UNIVERSITY OF PIRAEUS
Department of International & European Studies
MSc in Energy: Strategy, Law and Economics

Cybersecurity in the energy sector

A holistic approach

Konstantina G. Vasileiou

MEN 18012

Supervising Professor: Dr. Bossis, Mary

November 2019, Piraeus

On my own responsibility and being fully aware of the penalties stipulated under article 22 par. 6 of Greek Law 1599/1986, I, *Konstantina Vasileiou*, hereby declare that the intellectual work fulfilled and submitted based on the delivered master thesis is exclusive property of mine personally. Appropriate credit has been given in this diploma thesis regarding any information and material included in it that have been derived from other sources. I am also fully aware that any misrepresentation in connection with this declaration may at any time result in immediate revocation of the degree title.

Acknowledgements

I would like to express my special thanks for her invaluable assistance and her willingness to offer her time generously to my Supervising Professor, Dr. Mary Bossis. I would also like to thank my parents and my friends for their encouragement and support during the writing of this thesis.

Dedicated to my parents, Gregory and Anna

Table of contents

Executive Summary

Energy has been over time a sector of national interest and thus extremely vulnerable to risks. The emergence of new technologies revealed a new, unknown peril for the energy industry. Cyber threats are permanent and persistent risks that can disrupt energy supply and cause financial, environmental or any other kind of damage. This thesis offers a holistic approach to cybersecurity as a coordinated response to cyber threats.

In the first chapter of this thesis is presented the evolution path of the energy sector, which is characterized by the energy transition that goes hand in hand with the digitization of the energy infrastructure and the market and organizational changes. Despite its positive contribution to the energy industry, this evolution has revealed many vulnerabilities and cyber threats that stakeholders need to overcome.

In the second chapter, the interest is focused on answering some basic questions about the nature of cyber-attacks, the types, their origins, but most important the motives behind them and their severe impacts. What is more, some of the most popular cyber-attacks in the energy sector are described in detail.

The last chapter attempts to approach the notion of cybersecurity and correlate it to the broader concept of energy security. Deconstructing the doctrine of cyber governance, this thesis reaches some interesting conclusions about the proper environment and the actors that could achieve the ideal level of cybersecurity and bring this venture to fruition.

Introduction

Historically, energy security was associated with the undisrupted supply of oil in an affordable price. Today, though, this approach is obsolete. The digitization of energy infrastructure through the deployment of Information and Communication Technologies (ICTs) as well as the growing deployment of renewable energy sources are characteristics of the upgrade of the energy industry during the last decades. This 'revolution' may have increased the rationalization of the energy production and the efficiency of consumption, but it has also multiplied the challenges the energy industry is facing. So, besides the classic threats against energy security, cyber threats come to be added. The question that naturally arises is "How can the security of cyberspace be ensured?" Critical infrastructure networks are interconnected and their protection mechanisms are usually outdated. Many cyber-attackers have taken advantage of these vulnerabilities over time, each having different motives, from financial to political ones. Cyber criminals, state sponsored actors, hacktivists and terrorists are included in the attackers. The energy sector is considered to be among the five most targeted sectors worldwide.[1] Undoubtedly, energy is a sensitive and financially lucrative sector, on which lies the national security and the proper economic and social balance of a state. Thus, cybersecurity is an issue of big concern, since a cyber-attack could cause from operational or financial disruption to massive environmental damage or even loss of life. The need for resilient energy infrastructure and robust and stable systems has become a priority for states, system operators and the whole energy industry. In a global scale, there have been set multiple national policies and legislative frameworks to deter cyber threats and raise awareness about cybersecurity issues. Indeed, this October, Europe established for the first time the campaign of European Cybersecurity Month (ECSM), similar to the National Cybersecurity Awareness Month (NCSAM), a campaign held every October in the U.S. to raise awareness and educate people and industries on how to protect from digital assaults. Yet, the absence of international cooperation and common developed standards and norms against cyber risks undermines any effort to effectively address the issue.

[1]Candid Wueest (2014), Targeted Attacks Against the Energy Sector, Symantec Corporation.

This thesis aims to shed light on a route that starts from the fact that the energy sector is a prime target of cyber-attacks and ends up with the awareness of the need for a collective cybersecurity strategy. It is a scientific document aiming to provide a comprehensive picture of the current situation in the energy cyber ecosystem. It describes the state of relations in cyberspace, answers the questions why the energy sector is an attractive target for cyber-attacks, which are its vulnerabilities, which are the attackers' motives and analyzes the efforts of governments, companies and every stakeholder to build resilience walls and ensure cyber hygiene against cyber-attacks. Last but not least, it demonstrates the current cybersecurity policies and strategies and underlines the need of harmonization and international cooperation. Cybersecurity in the energy sector is a newly analyzed matter and each report approaches it from a different perspective. This thesis' purpose is to introduce the readers to an issue that is unknown to the general public and make them familiar to it. At the same time, a reader familiarized to the issue of cybersecurity, through this document can understand the correlation of cybersecurity and energy and reflect on the policy recommendations for governments and energy companies respectively.

1 A power sector in transition

Critical infrastructures are essential for the smooth functioning of the society and are considered as the backbone of a state's economic activity. Among these critical infrastructures are energy, telecommunications, health, finance, transportation, particularly air, rail and maritime; and water and wastewater treatment.[2] The energy sector consists of diverse and geographically-dispersed critical assets and systems. It is divided in four subsectors: electricity, oil and gas, including the generation, refining, storage, and distribution of oil, gas and electric power, nuclear energy and alternative fuels. It is arguably the most complicated, because all the other sectors rely on it in order to carry out their own essential services. For instance, it supplies fuels to the transportation industry and electricity to households and businesses. Any possible lack of supply of energy or potential disruption for a long time period could have significant cascading effects on the economy, impact on the industry, trade and as a result the Gross Domestic Product (GDP) of a state. Such a disruption creating the risk of a potential black-out could, among others, be caused by potential cyber incidents or cyber-attacks.

1.1 Changes in the infrastructure and Digitization

For a long period, energy systems were autonomous in relation to digital technologies, since they used mechanical or analogue equipment and had no connection to the outside world. Even if someone tried to attack a system, it could only take place by placing malicious and infiltration software in a specific installation without being able to affect the whole system. Thus, energy industry was only little exposed to the risk of cyber-attacks. [3]

However, currently, the energy industry is on the verge of a digital revolution. Digitalization 4.0 strongly benefits the energy industry enabling countless new opportunities and facilitating a more integrated, intelligent, flexible, sustainable, customer-centric system.[4]

The energy infrastructure is being modernized as a result of the integration of small-scale renewables, microgrids, distributed generation, consumer participation in

[2] Energy Expert Cyber Security Platform Report (2017), Cyber Security in the Energy Sector.
[3] Gabrielle Desarnaud (2017), Cyber attacks and energy infrastructures, ifri center for energy.
[4] International Energy Agency (2017), Digitization & Energy.

the energy market and so on. New intelligent components, such as digital valves or pumps, electricity or gas smart meters, Internet of Things (IoT) nodes are introduced in many parts of the energy grid and are based on Information and Communication Technology (ICT). [5] Respectively, new inserted methods, such as seismic studies, oil drilling, pipeline pressure and temperature management are also carried out using ICT. [6]

The deployment of ICT across energy infrastructures allows optimization and efficiency both in the supply chain and in customized services. The processes of production, transformation, storage and consumption are gradually changing. A smarter energy system can perform these processes with better precision and faster response than a human-dependent system.[7] ICT also introduces components capable of managing large amounts of data, which contribute to the rationalization of production, distribution and consumption. Finally, it facilitates the communication of different sites in a real time data system, allowing remote controlling and improving the decision making in the near future. [8]

At the heart of digital revolution in energy lies the electricity sector. Digitization plays a key role in the balancing of grids, as distributed energy sources are growing. A smart grid is "an electricity network that can intelligently integrate the actions of all users connected to it - generators, consumers and those that do both—in order to efficiently deliver sustainable, economic and secure electricity supplies."[9]. Smart grids by connecting industrial and domestic infrastructures allow to the energy industry to acquire a holistic vision of electricity generation, transmission, distribution and consumption at different levels of geographical territory and by collecting data better anticipate demand.[10]

To meet its new needs, the energy industry has turned towards industrial control systems (ICS). From a technical perspective, energy control systems involve a hierarchy of interconnected physical and electronic sensing, monitoring and control devices, acting in real time and connected to centralized control stations or centers. A

[5] Supra note 2
[6] Supra note 3
[7] ibid
[8] Arnault Barichella (2018), Cybersecurity in the energy sector: A comparative analysis between Europe and the United States," ifri center for energy.
[9] Tamilmaran Vijayapriya, Dwarkadas Pralhadas Kothari (2011), 'Smart Grid: An Overview, Smart Grid and Renewable Energy, 2, 305-311.
[10]Supra note 8

modern power system includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs) and programmable logic controllers (PLCs). In particular, SCADA systems are the central nerve system that provides provides monitoring and control operations of transmission and distribution networks dispersed over large geographic areas. DCSs control local facilities in a small geographic area or single facilities. SCADA and DCSs are connected to remote components such as remote terminal units (RTUs) and programmable logic controllers (PLCs). [11]

The digital revolution in the energy sector has revealed technological innovations such as the growth of Internet of Things, which allows users to connect household appliances and the energy infrastructure. As billions of new devices become connected, large amounts of data are being generated from ICS networks and customer information systems. Data Analytics are techniques applied in order these large data sets, 'big data' to be managed and turned into useful information.[12]

The exponential growth of data made obvious the need for data centers and network services.[13] Nevertheless, when it comes to data processing and storage, cloud data services are more cost-effective than running up a data center.[14] Cloud computing is based on the delivery of computing as a service and allows the fast development of integrated infrastructures. Taking a closer look at the energy sector, oil and gas companies are increasingly creating subsidiary firms and groups of partners, service organizations, consultants outside the protective membrane of the company. Cloud computing allows them to communicate and exchange data without restrictions and delays.[15]

[11]Fleury T., Khurana H., Welch V. (2008) Towards A Taxonomy Of Attacks Against Energy Control Systems. In: Papa M., Shenoi S. (eds) Critical Infrastructure Protection II. ICCIP 2008. The International Federation for Information Processing, vol 290. Springer, Boston, MA.
[12]Richard J. Campbell (2018), Electric grid cybersecurity, Congressional Research Service.
[13] Supra note 4
[14]Antonello Monti et al.(2018), Digitalization of the energy system and customer participation: Description and recommendations of Technologies, Use Cases and Cybersecurity, ETIP SNET.
[15] Pradeep Kumar Kukreja, SRM Karnawat (2012), ONGC, Cloud Computing – Next generation tools for Oil and Gas Companies?, 9th biennial international conference & exposition on petroleum geophysics.

The introduction of blockchain technology is relevant to the management of decentralized complex energy systems and microgrids, but also to the wholesale energy trading facilitation.[16]

1.2 Changes in the market – Organizational changes

The energy field during the last years has undergone profound changes. The two main poles of these changes are market liberalization and competition. The deployment of digital technologies and the shift towards renewables made new players get involved in the energy scheme, such as aggregators, prosumers and third parties managing supply and demand.[17] Operators use demand-response for the balancing of demand and supply, which at the same time affects the cost of energy in the wholesale and retail market. The introduction of renewable resources has also changed the market environment through dynamic pricing. Moreover, the development of renewable energy systems and the public awareness about climate change have been crucial factors for the emergence of decentralized energy systems. Distributed energy systems bring the production closer to the consumer, enable energy collection from different sources and may reduce environmental impacts and improve security of supply.

1.3 Threat landscape

Nothing comes without a price. The widespread use of ICTs creates vulnerabilities and increases the risk of cyber-attacks. The threat landscape that has been set imposes many challenges to the cybersecurity objective.

