk management processes. Organizations can utilize frameworks to select and direct improvements in cybersecurity risk management for their IT and ICS environments dynamically. In addition to providing a flexible and risk-based implementation, frameworks are also adaptable to work with a wide array of cybersecurity risk management processes. Ideally, organizations using Frameworks will be able to measure and assign values to their risks, along with the cost and benefits of steps taken to reduce risk to acceptable levels. Having a better understanding of cybersecurity risks, costs, and benefits will help an organization make more rational, effective, and valuable cybersecurity investments and approaches. (Cybersecurity, 2018)

Cybersecurity Capability models are part of frameworks developed for the response to cyber incidents in critical infrastructures. The convergence of IT and OT technology brought to life a new concept of online systems, alongside multiple innovations in the management of Critical Infrastructures (CI).

Using a maturity model, an organization can assess how well its security practices and processes are following industry best practices. Over time, this can result in a more robust security footing, reducing the number of successful cyberattacks and allowing for a quicker return to normal operations when an attack occurs. In spite of the fact that maturity doesn't necessarily mean security, a higher level of maturity means security practices and policies can be repeatable and measurable, which can be useful tools for improving security. Using a maturity model, organizations can determine what steps need to be taken to improve security. Maturity, however, has a cost. The process of progressing even a single step along the maturity model can be extremely challenging in large enterprises. (Holcomb, 2016)

The cybersecurity maturity model has emerged from the capability maturity model that has been designed from the quality management field in the 1930s. Developed by

software engineering institutions in the 1990s, it became widely used. Almost all of these models are based on this basic model, which features a set of structured operations and activities that improve over time. A number of studies later adopted the model in order to identify or measure the maturity level of an organization, a process, or even product quality. Developed for software industries, the capability maturity model (CMM) has some key elements for an effective software development process. The model has five basic maturity levels: initial, repeatable, defined, managed, and optimizing. In order to evaluate the maturity of each process, best practices and process efficiency are provided at every five levels (Garba-2020)



(Garba-2020)

We will go into more detail about the C2M2 and the ONG-C2M2 later in this paper, so for now we will just mention the other models.

- *(ES-C2M2)- Electricity Subsector Cybersecurity Capability Maturity Model*
- *(NICE)- National Initiative for Cybersecurity Education Capability Maturity Model*
- *(FFIEC- CMM) Federal Financial Institute of Examination Council Capability Maturity Model*
- *(AUMMCS)- African Union Maturity Model for Cybersecurity*
- (CCSMM)- The Community Cybersecurity Maturity Model (Garba-2020)

ONG C2M2- Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model

The ONG-C2M2 was specifically designed to address the problems facing the oil and gas sector. It was developed or derived from the ES-C2M2 first version in order to address the unique threats and vulnerabilities of the Oil and Natural Gas subsector. Organizations can use this model as a tool to assess and benchmark their cybersecurity capabilities in the ONG sector. Through pilot facilitation and working sessions, this model was developed in close collaboration with public and private sector experts. This model covers exploration, gathering, production, processing, storage, and transportation of petroleum liquids and natural gas. Threats can occur at any point in the process, from exploration to storage, since technology is used in every step. If security is not tightened well, an attacker can interfere with the process or even stop it altogether. (Garba-2020)

In order to strengthen cybersecurity capabilities within the ONG subsector, the model can be used to: Enable ONG organizations to evaluate and benchmark cybersecurity capabilities effectively and consistently. In order to improve cybersecurity capabilities, it is important for the subsector to share knowledge, best practices, and relevant references. Enable ONG organizations to prioritize actions and investments to improve cybersecurity.

The ONG-C2M2 is designed to be used with a self-evaluation methodology and toolkit for an organization to measure and improve its cybersecurity program.

The ONG-C2M2 provides descriptive rather than prescriptive industry focused guidance. The content of the model is presented at a high level of abstraction so that it can be interpreted by subsector organizations of different types, structures, and sizes. (ONG C2M2)

C2M2 - Cybersecurity Capability Maturity Model

Developed in 2014, the Cybersecurity Capability Maturity Model was designed by Carnegie Mellon University and the US Department of Energy. Each domain consists of a set of cybersecurity practices. The model contains ten domains with grouped objectives and maturity levels that represent achievements, and many objectives are grouped into one domain to represent achievements. (Garba-2020)

Table 7. C2M2 Domains and Abbreviations

Domain	Abbreviation
Asset, Change, and Configuration Management	ACM
Cybersecurity Program Management	CPM
Supply Chain and External Dependencies Management	EDM
Identity and Access Management	IAM
Event and Incident Response, Continuity of Operations	IR
Information Sharing and Communications	ISC
Risk Management	RM
Situational Awareness	SA
Threat and Vulnerability Management	TVM
Workforce Management	WM

(Garba-2020)

Models provide guidance for implementing and managing cybersecurity practices related to information technology (IT) and operations technology (OT) assets. The framework does not replace any other cybersecurity-related activities, programs, processes, or approaches that organizations have implemented or intend to implement, including cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, and mission and business requirements. Additionally, the guidance does not

form part of any regulatory framework and it is not designed to be used for regulatory purposes. (CSM2- Model Cautionary note)

Conclusions. -

The challenges created by the integration of IT and OT for any organization are further exacerbated by two major issues in the oil and gas industry. First, the value chain is more integrated than in many other industries. Security is complex in the oil sector because it involves a number of upstream, midstream and downstream companies and organizations that engage in different aspects of the business. This environment includes independent oil companies, state-owned oil companies, smaller companies that focus on only certain streams, as well as armies of service providers and other third parties. Multiple points of entry and security gaps are created by this integration.