First of all, industrial networks from relatively isolated and protected have been opened up to new technologies and actors outside the utilities. ICS may be less expensive than proprietary control systems, but they are more familiar to the general public and thus more vulnerable.[18] An energy control system that is under attack cannot be easily disconnected from the network as this could result to malicious software diffusion not only to a specific installation, but to whole businesses and their subsidiaries, proving that the danger of contagion is here and growing. Especially attacks on SCADA systems can give the attackers direct control of operational

[16] Merlinda Andoni et al.(2019), Blockchain technology in the energy sector: A systematic review of challenges and opportunities," Renewable and Sustainable Energy Reviews 100, 143-174.
[17] European Cyber Security Organisation (2018), ECSO Energy sector report.
[18] Supra note 7

systems, which could lead to large scale power outages. The complexity of the coexistence of the old and new components of the industrial networks has also resulted in poor protection from the risk of cyber-attacks. The first ones are often aged and not programmed to use encryption or authentication protocols and thus are vulnerable to security risks. As a consequence, a complex landscape is slowly being created, where businesses add new layers of interconnectivity between themselves, their partners and customers.

Secondly, the interconnectivity of electrical grids and transport pipelines threatens the stability of networks and the reliability of energy systems. If the main system commanding the transmission or the distribution is attacked, the consequences for the balancing of the grid will be enormous. In any case, everything connected to the internet is inherently vulnerable to hacking. Security issues are also challenging in renewable energy generation, since it consists of highly interconnected systems and the production is controlled by central stations. Jason Staggs, a security researcher at the University of Tulsa stated that "It's a matter of having physical access to one wind turbine to rule them all."[19]

One important aspect of this challenge is the so called "weakest link" problem. This problem indicates that an interconnected system is as robust as the weakest part of it.[20] As a result, operators with low protection against cyber-attacks bear higher risk for causing blackout to operators with low system vulnerability. Therefore, for example, in the worst-case scenario that an attack in the European electricity grid takes place, even if it would initially have only regional impact, there is a high probability of a cascading effect on other Member - States too. In such a case, it is supported that only the British Isles would escape damage, because of the direct current (DC) lines that isolate them from the European network.[21]

Another serious concern is that decentralization led some countries to open their energy markets to smaller private suppliers. Their power plants like wind turbine or photovoltaic sites are included as components in power grids and affect the stability of the whole system. Taking into consideration that most of these operators do not

[19]Jarno Lötjönen (2018), Cyber Security in robotics, energy and health, JYVSECTEC/JAMK.
[20] Supra note 2
[21] Supra note 3

collaborate with IT experts and their computer technology remains uncontrolled, their systems' vulnerabilities could infect the grid.

Thirdly, the introduction of new highly interconnected technologies, as described above in detail, has also introduced the vital need of effective management and attention on cybersecurity risks emerging from this changing environment.

In particular, the deployment of the Internet of Things, which allows users to connect household appliances and communications' equipment with the energy infrastructure, widens the "attack surface", provides more entry points in the network and leads to a potential cyber assault.[22]

In addition, cloud computing has led to the outsourcing of information infrastructures and services. Outsourcing makes the highly reliable energy sector dependent on other sectors, which do not meet the requirements of robustness of an energy system. Having in mind that energy systems are also important for the national security, the decision to outsource critical infrastructure and services could possibly threaten the sovereignty in a case of conflict.[23] Another example of risk due to the energy transition is the limited security and data protection of smart meters.

To sum up, the growth of the Internet of Things, the cloud, big data are digital phenomena accompanied by a growth in the exposure of vulnerabilities.

Growing interconnectedness with the wider use ICT is a major threat in oil and gas industry, especially in upstream operations. High drilling activity, digital oil fields or smart fields, data based interaction between refineries and headquarters are only a few paradigms of the intrusion of ICT in Oil and Gas industry. The convergence of the already complex ecosystem in oil and gas companies with the deployment of ICT in many stages of the process has outpaced the industry's cyber maturity.[24]

Last but not least, a severe challenge for the energy industry to overcome is the lack of qualified human resources. ICT is difficult to handle and education

[22] International Renewable Energy Agency (2019), A New World: The Geopolitics of the Energy Transformation.
[23] ibid
[24] Deloitte Center for Energy Solutions (2017), Protecting the connected barrels: Cybersecurity for upstream oil and gas.

programs that cultivate sector specific skills are few. As a result, cyber attackers meet no obstacle to enter an energy system and disrupt it.

Nevertheless, cyber risk should not be solely considered as a pure IT risk, but as a key operational risk, that should be addressed systemically across the entire supply chain in order an effective risk management to be accomplished.[25]

1.3.1 The case of nuclear energy

Over the years nuclear power plant facilities have developed robust safety mechanisms because of the high possibility of facing physical risks. These mechanisms can also be used to address cybersecurity risks. First of all, equipment and communication processes are duplicated and the only information that a third party can have access to is data about voltage and power.[26] Moreover, nuclear facilities have developed many back up and emergency power systems, especially after the accident in Fukushima. Nuclear power plants may use ICS within a secure environment, but the increase in the use of information technology to monitor these control systems creates uncertainty towards cyber threats. In any case, the nuclear energy industry is a highly controlled sector and any form of attack is difficult to perpetrate its networks and cause extensive damage.

[25] World Energy Council (2016), World Energy Perspective – The road to resilience: managing cyber risks.
[26] Supra note 3

2 The energy industry under attack

During the last years cybersecurity is an issue of particular concern for the energy industry and is considered among the highest priorities for utilities and governments globally. Especially in parts of Europe and North America, cyber threats are among energy leaders' top uncertainty issues.[27]

Cyber-attacks to the energy sector are not a new phenomenon. Nevertheless, cybersecurity was not considered a realistic threat and thus energy systems never had security protocols attached. Energy companies could repel this danger by isolating the infected component of the system.[28] Today, things have changed due to the openness and interconnectivity of the networks. Since systems need to be updated and be "on" all the time, there is no time for their security improvement. We should also have in mind that buying energy systems equals to a long term investment, so such systems are not even easily replaced if vulnerable.[29]

The energy sector is an increasingly privileged target of cyber-attacks over the last few years due to its critical role for the national economies. In 2016, energy was the second most vulnerable industry to cyber-attacks.[30] Statistics on cyber-attacks may vary depending upon the source, but all agree that numbers are growing. According to a Symantec Corporation study, during the monitoring period from July 2012 to June 2013, there was an average of 74 cyber-attacks per day globally, from which 9 per day had targeted the energy sector.[31] Symantec Corporation also estimated an increase in energy sector cyberattacker groups, from 87 in 2015 to 140 in early 2018.[32] In 2014, the American authorities were solicited 245 times for attacks in industrial systems, almost a half of which considered as advanced persistent threats.[33] Almost 80% of EU businesses have experienced at least one cybersecurity incident in 2016.[34] The magnitude of the situation is also obvious from data published in Houston Chronicle according to which "Exxon Mobil reportedly blocks 64 million emails, 139

[27] Supra note 25
[28] ibid
[29] Candid Wueest (2014), Targeted Attacks Against the Energy Sector, Symantec Corporation.
[30] Supra note 24
[31] Supra note 1
[32] Don C Smith (2018), Enhancing cybersecurity in the energy sector: a critical priority, Journal of Energy & Natural Resources Law," 36:4, 373-380, DOI: 10.1080/02646811.2018.1516362
[33] Supra note 8
[34] Europol (2017), Internet Organised Crime Threat Assessment.

million Internet access attempts, and 133,000 other potentially malicious actions every month."(March 2, 2017).[35]

Cyber threats today tend to acquire a more sophisticated and dynamic character. The improvement of the know-how of attackers and the poorly trained staff, on the other side, increase the phenomena of cyber breaches. As defenses are enhanced, attackers adapt and innovate.[36]

In 2012, Robert S. Mueller, III, Director of the FBI stated: "There are only two types of companies: those that have been hacked, and those that will be. And even that is merging into one category: those that have been hacked and will be hacked again." [37]

Most cyber-attacks in businesses target sensitive or financially lucrative data, such as business secrets, confidential or banking data or medical records.[38] However, the double character of the energy industry, both private and public, reveals except for financial also political motives to cyber incidents. The importance of the energy sector both strategically and for other vital state functions, such as defense and communications, creates a battleground for geopolitical confrontation between great powers.

2.1 Defining cyber threats

According to the Regulation 2019/881 of the European Parliament, "cyber threat means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons."

Generally, a security risk in the energy sector can vary from a simple security incident, a security breach or a data breach.

A security incident can have as root causes environmental conditions, such as floods, but also human error, malicious attacks, hardware or software failures, and third party failures. A security breach is a security incident, usually of malicious nature, that creates the need of penetration of a barrier or some other form of security mechanism.

[35] Karen E. Kahle et al. (2017), Cybersecurity and the Energy Sector: Practical Considerations, Powerpoint Presentation.
[36] Marsh (2015), Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers.
[37] Cyber Security Conference, San Francisco, CA March 01, 2012.
[38] Supra note 25

A data breach takes place when the incident has impact on data that could harm the functioning of the system, such as a fraud committed by misuse of data or any liability arising from data storage. [39]

Yet, not all of these incidents can be considered as cyber-attacks, but as a precursor to possible cyber-attacks. Cyber incidents, in order to be called attacks, should cause physical or non-physical damage.

In particular, physical damage is caused when attackers target the integrity of information by infecting software, which can cause supply disruptions, blackouts and generally impact control systems. Non-physical damage is caused when attackers target the availability and confidentiality of information[40] and includes data corruption, theft of intellectual property, extortion or the threat of extortion and theft of private or financial data, such as theft of business strategy projects, employee and payments information and so on.[41]

2.2 Definition of cyber-attack

For NATO, a cyber attack is "an action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself."[42]

For EU, there is no definition as cyber-attack. The term that is used is the 'attack vector'. "An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome".[43] According to the European Union Agency for Network and Information Security (ENISA), cyber-attacks cover all cyber incidents triggered by malicious intent where damages, disruptions or dysfunctionalities are caused.[44]

For US, a cyber attack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the

[39] Mr Neil Robinson et al. (2013), Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts, Directorate General for internal policies policy department A: economic and scientific policy industry, research and energy.
[40] ibid
[41] Supra note 25
[42] NATO Glossary of Terms and Definitions, Edition 2014.
[43]Koufopoulou, A. Ioanna (2019), "The Evolution of Cyber Terrorism and a possible electronic Pearl Harbor; The case of Stuxnet, Department of International and European Studies, University of Piraeus
[44] Louis Marinos and Marco Lourenço (2019), ENISA Threat Landscape Report 2018.

data or stealing controlled information." [45] We observe that despite the dramatic increase of cyber-attacks, there has been no international treaty providing a mutually acceptable legal definition.[46]

2.3 Types of attacks

The most common types of attacks are the following:

- *Malicious software (Malware)*: a general term for a file or a programm is designed to harm devices or networks .It can include viruses, worms, Trojan horses, spyware and ransomware. *Ransomware* encrypts data and disrupts the access of users to files until they pay a ransom or carry out a specific action. [47]
- *Distributed Denial of Service (DDoS)*: attacks on energy generation and delivery systems that make services or resources unavailable by flooding them with more requests than they can handle.[48]
- *Social engineering or (spear) phishing*: cyber incidents that allow unauthorized access to networks for data theft or cyber espionage. Usually in the form of emails appearing to come from reputable sources, that manipulate users to disclose confidential information.[49]
- *Advanced persistent threats (APTs)*: multistage, multidisciplinary attack with the aim to remain undetected for the longest possible time period. APTs are usually state-linked and target critical sector such as energy.

However, cyber incidents are not always external, but they can be also internal. For instance, as an internal cyber incident could be characterized employee negligence. Given the complexity of cyber space and the lack of training of employees, *human errors* should be taken into serious consideration. People are the weakest link of the production and that is why attackers target them by delivering malware through emails or USB sticks.

Several times, except for human errors, the phenomenon of intentional or malicious actions of employees or former employees has been observed. These are

[45] Committee on National Security Systems CNSSI No. 4009 April 6, 2015.
[46] Carr Jeffrey (2010), Inside Cyber Warfare, O' Rilley Media Inc., Sebastopol.
[47] Pablo Gutierrez Astilleros et al. (2018), Cybersecurity Guidelines and Best Practices for Emergency Services," European Emergency Number Association (EENA) Document.
[48] European Court Of Auditors (2019), Briefing paper Challenges to effective EU cybersecurity policy
[49] ibid

the so called *insider attacks*.[50] The target of an insider attack is not always clear. An insider might use this "power" to gain account privileges and a former employee might want to take revenge for their dismissal. In any case, an insider is a person that is or was close and trusted to the business.

2.4 Origin of attacks

Cyber threat agents vary from state actors to non-state actors, such as cyber-criminals, insiders, cyber-spies, hacktivists, cyber-offenders, cyber-fighters, cyber-terrorists and script-kiddies. It should be noted that the sequence of mentioning these actors is according to their engagement in the threat landscape.[51]

In 2019, *cyber-criminals* remained the most active threat agent group in cyberspace, being responsible 78% of the registered incidents. They are ranking from rogue hackers that target victims with high monetization potential, to terrorist organizations. Cyber-criminals also make significant income by providing services that are sold as "Crime-as-a-Service".[52]

Hacktivists try to make their voice be heard on issues of political nature, religious belief or social ideology. According to Dan Lohrmann, chief security officer for Security Mentor " Hacktivism is a digital disobedience. It's hacking for a cause."[53] A characteristic paradigm of hacktivism, is the attack named "Operation Petrol" of Anonymous group in 2012, which hacked into servers of multiple international oil companies in order to protest against drilling plans in the Arctic.[54]

Insiders remain quite high on the list of cyber attackers. This group of attackers consists of malicious, accidental or negligent insiders.

In 2019, the activity of *Nation States* in cyberspace occupies a large slice of the pie of cyber threats and thus has been encountered several times in the international headlines. It can range from cyber espionage to cyber warfare and must be analyzed under the prism of diplomatic, geopolitical and military developments.[55]

---

[50] Supra note 39
[51] Internet Organised Crime Threat Assessment (2018), EUROPOL.
[52] Supra note 44
[53] JavaTpoint, Types of Cyber Attackers, https://www.javatpoint.com/types-of-cyber-attackers
[54] Hackers Attack Servers of Oil Companies Working in Arctic, *The Moscow Times*, 16.07.2018, https://www.themoscowtimes.com/2012/07/16/hackers-attack-servers-of-oil-companies-working-in-arctic-a16275

[55] ibid

Infrastructure companies, such as energy firms, are mainly vulnerable to attacks by profit-seeking criminals or Nation States with geopolitical motives.[56]

2.5 Attack motives

The classification of a cyber attack is mostly dependent on the motive of the attacker. There are cases that the attacker is motivated by financial factors. Cybercriminals, who belong to this category of attackers, do not have the need to disguise their motive, since their only concern is to avoid legal enforcement. On the other hand, attackers who are motivated by political and geopolitical reasons have a strong incentive to hide their identity.

The motives of cyber-attacks in the energy sector are pretty much the same as the motives of cyber-attacks in general. Energy businesses are financial colossuses, with vulnerable control systems and are included in the critical infrastructure responsible for the smooth functioning of a nation state.

2.5.1 Financial motives

The majority of cyber-attacks against information systems and their data are financially motivated. Non-state actors are a considerable danger in cyberspace and mainly consist of cyber criminals.

Cybercrime is the "criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes data theft, fraud and internet scams among other activities. Cybercrime is distinguished from other forms of malicious cyber activity, which have political, military or espionage motivations."[57]

Obviously, cybercrime is popular in the energy sector, because as a critical infrastructure is considered to be extremely lucrative.

Cybercriminals invade into the control systems or the grids of energy firms, either for criminal purposes, such as *data theft or fraud* or to commit *industrial espionage* seeking any valuable information, such as maps of new gas fields or documents about targeted plants. The information gained can be sold to competitors or can be used by the attackers in order to make profit by blackmailing the company. For instance, in January 2013 a group claiming to be Anonymous posted access details to Israeli

[56] F-Secure white paper (2019), The state of the station: A report on attackers in the energy industry.
[57] Tim Maurer & Robert Morgus (2014), Compilation of Existing Cybersecurity and Information Security Related Definitions.

SCADA systems for power plants. [58] In December 2014, attackers against the operator of South Korean power plants released sensitive and confidential information online, including the plant's equipment designs and manuals.[59]

The energy sector is also a target of *sabotage attacks.* This kind of crimes can be committed through a disruption in a specific financial service as a form of violation of the integrity, confidentiality and availability of a system. To achieve this, the attackers use the stolen data. Sabotage is a form of gaining indirect profit, for example as a competitor who wants to ruin the reputation of their rival company.[60]

So, we conclude that cybercrimes seem to have a pure opportunistic character and this financial motivation has led to the formation of a well-organized crime market for trading in malware and stolen data.

Nevertheless, the profitability of cybercriminals is limited. In order to attack the industrial control systems of an energy company, except that they need specific technical knowledge, they also need means within which they do not have access.

Analysts believe that states will tolerate cybercrime only under the condition it stays at "acceptable levels", that is less than 2% of GDP.[61]

2.5.2 Terrorism

Some attacks are not solely aiming for the financial gain, but are conducted in promotion of political and social objectives, and thus have at least some elements of cyberterrorism. In order for cyberterrorism to be considered a political threat, two circumstances should be met: First of all, the target should be vulnerable to an attack that could lead to severe harm or violence and the attackers should have the motivation to carry out the attack.[62] The motivation of cyber terrorists stems from their political agenda. Their attacks are mainly directed to critical infrastructures. Under the umbrella of this political agenda cyber terrorists gather individual hackers and transnational criminals to cooperate on a common goal.[63]

---

[58] Supra note 1
[59] McCurry, South Korean nuclear operator hacked amid cyber-attack fears, *The Guardian*, 23.12.2014, https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack
[60] ibid
[61] McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies.
[62] Dorothy E. Denning (1999), Information Warfare and Security, ACM Press, New York.
[63] Murat Dogrul et al. (2011), Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism, 3rd International Conference on Cyber Conflict, Tallinn, Estonia.

Dorothy E. Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School, (2000) defines the term cyber terrorism as "the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[64] This definition is one of the many existing, since there is no consensus among scholars on a widely accepted definition.

Internet has become the new tool of terrorists, jihadists, and transnational criminal organizations (TCOs) worldwide.[65]As the active participants on the internet are increasing, terrorists use cyberspace to communicate, recruit, proselytize, make propaganda, share information about an operation and gain financial support. At the same time, Internet is a weapon in the arsenal of cyber terrorists, who can release attacks that can cause serious damages. Especially now that Internet of Things (IoT) and Big Data have widened the surface of cyber-attacks, it is much easier for them to find an entry point in systems.

Nevertheless, for the time being, cyber terrorism is not considered an imminent threat. Hardly does one think of cyber-attacks against critical infrastructure via a computer virus or by an enemy sitting on his couch in a "rogue" or "failed" state and away from the calves of the law. Virtual attacks may cause billions of dollars of damage in a national economy, but they are not so photogenic. The main purpose of terrorists is to spread terror and panic and it can only be achieved through traditional terrorist activities, such as bombings and suicide missions. One could argue that a cyber attack in a control system of a nation's critical infrastructure could also have terrifying

[64] Supra note 62
[65] José de Arimatéia da Cruz, Terrorism, War and Cyber (In)Security, *Small Wars Journal*, 27.10. 2013, https://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity

physical impacts, but the likelihood of such an attack is unknown.[66] Terrorists lack the sophistication and capability to attack a critical infrastructure due to its complexity and the outcome of the attack is not so certain.

It has, though, been expressed a completely opposite view that with traditional terrorist activities, the public opinion pays attention to a possible loss of life or destruction of a property and the main purpose of this attack stays in the background. A virtual attack that can be conducted remotely and anonymously, by affecting wider amount of people, may give greater political and social substance to the operation and for this reason may be preferable by terrorists.[67]

Whatever opinion is right, to date, no big physical damage has been caused in any critical infrastructure and especially in any energy control system or grid as a result of a cyberterrorist.

However, Keith Lourdeau, deputy assistant director of the FBI's Cyber Division predicted that "terrorist groups will either develop or hire hackers, particularly for the purpose of complementing large physical attacks with cyber-attacks"[68].

2.5.3 Political and Geopolitical motives

In an era of great-power competition, in which states spend significant capital on developing military capabilities to deter or respond to armed attack, it is important to have strong cyber capabilities, both for resilience and for operational use.[69]

Cyberspace is an appealing forum for nation states to achieve their key objectives. Internet is the realization of the classic realism theory of international relations that the world is anarchic. This does not mean that all nation states are equal in terms of power, but there is not only one big sovereign player. Power is a matter of context, so there are nation states that have more capacity to exercise power in cyberspace than in any other traditional domain.[70]

---

[66] Irving Lachow (2011), Cyber terrorism: Menace or myth?
[67] M. J. Warren (2008), Terrorism and the Internet, Cyber Warfare And Cyber Terrorism, Information Science Reference, pp.42-49.
[68] D. Verton, CIA to publish cyberterror intelligence estimate, *ComputerWeekly.com*, 25.02. 2004. http://www.computerweekly.com/Articles/2004/02/25/200518/CIA-to-publishcyberterror-intelligence-estimate.htm
[69]Franklin D. Kramer and Robert J. Butler (2019), Cybersecurity: Changing the model, Atlantic Council.
[70]Joseph S. Nye Jr. (2010), Cyber power, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Nowadays, many states have the capability to conduct cyber-attacks. The fertile ground of cyberspace can host cyber-attacks as a strategic tool designed to provide political advantage and influence. The most famous states - cyber attackers are China, Russia, North Korea, Iran and Syria. One possible reason behind it is that these countries face fewer legal constraints in conducting cyber-attacks in relation to others. Each sector tends to worry about different countries as potential attackers. For instance, energy company executives worry most about Russia.[71]

The offensive activities of a state against other states in cyberspace could be considered as an act of war. As in the real world, uncertainty and mistrust are present in cyberspace too, so states develop offensive cyber weapons in order to prevent other states from overstepping the digital borders.[72] The nature of warfare has undergone important changes with the development of technology. Cyber warfare is a silent war with the use of computer systems, authorized mainly by state actors. What states cannot do with guns, are trying to achieve it by establishing their sovereignty in cyberspace. Their purpose is to destabilize adversarial regimes or institutions, prevent hostile actors, achieve operational advantage and gain diplomatic power. Many countries, in order to cover their footprints, "hire" cyber criminals to conduct cyber-attacks. They mostly use cyber espionage as a method to sabotage or damage a hostile state's reputation. However, outbursts of cyber-attacks are not regarded internationally as an act of war, but are treated by the state as a criminal phenomenon.[73] Both at UN level and at regional level, cyber-attacks are not perceived as 'armed attacks', while there are no multilateral transnational agreements on the subject.[74] As a result, beyond the political protests, there are no official retaliation records from the victim state. The absence to date of any "digital Pearl Harbor" or "cyber 9/11" catastrophes provides cold comfort.[75]

[71]Stewart Baker et al. (2009), In the crossfire: Critical Infrastructure in the Age of Cyber War, McAfee.
[72]A. Liaropoulos (2015), Cyber – Security: A Human - Centric Approach, Conference Paper DOI: 10.13140/RG.2.1.4855.8160
[73] Carr Jeffrey (2010), Inside Cyber Warfare, O'Rilley Media Inc., Sebastopol.
[74] Libicki Martin (2009), Cyber Deterrence and Cyber War, Rand Corporation, Santa Monica, CA.
[75] Jon R. Lindsay , Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 53–67, https://doi.org/10.1093/cybsec/tyv003

The energy industry has faced several attempts of sabotage for geopolitical reasons. By attacking its critical infrastructure, the whole state is weakened and destabilized. The two most devastating attacks known in the energy industry are Stuxnet in 2010 and BlackEnergy in 2015. After investigations, it was suggested that these attacks were state sponsored. The complexity of energy networks and the specificity and sophistication needed to disrupt these systems could only be bolstered by considerable finance and skillful teams of hackers.