Furthermore, new technologies are coming into the industry at a rapid pace, adding to the complexity of a highly integrated industry already dealing with integrated IT and OT systems.

There are a number of new technologies entering the oil and gas industry that could create additional vulnerabilities, such as digital oil fields connected to cloud platforms running big data analytics, drones used for upstream surveys or environmental monitoring, and third-party companies hosting 3D modeling for wells and fields. (Holcomb, 2016)

In order for all organizations to know about cybersecurity measures, it is important to identify their organizational maturity level and knowledge of cybersecurity, as well as to know what model is used to identify the maturity level. Since cybersecurity maturity models are a new area of research and growing exponentially, there is little research on their application. (Garba-2020)

Policies or frameworks for cybersecurity in the sector should include training for implementation, audits to ensure compliance, and monitoring systems to detect changes. As the emphasis is on reliability and stability of OT and IT systems, some risks will remain,

and policies should address how to mitigate and manage these risks. In the future, these models will need to be applied to other case studies to validate their application and identify challenges.

The creation of more processes to integrate risk management practices with sophisticated cyber-security technologies may not be necessary. As a research priority, researchers should identify models that can generate vital information in a more efficient and effective manner.

No There is no doubt that the established frameworks have contributed to a greater understanding of cyber risk management, but further research and development are still required for these models. Different regions, however, need to interpret and modify these frameworks based on their differences in industrial, political, and socio-cultural landscapes.

In the oil and gas sector, effective cybersecurity must continue to be a collaborative effort involving government and industry.

Bibliography

Holcomb, Jason. "Definitive Guide to Cybersecurity for the Oil & Gas Industry." *LEIDOS Ebook Report; LEIDOS Holdings Inc.: Reston, VA, USA* (2016).

Bronk, Christopher, and Eneken Tikk-Ringas. "Hack or attack? Shamoon and the Evolution of Cyber Conflict." (2013).

Mittal, Anshu, Slaughter, Andrew, Zonneveld, Paul, “Protecting the connected barrels, cybersecurity for upstream oil and gas”, Deloitte Center for Energy Solutions, Deloitte University Press, Houston, 2017

Cybersecurity Capability Maturity Model C2M2, US Department of Energy, June 2022.

Cybersecurity, Critical Infrastructure. "Framework for improving critical infrastructure cybersecurity." *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP* 4162018 (2018).

Oil and Gas Cybersecurity Capability Maturity Model “ONG C2M2”, US Department of Energy, February 2014.

Garba, Adamu Abdullahi, Maheyzah Muhamad Siraj, and Siti Hajar Othman. "An Explanatory Review on Cybersecurity Capability Maturity Models."(2020)

Plėta, Tomas, Manuela Tvaronavičienė, Silvia Della Casa, and Konstantin Agafonov. "Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases." (2020).

Watney, Murdoch. "Cybersecurity Threats to and Cyberattacks on Critical Infrastructure: A Legal Perspective." In *European Conference on Cyber Warfare and Security*, vol. 21, no. 1, pp. 319-327. 2022.

ELAND CABLES WEB SITE: https://www.elandcables.com/the-cable-lab/faqs/faq-what-are-upstream-and-downstream-works-in-the-oil-gas-industry , In Oil & Gas what is upstream and downstream? Accessed 02-09-2022.

Dalvi, Samir. *Fundamentals of Oil & Gas Industry for Beginners*. Notion Press, 2015.

Ediger, Volkan Ş., and Istemi Berk. "Geostrategic challenges in the oil and gas sectors." In *Energy economy, finance and geostrategy*, pp. 173-197. Springer, Cham, 2018.

Mojarad, Ali Asghar Sadeghi, Vahid Atashbari, and Adrian Tantau. "Challenges for sustainable development strategies in oil and gas industries." In *Proceedings of the International Conference on Business Excellence*, vol. 12, no. 1, pp. 626-638. 2018.

Imran, Huma, Mohamed Salama, Colin Turner, and Sherif Fattah. "A systematic literature review on the technical and non-technical cyber risk management models in the oil and gas sector." *Economic and Social Development: Book of Proceedings* (2021): 218-234.

Mc Ewan, Kayla Ann. "Cyber-threats as political risk: increased risk for the oil and gas industry." PhD diss., Stellenbosch: Stellenbosch University, 2020.

Rick, Katharina, and Karthik Iyer. "Countering the threat of Cyberattacks in oil and gas." (2016).

Brun, Louis, and Rocco Bellanova. "The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity." *Université catholique de Louvain* (2018).

Dawson, M., Bacius, R., Gouveia, L.B. and Vassilakos, A., 2021. Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, *26*(1), pp.69-75.

Lamba, Anil. "Protecting ‘cybersecurity & resiliency’of nation’s critical infrastructure–energy, oil & gas." *International Journal of Current Research* 10 (2018): 76865-76876.