Nevertheless, attackers who may be politically motivated, such as governments, seek to protect themselves from being disclosed. Most of the times, they disguise the state-sponsored attack as a form of hacktivism or a cyber criminal incident in order to avoid a government-to-government response. As a result, there is a difficulty in the identification of the origin of an attack due to the use of false flags. This is known as the attribution problem.[76] A positive aspect of the attribution problem is that states refrain from retaliating against the wrong actors. A risk that can be mistaken for a government sponsored action could possibly lead to a wider cyber war or a physical war. In any case, the suspicion that behind a destructive cyber attack lies a nation state, may lead to diplomatic tensions.

Experts support that there are a few states that have the means to conduct large-scale attacks, but the economic and diplomatic cost of sabotage is bigger than the benefit for the attacking state.[77] For major cyber-attacks is needed a lot of money, not for the operation itself, but for the establishment of defense walls.

An example that indicates that state-to-state cyber espionage is considered as a highly political motive is the recent case of State Grid. State Grid is the world's largest utility company and China's largest state-owned enterprise and made an offer to purchase shares in certain electricity networks and utility companies in Australia, Belgium and Germany. The authorities of the countries invoked "national security" justifications to prevent the purchase. The assessed reasons of this decision probably included the threat of cyber espionage as well as the risk to allow a third country to gain partial control over critical national infrastructure.[78]

[76] Simone Vernacchia (2018), A practical method of identifying cyberattacks, PWC Middle East.
[77] Supra note 3
[78] Supra note 22

As political motives are also characterized the initiatives of hacktivists, that have been analyzed above.

2.5.4 Geoeconomic motives

Most of the cyber-attacks that are politically motivated, also have an economic interest. Cyber is among the most powerful geoeconomic instruments. A cyber attack, to be considered geoeconomic, should meet two different criteria. First of all, the attack should be state sponsored and it should also involve an attempt of economic influence.[79] A geoeconomic attack in general aims to disrupt the control system of a company and to destabilize it by making use of financial market mechanisms (i.e. theft of commercial intellectual property) and imposing economic costs as a form of a wider geopolitical plan. In order for the attack to be economically destructive for a country and produce geopolitical benefit, it should target the critical infrastructure or major economic entities of a country. The states that suffer disruptive attacks in their national economy tend to become more receptive to external geopolitical manipulation.

Energy is once more among the most attractive targets. Geoeconomic cyber-attacks are manifested as cyber espionage, as retaliatory actions or as acts of intimidation.

In September 2012, Chinese hackers penetrated the control systems of Telvent, a firm that monitors oil and gas pipelines of North America. The fear that China was planning to disrupt energy supplies and cause black out in the power grid in case of a US- China crisis, made Telvent stop remote access to its client's systems. [80]

In 2013, American researchers uncovered systematic Russian hacking attacks in more than one thousand Western oil and gas computers and energy investment firms. The motive of these attacks was at least cyber espionage, since Russia has a big interest on oil and gas industry as a big player in it.[81]

[79] Robert D. Blackwill and Jennifer M. Harris (2016), War by other means: Geoeconomics and Statecraft, HARVARD UNIV PR.
[80] Nicole Perlroth, David Sanger, and Michael Schmidt, As Hacking against U.S. Rises, Experts Try to Pin Down Motive, The New York Times, 03.03. 2013, https://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?pagewanted=all&_r=0
[81] David E. Sanger and Nicole Perlroth, New Russian Boldness Revives a Cold War Tradition: Testing the Other Side, The New York Times, 30.10. 2014, https://www.nytimes.com/2014/10/31/world/europe/new-russian-boldness-revives-a-cold-war-tradition-testing-the-other-side-.html

2.6 Impacts of cyber-attacks in the energy sector

Cyber-attacks are a legitimate concern in the global energy community due to their various impacts.

First of all, cyber-attacks may cause market disruption. Decisions in the energy market are greatly affected by the energy wholesale markets, which are used to manage demand and supply and provide low cost opportunities. A disruption in energy organized market places could impact the energy security, while wrong or hacked data will not be reliant for the planning of the capacity required, as well as the commodity pricing. This is actually an impact on electricity markets that rely on short term planning. In oil and gas sector, a hacking of data on reserves could impact the derivatives and the future market.[82]

Network effects are also a crucial issue, since the breach in a control system could interrupt the continuity of the service and disrupt the system itself or cause information loss. Additionally, in the case of service disruption the credibility and the reputation of the company are ruined.

The reputation of a company can also be affected in case that the attackers gain unauthorized access to its systems, infringe intellectual property rights and release confidential confirmation. As a consequence, the company might face loss of customers, investors or even a collapse of its stock in the stock market.

Cyber-attacks in energy companies are possible to result in significant impacts on a state's economic prosperity, international competitiveness, public safety, social wellbeing and national security, as energy is a sector of national interest and belongs to a state's critical infrastructure.[83] Therefore, such an attack could paralyze whole sectors, such as transportation and health, decrease the state's international competitiveness and set the national defense in danger. Nevertheless, the most severe impacts of cyber-attacks in the energy sector are human harm, the physical damage of the infrastructure and the financial losses of the companies.

Cyber-attacks may cause human harm, for example in a case of attack on nuclear plant equipment that could end up in radioactivity leakage. For the time being, death and body injury because of a cyber attack are considered to be negligible as

[82] Supra note 2
[83] Australian Government, Cyber Security Strategy.

possibilities. In future, though, as more devices go online, cyber-attacks could pose a more material threat to human life.[84]

Cyber crossing over to physical is the biggest nightmare of businesses that are potential victims of cyber-attacks. The most exposed targets include offshore drilling rigs, power generation plants and pipelines directly connected to IT systems. A cyber attack in one of these systems could lead to fire or explosion and consequently, damage to property, environmental harm or loss of life. [85]

Referring to financial losses, it is included the cost to replace broken equipment and upgrade systems after the attack as well as regulatory fines, loss of intellectual capital and liability issues towards third parties affected by the disruption.[86] In 2015 the Lloyd's insurance market simulated the cost of a cyber attack in various electricity generators in the US. The result was that a blackout of the network in 15 states would cost to the country between $243 billion and $1 trillion in total.[87]

2.7 Most popular cyber-attacks in the energy sector

Stuxnet (2010)

Stuxnet marks the awakening of the international community that cyber tools can be used against critical infrastructures and thus provoked a wave of national cybersecurity strategies. The target of the attack was an Iranian nuclear plant and uranium enrichment site in Natanz. It has been the most advanced and sophisticated cyber attack so far, since the nuclear plant of Natanz did not have any connection to the Internet or other networks and as a result it was not exposed to external threats. Stuxnet was a specific worm, i.e. a piece of malware that probably passed in the industrial system via an infected USB drive. It focused on PLCs, manipulating the spinning frequency of rotors by speeding the centrifuges up and slowing them down repeatedly. This caused damage to the centrifuges and compromised the enrichment operation.[88] This program was the first one specifically designed to attack a particular facility and what is extraordinary in its function is that it could escape detection acting

[84]Marsh (2015), UK Cyber Security: the role of insurance in managing and mitigating the risk.
[85]Supra note 25
[86] ibid
[87] Lloyd's and University of Cambrige (2015), Business Blackout- the insurance implications of a cyber-attack on the US power grid.
[88] Marie Baezner and Patrice Robin (2017), Stuxnet," Risk and Resilience Team Center for Security Studies (CSS) Cyber Defense Project, ETH Zürich.

as a "ghost file". Its level of complexity and the major amounts of money invested prove that it should have been nothing but a state sponsored attack.

The relations between US, Israel and Iran are in constant tension during the last years. Iran's extremist political strategies and the plan to enrich its nuclear capacity in order to reinforce its national sovereignty have posed a major threat to its Middle East enemies, such as Israel, as well as to its international enemies, such as US.

Although the certain attribution of the attack is a difficult task, several investigations have concluded that it was supported by the American and Israeli governments. New York Times reporter, David Sanger, published an account of the covert program in which Stuxnet was created, in his chronicle of the Obama national security doctrine in June 2012. Sanger claimed that US organized a major cyber attack program against the nuclear facilities of Iran with the code name "Olympic Games". [89]

The information about "Olympic Games" was classified, but it is deduced that the prime target of Stuxnet was to postpone Iran's nuclear program in order diplomatic negotiations to be completed undistracted.[90] In fact, Stuxnet succeeded delaying Iran's uranium enrichment program and slightly alleviated the tensions between Israel and Iran that could escalate to another Middle East war and peak volatile oil prices.

Shamoon/ Disttrack (2012)

On August 15th, 2012, a malware called Shamoon hit an estimated 30,000 computers of Saudi Aramco, one of the largest oil producing companies of the world in Saudi Arabia. The virus erased data on three-quarters of Aramco's corporate PCs replacing it with an image of a burning American flag. Part of Shamoon's function was to delete data on computer hard drives, but its main intent seems to have been sabotage by wiping the operating system, in order to render the computers unusable. In fact, the malware knocked out part of the company's system for 2 weeks, but did not contain any functions designed to attack the ICS computers used in drilling or refining operations at Aramco.[91] As a result, the physical operations of the company remained unharmed. Saudi Aramco seems to have had adequate protection following the policy of segmentation between computer systems responsible for general

[89] D.E. Sanger (2012), Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, New York, Broadway Books.
[90] Supra note 8
[91]Christopher Bronk and Eneken Tikk – Ringas (2013), Hack or Attack? Shamoon and the evolution of cyber conflict, Rice University's Baker Instutute of Public Policy.

business operations and computer systems employed in monitoring and controlling upstream and downstream operations. So, Shamoon remained restricted to the company's management network and its spread was limited.

Were the attack more successful in destroying the company's operational system, it could lead to the disruption of oil production and supply from Saudi Arabia and to the rise of oil prices globally. As we see today, a corresponding event, the physical damage in the infrastructure of Saudi Aramco from drone attacks knocked out 5% of global supply and triggered a surge in oil prices.

An "anti- oppression hacker group" has taken responsibility for the attacks, including posting blocks of I.P. addresses of Aramco PCs online as proof.[92] True or not, the taking of responsibility of the attack by hacktivists shows that disruptive attacks are not necessarily state-sponsored. However, many experts believe Shamoon is a nation-state malware used in cyber-espionage campaigns. Speculation on Shamoon has mainly focused on the dispute between Iran and Saudi Arabia over Oil Embargo on Iran from the US and the European Union. Iran definitely had the motive to attack Aramco, because, in the face of trade sanctions imposed on July 1st, 2012, the Iranian oil remained unsold on tankers unable to find market, while Saudi Arabia was producing 10 million barrels of oil per day.[93]

A few weeks later Rasgas, a Qatari natural gas company, was also hit by the Shamoon virus and this attack brought the whole network offline.

As a closing remark, taking into consideration the ability of Aramco to supply 10% of the global demand for oil, this major computer hack alerted the world to the horrifying possibility of a cyber Pearl Harbor. [94]

BlackEnergy (2015)

On December 23rd, 2015 BlackEnergy malware attacked Kyivoblenergo, a regional electricity distribution company and caused power outage in Ivano-Frankivsk Oblast in Ukraine. This was the first publicly acknowledged power outage incident caused by a cyber attack and confirmed how vulnerable power grids are. The outages were originally thought to have disconnected of electricity approximately 80,000

[92] Daily Report: How Aramco Got Hacked, The New York Times, 24.10.2012 https://bits.blogs.nytimes.com/2012/10/24/daily-report-how-aramco-got-hacked/
[93] Supra note 91
[94] Paravantis, John (2019), History of Energy Security: A Geopolitical Perspective, Department of International and European Studies , University of Piraeus.

customers for three hours. Later, it became known that two other distribution companies had been attacked, so the total outage reached to 225,000 customers across the country.[95]

The attack exploited security lapses in IT and SCADA systems of the company as well as human negligence. A phishing campaign introduced the malware in the companies' industrial control systems in order to remotely control the distribution process. The attackers switched off about 30 electricity substations and managed to damage hard drives, preventing the functioning of operation systems. As a last part of the attack, the attackers deployed a TDoS (telephony denial of service) on the companies' call centers so that the customers could not inform the companies about the outage. If we would like to categorize this attack, it would definitely be an operation of sabotage. The Ukraine case demonstrates the vital need for the training of employees on cyber incidents, except for the enhancement of cybersecurity on the grid itself.

As far as it concerns the attribution of the attack, Ukrainian government officials point finger at Russia, although there is no proof provided.[96] The sophistication of the attack enhances the possibility that behind this multistage attack can be hidden a cooperation between cyber criminals and nation state actors. This scenario is a possible explanation, given the tension in the relation of the two states after the annexation of Crimea by Russia in 2014.

[95] Lee Robert, Michael Assante and Tim Conway (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems.
[96] Supra note 62

3 Building resilience to cyber threats

3.1 Illustrating the concept of cybersecurity

The growing number of cyber-attacks due to the inherent vulnerabilities of ICT systems demonstrates the need of cybersecurity in a global scale. There is no universally accepted definition of cybersecurity. There is, though, a wide range of terms that describe aspects of cybersecurity, such as Information security, ICT security, network security, internet security and critical information infrastructure protection.[97] Cybersecurity is also sometimes conflated with other notions such as privacy, information sharing, intelligence gathering, and surveillance.[98]

In the 'EU Cybersecurity Act' that was adopted in 17 April 2019, cybersecurity has been defined as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". However, cybersecurity is not only limited to the protection of information and network systems, but involves preventing, detecting, responding to and recovering from cyber incidents of any kind.[99] Such cyber incidents, as it is thoroughly analyzed above, may encompass from theft of data and disclosure of information to the commitment of cybercrimes, such as espionage, sabotage or acts of terrorism.

3.1.1 Cybersecurity notion in Energy

According to the International Energy Agency (IEA), energy security is the uninterrupted availability of energy resources at an affordable price. Cybersecurity is an integral part of energy security. A potential cyber threat against an energy system could affect all aspects of energy security that is the accessibility, affordability, availability and acceptability of the service.[100]

Cybersecurity in the energy sector aims to reinforce the reliability and the resilience of an energy system. In a few words, it aims to strengthen the ability of the system to

[97] Supra note 72
[98] Eric A. Fischer (2016), Cybersecurity Issues and Challenges: In Brief, Congressional Research Service.
[99] Supra note 48
[100] Uzunov Simon, Presentation, Smart Grids and Cybersecurity, 23rd Energy Community Electricity Forum Athens, 7 June 2018

resist disruptions and offer security of supply and even in case of attack to absorb the effects of disruptions and recover, minimizing their magnitude and duration.[101]

According to Dr. Klimburg, member of NATO in 2012, cybersecurity refers to the "[p]reservation of confidentiality, integrity, and availability of information in the Cyberspace".[102] This definition is also accebtable by ENISA, the European Cybersecurity Agency. [103] Confidentiality, Integrity and Availability (CIA) are three goals of high priority. The confidentiality criterion refers to the protection of privacy and proprietary data from disclosure by unauthorized actors. Integrity refers to the maintenance of the accuracy and the trust of data and requires protection from destruction. The final pillar, Availability, refers to the reliable and timely access and use of information.[104]

It is undisputable there is a need of cybersecurity response at all stages of the energy cycle. For the processes of generation and transmission, integrity and availability are the most protected goals, as altered or delayed data could harm the functioning of the industrial system. For the metering infrastructure, most important is confidentiality so that customers' personal data are being protected from theft or unlawful use. In nuclear, cybersecurity is part of the nuclear security.[105] Computer security, as it is otherwise called, prevents, among others, the cyber acts of theft, sabotage or malicious acts involving nuclear material.[106]

Most scholars address cybersecurity as a pure national security issue.[107] Cyberspace becomes a battlefield and cyber-attacks replace military attacks. States feel insecure in the anarchic formation of the web and thus develop offensive and defensive cyber weaponry. Each state, though, has its own perception on cybersecurity and sets different priorities depending on its national agendas and its dynamics in cyberspace.

---

[101] Michael Ingram and Maurice Martin (2017), Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities, National Renewable Energy Laboratory.
[102] Adams, S., Brokx, M., Dalla Corte, L., Galic, M., Kala, K., Koops, B. J., ... Skorvánek, I., "The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK," Tilburg University, 2015
[103] European Union Agency For Network And Information Security (2016), Report on Cyber Security Information Sharing in the Energy Sector.
[104] Z. Elmrabet et al. (2018), Cyber-Security in Smart Grid: Survey and Challenges, Computers and Electrical Engineering, Volume 67, Pages 469-482.
[105] Supra note 2
[106] International Atomic Energy Agency (2011), The International Legal Framework for Nuclear Security, GOV/2005/50
[107] Supra note 72

Of course full protection is impossible. Especially in the energy sector, digital components of energy systems are continuously acquiring new functions, so they may entail undetected weaknesses.

3.2 Cybersecurity governance

Resilience to cyber risks is an issue that demands a cross-industry, risk-based approach from companies and governments worldwide.[108] A cybersecurity framework in order to be successful shall aim at the development of a cybersecurity culture. Thus, it shall include national and international cooperative efforts to develop standards and processes that align policy comprising legislation, business, education and technology approaches to address cyber risks.[109]

'Cybersecurity governance' can be defined as the approaches used by multiple stakeholders to identify, frame and coordinate proactive and reactive responses to potential threats to the confidentiality, integrity, or availability of the computers, networks, and information that together constitute cyberspace.[110] Governance represents a system of governing methods where the borders of public and private sectors are unclear.[111] "There are three approaches that frame the debate on cyberspace governance: distributed governance, multilateral governance, and multi-stakeholderism."[112] The most discussed model is the multi-stakeholder process. Generally, in modern society, states do not have the monopoly of power, but share it with international organizations and non-state actors. Although the state remains the dominant actor, private companies can contribute to the fight against cyber threats by offering technical knowledge and management tactics. Some issues concerning cyber governance require technical solution and this is where technical knowledge is necessary. Nevertheless, even if private companies are monitoring enough and building robust systems, they still need guidance from the public sector. The policy planning and the implementation of laws against cyber attackers are up to the government. So, in the framework of cyber governance, governments are only one particular form of actors in cyber governance and regulation is only one particular

[108] Marsh (2014), Advanced cyber-attacks on global energy facilities.
[109] Teplinsky (2013), American University Business Law Review, 300.
[110] Supra note 98
[111] Andrew Liaropoulos (2014), Proceedings of the 13th European Conference on Cyber Warfare and Security, University of Piraeus.
[112] A. Liaropoulos (2016), Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics, Journal of Information Warfare, Volume 15, Issue 4, p. 9

feature that can help address cyber risks. Governance is not only about preventing or punishing, but also an effort of coordination with the long-term aim of a cybersecurity culture implementation.

3.2.1 Governments

A. Policies and legislation

-Preventive regulation-

Governments have recognized the magnitude of the threat of cyber-attacks and therefore have applied cybersecurity strategies in order to mitigate the possibility and the effect of these attacks on their critical infrastructure. Preventive regulation is more common in critical infrastructure sectors, because investment in this field makes more sense than spending money for a recovery after the attack. More than 30 countries such as Germany, Italy, France, the UK, the US, Japan, Australia, South Korea, India have taken a number of initiatives reinforcing cybersecurity.[113]

This thesis will focus on the policies and the legislation that the United States and the European Union have put into force respectively to protect the energy sector from cyber-attacks. On the one hand, US policy is strict and detailed and is implemented by institutions with the use of coercive measures. On the other hand, EU strategy is more flexible. In contrast to the US policy, is more exhaustive and gives more emphasis to electricity distribution, renewable resources and is more protective on personal data.[114]

United States

The economic and national security of the US depends on the seamless operation of its critical infrastructure. The American authorities have since years realized the importance of the energy sector. Indeed, the US electricity grid has been referred as the 'largest interconnected machine' in the world. [115]

The most prominent regulatory frameworks protecting the energy infrastructure in the US are the following.

In 2005, the US Congress ratified the *Energy Policy Act*, which gave the Federal Regulatory Commission (FERC) the authority to designate an Electric

[113] Supra note 25
[114] Supra note 8
[115] Supra note 32

Reliability Organization (ERO) and the power to approve the security standards proposed by this organization. This entity in the US is the private 'North American Electric Reliability Organization' (NERC) and proposes a series of cybersecurity norms of critical infrastructure protection (NERC CIPs) that are regularly updated in order to keep up with the evolution of cyber-attacks.[116] These are among the most detailed and comprehensive cybersecurity norms, mandatory for all electric utilities in the US.[117] In case of non compliance, the state has the authority to apply coercive measures, such as enforcement or penalties. Normally, all entities that interact and are parts of the electric grid should be under minimum cybersecurity standards. However, NERC CIP measures apply only to the electricity transmission system. Distribution facilities operate outside of FERC jurisdiction and a possible disruption could affect the whole grid. Moreover, NERC has established a system called 'NERC Alerts', that informs simultaneously all utilities in the US for imminent threats.[118]

In February 2013, President Obama signed the *Executive Order (EO) 13636*, titled "Improving Critical Infrastructure Cybersecurity" and two accompanied Presidential Policy Directives (PPD). This EO fosters the sharing of information between government and private actors and requires the U.S. Department of Homeland Security (DHS) to indicate which critical infrastructure could be potential target of cyber attack. Its most important aspect, though, is that it and grants the National Institute of Standards and Technology (NIST) the role of developing a cybersecurity framework "to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." The key of NIST proposal is a defense-in-depth strategy, applying industry standards and best practices of risk management to address cyber risks.[119] It provides a common language, so that the companies of the energy sector can assess how cyber resilient their systems are in a possible digital assault. This Framework is not one-size-fits-all approach, as cyber risks are evolving by the time. It is a living document that will be updated parallel to the industry

[116] Cyril W. Draffin, Jr. (2016), Cybersecurity White Paper, MIT Energy Initiative Utility of the Future.
[117] Supra note 7
[118] ibid
[119] Supra note 116

feedback.[120] The Cybersecurity Enhancement Act of 2014 (CEA) updated the role of the NIST formalizing its previous work under the EO 13636 and providing guidance for future changes.

The U.S. Department of Energy (DOE) may not be a regulatory body, but is designated as a federal energy agency to inform the President annually about the account of the participation of owners of vulnerable energy infrastructure in the NIST program. NIST Framework even if voluntary, has been adopted by most US companies and has affected the cybersecurity strategies that have been adopted worldwide.

President Trump, recognizing the strategic importance of critical infrastructure cybersecurity for his state, followed the path of his predecessor and signed in 2017 the *Executive Order 13800*, titled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure". This Order includes a review of all norms applied for the scope of cybersecurity and mandates the Secretary of Energy to identify the potential necessity of updates.

The Department of Energy has prepared a Cybersecurity Strategy for the years 2018-2020, a plan for an effective, collaborative enterprise-wide cybersecurity posture and defense.[121] This strategy incorporates four principles of success:

i. The "One Team, One Fight" principle, which underlines the need for DOE's leadership towards common policies and coordination,
ii. Employment of Risk Management Methodology, so that DOE analyzes and evaluates risks,
iii. Prioritized Planning and Resourcing, which focuses on resource allocation and prioritized requirements as an approach to cybersecurity. This principle is associated with the implementation of Executive Order 13800.
iv. Enterprise-wide Collaboration, which is based on the idea that cybersecurity relies on collaboration of stakeholders and customer engagement.

These principles are intended to be applied across four IT Strategy goals. Each of these goals is linked to particular cybersecurity objectives. The following analysis briefly outlines these goals and objectives. The first goal is the delivery of high-

[120] National Institute of Standards and Technology (2014), Framework for Improving Critical Infrastructure Cybersecurity.
[121] U.S. Department of Energy, Cybersecurity Strategy 2018-2020

quality IT and cybersecurity solutions through secure and reliable information access. The second objective is the improvement of cybersecurity posture through the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover). The third IT Goal, namely 'Transition from IT owner to IT broker for better customer focus' is linked to cybersecurity focused on customer's specialized needs. The fourth goal, namely 'Excel as stewards of taxpayer dollars' is linked to a risk based approach that is required in every part of the process for the success of cybersecurity strategy.

European Union

Cybersecurity and the protection of critical infrastructure were first set in the European agenda in 2004, when ENISA, a new specialized EU Agency was founded, approximately the same time as in the US. European Union's policies and legislation were not so targeted and detailed from the beginning. The European Commission adopted the Communication on the *European Program for Critical Infrastructure Protection (EPCIP)* in 2006 in order to provide an all-hazard, cross-sectoral approach to the protection of critical infrastructures.[122] This paper resulted in the European Program for Critical Infrastructure Protection in 2007 and in the *European Critical Infrastructure Directive* in 2008 (2008/114/EC), which establishes a process for identifying and designating European critical infrastructure for the energy and transport sectors. This legislative effort, though, entailed only general and precarious criteria for critical infrastructure cybersecurity.

In February 2013 was adopted the *EU Cybersecurity Strategy*, which entails a list of strategic priorities in the critical infrastructure field, including the energy sector. It mainly focuses on the need of a coordinated international cyberspace policy that aims to achieve cyber resilience. Yet, the document does not propose feasible measures rather than refers generally to desirable targets.

In 2015, the *European Agenda on Security* and the *Digital Single Market Communication* pinpoint the need for a common approach to address cyber threats across Europe. The first one mainly focuses on security against cybercrime and cyberterrorism, while the second one makes more general references on cybersecurity and emphasizes on the economic benefits of the creation of a Digital Internal Single Market.

[122] Supra note 2

By mid-2016, the European Commission initiated a *Contractual Public Private Partnership (cPPP)* on cybersecurity that intends to foster the cooperation between different actors, such as market players, researchers, national administrators with knowledge and innovative minds under the common purpose of enhancing cybersecurity in critical infrastructure sectors.

In August 2016 entered into force the *Directive 2016/1148 on Security of Network and Information Systems (NIS)*, the first horizontal legislation for the protection of network and information systems across the Union. NISD introduces the obligation for Member States to adopt a national NIS strategy and to designate national competent authorities to monitor its application as well as the obligation to create a Cooperation Group to support the exchange of information between Member States. In the articles that follow, the Directive establishes security requirements and incident notification for operators of essential services (OES) and digital service providers. It also requires that they take the appropriate technical and organizational measures to manage risks in NIS.[123]The energy sector falls within the scope of this Directive if we consider the reference in operators of essential services, since electricity, gas and oil supplies are essential services.

The NIS Directive may be a promising first step for the building of resilience and the protection of networks and information, but it is accused for not being precise and explicit enough, because the cybersecurity measures that should be implemented are very generally described.[124] Moreover, Directives are not directly applicable and need to be transposed into national law, so every Member State has the discretion to interpret their content in a different manner. As a result, the inconsistent transposition of EU legislation among Member States creates a problematic situation, since Member States with the least developed cybersecurity norms constitute weak links for all members of the European Union.[125]

At the same year, in April 2016, became applicable the *General Data Protection Regulation*, with the aim to protect the personal data of individuals and

[123] Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert, "The new EU cybersecurity frame-work: The NIS Directive, ENISA's role and the General Data Protection Regulation," Computer Law &Security Review: The International Journal of Technology Law and Practice, https://doi.org/10.1016/j.clsr.2019.06.007

[124] Supra note 116

[125] Supra note 8

ensure their free movement within the EU. Although the law making process of these two legal instruments took place in parallel, none of them acknowledges each other in their texts. GDPR includes that "*processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security constitutes a legitimate interest of the data controller concerned*", so it seems to take under consideration the cybersecurity issue, but regarding the aim of protecting personal data. In cases that network and information systems process personal data, both instruments find application and complement each other.[126]

On 13 September 2017, the former European Commission President Jean-Claude Juncker, in the State of the Union Address, made the following statement: "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. […] Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks." [127]Indeed, that day the European Commission proposed a range of concrete measures for the strengthening of EU's cybersecurity, a *Cybersecurity Package* in the Joint Communication to the European Parliament and the Council. The core of this package entered into force on 17 April 2019 with the Regulation 2019/881. The changes this Regulation brings are twofold: At first, it includes a permanent mandate for ENISA, the 'EU Cybersecurity Agency' so as to better support Member States, the EU institutions and businesses to tackle cyber threats. The new ENISA is empowered to contribute to cooperation and crisis management across the EU. Secondly, it creates a European cybersecurity framework for the certification of Information and Communication Technology products and services, which is of particular interest for the energy sector.

All these legislative papers may focus on cybersecurity for critical infrastructure sectors and operators of essential services, but they make no differentiation among them. Taking into account that energy is a sector of specific characteristics and requirements and that it is undergoing a major transition, the European Commission has issued several papers highlighting the growing need to protect the energy sector from digital assault.

[126] Supra note 124
[127] State of the Union 2017, Resilience, Deterrence and Defence: Building strong cybersecurity in Europe

One of them is the *Clean Energy for all Europeans Package* that was proposed in November 2016 by the Commission and consists of eight legislative acts. The Clean Energy Package was completed and adopted in May 2019 and is entails rules for that cover energy efficiency, energy security, renewable resources, the design of electricity market and governance rules for the Energy Union inspired by the Juncker Commission. It, though, acknowledges the importance of cybersecurity in the energy sector and stresses the need to assure risk preparedness and crisis management and to adopt preventive measures.

The *Regulation on gas security of supply* also includes provisions to consider cybersecurity as part of Member States' national risk assessments.

Quite recently, in April 2019, the European Commission adopted *Recommendation on cybersecurity in the energy sector* to raise awareness and provide guidance on how to tackle cybersecurity issues in the energy sector. Taking into account the specific characteristics of the energy sector, such as the real-time requirements of energy infrastructure components, the possible cascading effects of cyber-attacks and the vulnerable combination of legacy and state-of-art technology, the Commission identifies the main actions that should be taken in order to be built cyber resilience in energy systems across the EU. This is undoubtedly the most detailed guidance issued by the Commission in relation to the energy sector and up to the international standards.

The next steps the Commission is planning are the application of the Recommendation through Regulation (EU) 2017/1938 on Gas Security of Supply and the Regulation on Electricity Risk Preparedness, through the NIS Cooperation Group and through other outreach activities as well as the preparation of a "Network Code" according to the New Electricity Regulation in cooperation with ENTSO-E and ACER.[128]

B. Harmonization efforts

As it is obvious, the EU and the US consider the security of their critical infrastructure systems a prerogative. Cybersecurity is a domain that transatlantic cooperation could be achieved through the adoption of common measures and standards. However, such cooperation will not be viable, until the EU harmonizes the

[128] Rémi Mayet (2019), Cybersecurity in the energy sector, Directorate General for Energy Deputy Head Security of Supply European Commission.

cybersecurity frameworks of its Member States. Most of the legislative initiatives are introduced as Directives, which means that each State is absolutely responsible for their transposition into national legislation. In addition, most norms do not have a mandatory, but a voluntary character. For example, within the framework of the Cooperation Group, the evaluation of national strategies on the security of network and information is voluntary. Moreover, under the certification scheme in the Cybersecurity Act, the application of certification for ICT products and services is also voluntary.[129] This situation naturally leads to divergences in each State's approach to the measures that should be adopted, complexity of legislation and lack of coordination among Member States. As a last observation, there are states with more mature approach to cybersecurity that have already designed national authorities for this purpose and have been technically equipped to meet the certification needs and the safety standards imposed. Given the wide differences in terms of capacity and engagement[130] among Member States, the EU has to create an environment of fruitful cooperation and trust as well as to improve their capacities through funding programs.

The harmonization of standards is a crucial goal not only within the EU, but at the international level too. The U.S. and EU policies that have been analyzed may have started from different origins, but they aim to have the same effect: to encourage businesses to adopt rigorous risk management practices and share information on the changing risk profile, thereby increasing awareness.[131] Cybersecurity frameworks should be developed with a view to international adoption. Any cyber attack today, even in a remote country, could be harmful for an entire network because of the globalization of digital technologies. Therefore, transatlantic cooperation will be beneficial for both U.S.A and the EU. The American model can contribute to the improvement of the weaknesses of the European model and vice versa. Besides, governments should realize that overlapping or competing regulations will be a serious hurdle to the establishment of security standards and coordination is the most viable solution. Many companies have expressed their concerns about the different cybersecurity requirements worldwide. There is a need of alignment of cybersecurity

[129] International Conference Report (2011), Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Institute for Peace Research and Security Policy at the University of Hamburg.
[130] European Commission, Assessment of the EU 2013 Cybersecurity Strategy, SWD(2017) 295 final, 13 September 2017
[131] Supra note 108

standards in order duplication or conflicting expectations to be avoided.[132] A global agreement would definitely be difficult to achieve, but the Montreal Protocol on Substances that Deplete the Ozone Layer, the Chemical Weapons Convention and other examples prove that nothing is impossible.[133] Transatlantic cooperation could be supported by multilateral institutions, such as the United Nations or NATO. The United Nations have the necessary network that includes nation states, but also multinational and law enforcement organizations to facilitate the opening of discussions. Cybersecurity is an issue of concern for NATO too, so it has already developed a large-scale cybersecurity exercise with many nation states and has simulated cyber attack on electricity network in 2017.[134] These steps are crucial for the future of cybersecurity in general and for the future of the cybersecurity of the energy sector in particular.

C. International cooperation against cyber warfare & cybercrime

-Repressive regulation-

There is a lacuna in international law regarding the response to cyber-attacks. So far, only few attacks have triggered state responses.[135] This is a result of the jurisdictional fragmentation and the attribution problem. Jurisdiction is inherently linked to state sovereignty and represents the exclusive responsibility of the state over its people and within its territory. But who can claim jurisdiction in cyberspace incidents? Most cyber acts involve a transnational dimension and the interaction of multiple players. For cyber-attackers there are no boundaries and the use of digital means facilitates their activity. This situation implies multiple loci of liability and consequently problems with the enforcement jurisdiction. Given that, the law enforcement response must rely on trans-border mechanisms such as mutual legal assistance and extradition.[136] Nonetheless, these mechanisms cannot be directly applicable, since each state has different legal system and assesses differently which acts are criminally punishable. Only the interpretation of customary international law could lead to clarification of acceptable and non-acceptable behavior. Although most

[132]Evan Wolff et al. (2016), The global uptake of the NIST Cybersecurity Framework, Cyber Security Law & Practice.
[133] Supra note 116
[134] Supra note 8
[135] International Conference Report (2011), Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, Institute for Peace Research and Security Policy at the University of Hamburg.
[136] Alamie M. Weber (2003), The Council of Europe's Convention on Cybercrime, 18 Berkeley Technology Law Journal 425.

attacks take place in foreign states and multiple jurisdictions, there is no international regulation for international cooperation for the investigation of cyber issues and enforcement of cybersecurity mechanisms. This lack of coordination may stem from the fact that there are states that feel insecure and claim that their sovereignty is impaired by imposing foreign jurisdiction within their borders.

As far as it concerns the attribution problem, in the cyber realm it is not easy to distinguish who is hidden behind the attack. An individual is possible to act as an agent of a state or on his own, so the applicable law is different in each case. The Tallinn Manual, a comprehensive text on the international law applicable to cyber warfare, highlights this issue.[137] Identifying cyber attackers becomes more and more complex with the evolution of computer technology, which offers them anonymity and a safe haven to conduct attacks remotely. It is also common that many attackers use 'slave' computers to complicate the collection of evidence. States that have been targets of cyber-attacks in critical infrastructures should be certain for the nature and the origin of the attack in order to proceed with law enforcement. As attribution is not always possible, the exercise of Article 51 of the UN Charter, the right to self-defense, is not applicable, because the state should be identified as the attacker and the damage caused by a cyber-attack should equate to damage caused by an armed conflict or a criminal act.[138]

We shall admit that no state can achieve adequate cybersecurity without cooperation. Jurisdiction and attribution problems should be resolved and different approaches to privacy and sovereignty should be smoothened. Despite the challenges, common law enforcement measures are not only envisioned, but also applied more and more in an international scale. The Budapest Convention has set the goal to pursue a common criminal policy in order to foster international cooperation against cybercrime. Forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation.[139] Cooperation between law enforcement officers has been bolstered and relationships of trust have been developed between them. These efforts are extremely significant, because international coordination can contribute to the collection of data

[137] Schmitt (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, pages 29-37.
[138] Supra note 133
[139] Brenner (2012), Cybercrime and the Law: Challenges, Issues and Outcomes.

and evidence globally and the timely response that is needed especially with cybercriminals. In any case, the efforts have to be stepped up and the cooperation should be strengthened through a legal imprint on an international text.

However, preventive and repressive forms of regulation do not guarantee resilience.

3.2.2 Energy Industry

A. Technical solutions

The constant connectivity of network systems of an energy company to the Internet represents a constant threat for their cyber-hygiene. Technology sector can serve the energy sector in terms of cyber resilience. It is crucial that robust security safeguards are implemented in order risk mitigation to be achieved. For instance, a strong defense mechanism could comprise of a next-generation firewall, which filters out websites with malicious content and protects from viruses, as well as of a Wireless Intrusion Detection System (WIDS) and an encryption program.[140] The effective monitoring of the synergy of legacy and next generation systems in energy industries is crucial so that it is ensured that the amount of data that flow into smart grids is secured. Moreover, the diversification of software across multiple infrastructures could make the system more robust, limiting by this way the surface for the attacks. Blockchain technology also contributes to the securitization of network systems, but it does not guarantee an immune from cyber-attacks system. Consequently, technology alone is not a panacea in the changing digital world.

B. Risk management strategies

The energy sector has to increase its maturity level in cyber risk management issues. Indeed, the low maturity of the energy sector in cybersecurity is related to the perception that physical attacks had always been above any other threat. Energy companies should realize that cyber risks are permanent and persistent threats that should be managed in the same way as any other business risk. An energy executive reviewed for the report of World Energy Council 'The Road to Resilience: Managing cyber risks' stated that "Energy companies must get used to the fact that cyber is now same kind of risk to a large infrastructure as a flood or a fire".[141] In order to make a

[140] Investment Industry Regulator Organization of Canada (IIROC), "Cybersecurity Best Practices Guide"
[141] Supra note 25

system robust and resilient, companies should improve risk assessment and simulation operations.

The traditional response to a physical attack is to put barriers or build a high wall in order to avoid duplication. Nevertheless, this approach is impossible in cyberspace, while the operational model of energy firms depends on interconnected networks and data that are accessible to thousands of computers. Therefore, the challenge for the industrial sector is to deter cyber threats at the same time that systems are open to third parties.

The Framework of the NIST includes a set of functions that are helpful for stakeholders to manage cyber risks. These functions are Identify, Protect, Detect, Respond and Recover.[142] In a few words, businesses should identify their critical assets vulnerable to cyber threats, protect them enough to provide secure services, detect timely possible threats, respond to a detected incident with an appropriate cybersecurity plan and recover timely to their normal operation. These steps are not exhaustively detailed, but could create a common cybersecurity culture among companies.

Risk assessment

Risk management is the ongoing process of identifying, assessing, and responding to risk.[143] There is no standard approach to risk assessment. According to the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity, it is essential that businesses identify their most valuable critical assets and data and how their value will change as a result of digital transformation, assess the possibility that a cyber-attack will occur, evaluate its potential impacts and understand the need to be protected at all costs. Through this tactic, businesses can set a limit that will represent the acceptable risk. Once the key assets and data are identified and the risk tolerance limit is set, businesses should quantify the cost of a cyber risk in order to choose the most suitable cybersecurity framework. Undoubtedly, putting a monetary value on cyber threats is not an easy task. There have been developed two approaches to quantifying cyber risk:[144]

[142] Hogan Lovells (2016), Cyber security: A growing threat to the energy sector An Australian perspective.
[143] Supra note 120
[144]David X. Martin and Raj Bector (2014), A new approach to cybersecurity: Leveraging Traditional Risk Management Methods, Oliver Wyman.

i. The asset-based approach, which entails the value of the corporate assets and the potential reputational damage after a cyber-attack, estimating at the same time the probability of the cyber attack to become a reality and the discount rate of the value of the assets.

ii. The liability-based approach estimates the liability to a business in the case of materialization of a cyber threat based on past lost event data, so it may lead to inaccurate conclusions.

Educational Training and Awareness

Businesses need to establish policies to make their workforce aware of cyber risks. As we have observed in the examples of popular cyber-attacks that have been analyzed in Chapter 2, their common element is human error. Employees are the most vulnerable components of a system and attackers are aware of that. They become victims of a variety of scams. The most common human errors, either intentional or accidental, include mainly clicks on attachments on emails as a part of a wider phising campaign, the use of infected USB drives or the use of weak passwords. 35% of employees in sectors such as energy, chemicals etc. have been vulnerable to USB initiated attacks.[145] These errors may seem relatively small, but they are really severe for the operation of the company. Therefore, energy companies need to develop a cybersecurity culture among their employees through training sessions and simulations. Head managers of all departments are responsible for the education of the employees in order to ensure their risk awareness. Many companies have already spent a lot of money in awareness campaigns without encouraging results. It is believed that companies need to make one more decisive step and develop a cybersecurity engagement program, so that the employees will be not simply aware, but engage the problem and will also be well equipped to deter it.[146] Many energy companies run cyber event simulations in order to create the necessary cybersecurity culture, improve cyber risk management and bolster their cyber defense mechanisms.[147] Moreover, energy industry faces the problem of the loss of skilled employees due to retirement that need to be replaced with new workforce that lacks of

[145] Verizon (2015), Data Breach Investigations Report.
[146] Brian Honan (2014), Forget Security Awareness, We Need Security Engagement, Security Intelligence.
[147] Supra note 25

experience. Thus, companies organize often workshops and conferences to educate them as much as possible.[148]

Information Sharing

One of the most crucial missions of the energy industry is the timely and reliant security of supply. In order to make the appropriate decisions on investments and security programs, energy companies along with governments should also ensure timely, reliant and secure information exchange. Information sharing mechanisms are crucial for increasing reporting, public awareness, but also for the identification of cyber attackers and their motives through the use of statistics. So, besides legislation, information sharing between private and public stakeholders is another feature of cyber governance, which sometimes seems to be underpinned by some form of regulation, such as contracts or another form of agreement between parties.[149]

Many information sharing mechanisms exist between private and public sector within the critical infrastructure community.

In the United States, three are the key private sector information sharing institutions in the energy sector: the Electricity ISAC (E-ISAC), ONG ISAC, and Downstream Natural Gas ISAC (DNG- ISAC).[150] Information Sharing Analysis Centers (ISACs) are institutions that have been set up to foster collaboration, identification of cyber threats and protection. E-ISAC, which is specialized for the electricity sector, is the intermediary between DOE and electric utilities for the exchange of information.[151]

Specifically for cybersecurity, the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) as well as the DOE Office of Electricity Delivery and Energy Reliability (DOE-OE) have developed a partnership called Cybersecurity Risk Information Sharing Program (‘CRISP’). CRISP is a public-private data sharing and analysis platform that facilitates the timely bi-directional sharing of unclassified and classified threat information among energy

[148] Homeland Security (2015), Energy Sector-Specific Plan.
[149] Supra note 102
[150] Supra note 149
[151] Supra note 8

sector stakeholders.[152] The participation in the platform is voluntary. However, until 2018, a vast majority of U.S. electric utilities has participated in CRISP, representing the 75% of American consumers.[153]

In Europe, ISACs have also been developed, but not widely, as organizations that set up platforms for the quicker communication between energy infrastructure owners and operators and for the maintenance of cyber threat awareness. Their main aim is to facilitate the flow of information, experience and knowledge on cyber-attacks between public and private parties. The European Energy – Information Sharing Analysis Centre (EE-ISAC) was established in order public and private parties to effectively communicate and share security information beyond the borders of Member States and there are also three national ISACs especially for the energy sector in the Netherlands and the UK.

Computer Security and Incident Response Teams (CSIRTs), which provide educational and preventative services, may be widely developed in Europe, but only few of them focus in the energy sector.[154]

Finally, stakeholders in the energy sector have developed some information sharing initiatives, such as the Energy Expert Cybersecurity Platform (EECSP) and the Incident and Threat Information Sharing EU Centre (ITIS-EUC).

The main issues hindering information sharing are the lack of trust among the members of such an initiative and the possible legal constraints that exist in relation to the privacy of data. Indeed, public and private sector partners should build a trusted relationship. This means that the government should feel secure that the information provided by the private sector is reliable and in a real time scale. Firms on their side are cautious and reluctant to share sensitive information, because making their bad experience of a cyber-attack public could harm their reputation. So, the public sector should be able to ensure that information will be protected from inappropriate disclosure. Moreover, as far as it concerns the legal constraints, the adoption of GDPR

[152]CESER, U.S. Department of Energy (2018), Cybersecurity Risk Information Sharing Program (CRISP): Enhanced threat analysis with U.S. Intelligence insights for faster threat identification and mitigation.
[153]Privacy and Information Security Law Blog (2018), Department of Energy Announces New Efforts in Energy Sector Cybersecurity.
[154] European Union Agency For Network And Information Security (2016), Report on Cyber Security Information Sharing in the Energy Sector.

that distinguishes which information should be strictly confidential inside the bulk of data, is expected to contribute to the elimination of other legal obstacles.

C. Cyber Insurance

Insurance may not be a substitute of investing in cybersecurity or in risk management, since the deterrence of a digital assault would definitely be more preferable, but at least provides to the companies compensation for their financial exposure to the energy market. During the last years, governments are encouraging companies to apply for cyber insurance coverage and the demand in insurance packages has grown rapidly. Since 2012, energy companies with revenues of more than one billion dollars have increased their cyber insurance coverage worldwide by 98 percent, according to Marsh Global Analytics estimates.[155]

Except for the coverage, insurance also contributes to cyber risk management, because risk assessment is a prerequisite for providing insurance services. Indeed, insurance providers review the effectiveness of technical and organizational control and security mechanisms that are established in companies and their risk management strategies generally in order to assess cyber risks. The insurance industry underwrites cyber risk by reviewing the severity and frequency of cyber events.[156] It usually provides financial compensation to a company after an attack for the recovery of damages in the infrastructure, for the expenses to respond and last but not least for the interruption of the operation of the company that leads to a severe loss of earnings. However, especially in the energy sector, insurance policies traditionally exclude cyber-attacks from providing the financial means for the recovery of damages or other expenses. This could be devastating for the infrastructure and the human resources of an energy company. Additionally, the interruption of business represents a vital threat for the energy industry, because it constitutes financial loss of billions of dollars or euro. Thus, cyber insurance is more than mandatory and the energy industry should cooperate with the insurance industry to achieve a good outcome and cover a big uninsured risk that is growing big and fast, cyber-attacks. In general, coverage limits of cyber insurance are relatively low in relation to other perils. This is a result of the nature of a cybersecurity incident. The evolution and the sophistication that is observed in cyber-attacks impede the ability of companies to develop probabilistic

[155] Sandro Melis, Angelo Rosiello and Silvio Sperzani (2016), Cyber-Risk Management Will Hackers Cause The Next Energy Crisis?, Oliver Wyman.
[156] Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk.

pricing and exposure management models.[157] So, insurance companies are conservative in providing significant amounts of coverage in an unstable environment.

Therefore, some new forms of insurance have been activated, such as captive insurance. A captive is an insurance company owned by a non-insurance parenting company, which has as a primary scope to insure the risks of its owners. The use of captives is still limited in the energy sector, but the demand is growing.[158]

Terrorism is a peril that is never included in insurance coverage, so the same goes for cyber terrorism too and no indemnity is provided. Nevertheless, cyber terrorism is an emerging threat for energy companies and thus there is a demand for standalone cyber terrorism insurance.[159]

To conclude, cyber insurance in the energy sector is still in its infancy. Insurance companies on the one side should adopt a more open approach to underwriting cyber risks. Energy companies on the other side should include cyber risks in their common business risks and better assess them, in order to provide more reliable data to the insurers and improve their collaboration.

[157] OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en
[158] Supra note 25
[159] ibid

Recommendations and Conclusions

Energy operational and infrastructure systems are experiencing digital changes. The nature of these changes challenges and will challenge any efforts being made to the direction of cybersecurity. Cyber risks are becoming more and more sophisticated and frequent. Undoubtedly, the prevention of all cyber-attacks is impossible. No system is immune. No matter how tight the controls are, the constant evolution reveals new weaknesses. Especially the energy industry, which operates with critical national infrastructure necessary for the functioning of economies and societies, faces unique threats. The impacts of cyber-attacks could end up being devastating not only for an energy company, but also for a whole economy. It is, thus, an obligation for stakeholders to coordinate proactive and reactive responses to cyber threats. Regulatory initiatives may allow the digital revolution without compromising the safety of energy systems. Measures have already been taken in many countries in the form of national legislation and policy making. European states followed by the European Union, the U.S., Australia, Canada, Israel, Singapore are only some of these countries. Yet, individual mobilizations create complexity and cannot tackle the problem successfully. There is a need for harmonization of laws and for international cooperation under a game plan against cyber-attacks. Some crucial steps of this game are the following.

At first, states should reach a common definition on what is cybersecurity and of which elements it is comprised. Given the novelty of cyber-attacks, it is natural that there is little consensus regarding definitions. The development of a common language could be a starting point. The same could also take place for the notion of cyber-attack, which would definitely facilitate the attribution of an attack and the punishment of the offender.

As a second step, harmonization of national legislations with the international legislation would be essential for the solution of the jurisdictional problem. Overlapping norms would be avoided and transatlantic companies would have a common point of legal reference. In this perspective, nation states could sign bilateral

or multilateral agreements on cybersecurity cooperation and this attempt could also be fostered by multilateral institutions, such as NATO and the United Nations.

Another step could also be the creation of an information pool, where companies would share information about their experience of the attack and states would collect data and electronic evidence in order to identify the attackers are act timely. Such an initiative has already been molded through ISACs.

The energy industry, on its side, in order to effectively mitigate cyber risks, should create attack response plans and develop a comprehensive strategy to identify and improve the weak points of the system rather than limit their focus on preventing cyber-attacks. However, this requires the previous recognition that not all cyber risks are pure technological issues. This approach is based on the three Cs of response: collaboration, context and control.[160] A new concept in cybersecurity is the art of having the right people, in the right place, at the right time, aware and well educated. Education should not only be built on awareness campaigns and simulations of attacks, but people working in the energy industry should engage the problem.

What is more, the energy industry should correlate cyber risks to real life risks and evaluate the damage they can cause through the risk management process. Only by this way companies could set a limit for their acceptable amount of risk. Besides, understanding the impacts, companies could have a better picture of how, why and where cyber-attacks are likely to invade their business. In any case, insurance is the most viable choice to fill in the protection gap against cyber threats. It may still not be a widespread solution, because of the lack of historical data, but it is definitely a serious counterweight of the financial exposure of energy companies.

To conclude, it is obvious that the energy sector can amplify the global epidemic of cyber threats only through the cooperation of industry associations and governments. System operators, also, should have the capacity to operate a system and carefully assign the responsibility of data management and recover a system after an attack. Properly implemented cybersecurity tactic is possible to make hard the life of cyber-attackers and ensure safety in a higher level for the whole energy industry.

[160] Supra note 56

References

Adams, S., Brokx, M., Dalla Corte, L., Galic, M., Kala, K., Koops, B. J., …Skorvánek, I. (2015), The governance of cybersecurity: A comparative quick scan of approaches in Canada, Estonia, Germany, the Netherlands and the UK, Tilburg University.

Andoni, M. et al. (2019), Blockchain technology in the energy sector: A systematic review of challenges and opportunities, Renewable and Sustainable Energy Reviews 100, 143-174.

Australian Government, Cyber Security Strategy.

Baezner, M. and Robin, P. (2017), Stuxnet, Risk and Resilience Team Center for Security Studies (CSS) Cyber Defense Project, ETH Zürich.

Baker, S. et al. (2009), In the crossfire: Critical Infrastructure in the Age of Cyber War, McAfee.

Barichella, A. (2018), Cybersecurity in the energy sector: A comparative analysis between Europe and the United States, ifri center for energy.

Blackwill, R.D. and Harris, M.J. (2016) War by other means: Geoeconomics and Statecraft, HARVARD UNIV PR

Brenner (2012), Cybercrime and the Law: Challenges, Issues and Outcomes

Bronk, C. and Tikk– Ringas, E. (2013), Hack or Attack? Shamoon and the evolution of cyber conflict, Rice University's Baker Instutute of Public Policy.

Campbell, Richard J. (2018), Electric grid cybersecurity , Congressional Research Service.

Carr, J. (2010), Inside Cyber Warfare, O' Rilley Media Inc., Sebastopol

CESER, U.S. Department of Energy (2018), Cybersecurity Risk Information Sharing Program (CRISP): Enhanced threat analysis with U.S. Intelligence insights for faster threat identification and mitigation.

Committee on National Security Systems CNSSI No. 4009 April 6, 2015.

Cyber Security Conference, San Francisco, CA March 01, 2012.

Daily Report: How Aramco Got Hacked, *The New York Times*, 24.10.2012 https://bits.blogs.nytimes.com/2012/10/24/daily-report-how-aramco-got-hacked/

David E. Sanger and Nicole Perlroth, New Russian Boldness Revives a Cold War Tradition: Testing the Other Side, *The New York Times*, 30.10. 2014 https://www.nytimes.com/2014/10/31/world/europe/new-russian-boldness-revives-a-cold-war-tradition-testing-the-other-side-.html

Deloitte Center for Energy Solutions (2017), Protecting the connected barrels: Cybersecurity for upstream oil and gas.

Denning, D. E. (1999), Information Warfare and Security, ACM Press, New York

Desarnaud, G. (2017), Cyber attacks and energy infrastructures, ifri center for energy.

Dogrul, M. et al. (2011), Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism," 3rd International Conference on Cyber Conflict, Tallinn, Estonia.

Draffin Jr., C. V. (2016), Cybersecurity White Paper, MIT Energy Initiative Utility of the Future.

Elmrabet, Z. et al. (2018), Cyber-Security in Smart Grid: Survey and Challenges, Computers and Electrical Engineering, Volume 67, Pages 469-482.

Energy Expert Cyber Security Platform Report (2017), Cyber Security in the Energy Sector.

European Commission, Assessment of the EU 2013 Cybersecurity Strategy, SWD(2017) 295 final, 13 September 2017

European Court Of Auditors (2019), Briefing paper Challenges to effective EU cybersecurity policy.

European Cyber Security Organisation (2018), ECSO Energy sector report.

European Union Agency For Network And Information Security (ENISA 2016), Report on Cyber Security Information Sharing in the Energy Sector.

Europol (2017), Internet Organised Crime Threat Assessment.

Fischer. E.A. (2016), Cybersecurity Issues and Challenges: In Brief, Congressional Research Service.

Fleury T., Khurana H., Welch V. (2008) Towards A Taxonomy Of Attacks Against Energy Control Systems In: Papa M., Shenoi S. (eds) Critical Infrastructure Protection II. ICCIP 2008. The International Federation for Information Processing, vol 290. Springer, Boston, MA.

F-Secure white paper (2019) The state of the station: A report on attackers in the energy industry.

Gutierrez Astilleros, P. et al. (2018), Cybersecurity Guidelines and Best Practices for Emergency Services, European Emergency Number Association (EENA) Document.

Hackers Attack Servers of Oil Companies Working in Arctic, *The Moscow Times*, 16.07.2018, https://www.themoscowtimes.com/2012/07/16/hackers-attack-servers-of-oil-companies-working-in-arctic-a16275

Hogan Lovells (2016), Cyber security: A growing threat to the energy sector An Australian perspective.

Homeland Security (2015), Energy Sector-Specific Plan

Honan, B. (2014), Forget Security Awareness, We Need Security Engagement, Security Intelligence.

Ingram, M. and Martin, M. (2017), Guide to Cybersecurity, Resilience, and Reliability for Small and Under-Resourced Utilities, National Renewable Energy Laboratory.

International Atomic Energy Agency (2011), "The International Legal Framework for Nuclear Security, GOV/2005/50

International Conference Report (2011), Challenges in Cybersecurity: Risks, Strategies, and Confidence-Building, , Institute for Peace Research and Security Policy at the University of Hamburg.

International Energy Agency (2017), Digitization & Energy.

International Renewable Energy Agency (2019), A New World: The Geopolitics of the Energy Transformation.

Internet Organised Crime Threat Assessment (2018), EUROPOL.

Investment Industry Regulator Organization of Canada (IIROC), Cybersecurity Best Practices Guide.

JavaTpoint, Types of Cyber Attackers, https://www.javatpoint.com/types-of-cyber-attackers

José de Arimatéia Da Cruz, Terrorism, War and Cyber (In)Security, *Small Wars Journal*, 27.10.2013, https://smallwarsjournal.com/jrnl/art/terrorism-war-and-cyber-insecurity

Kahle, Karen E. et al. (2017), Cybersecurity and the Energy Sector: Practical Considerations, Powerpoint Presentation.

Koufopoulou, I.A. (2019), "The Evolution of Cyber Terrorism and a possible electronic Pearl Harbor; The case of Stuxnet, Department of International and European Studies, University of Piraeus

Kramer F.D. and Butler R.J. (2019), Cybersecurity: Changing the model," Atlantic Council.

Lachow, I. (2011), Cyber terrorism: Menace or myth?

Liaropoulos, A. (2014), Proceedings of the 13th European Conference on Cyber Warfare and Security, University of Piraeus.

Liaropoulos, A. (2015), Cyber – Security: A Human - Centric Approach, Conference Paper DOI: 10.13140/RG.2.1.4855.8160

Liaropoulos, A. (2016), Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics, Journal of Information Warfare, Volume 15, Issue 4, p. 9

Libicki, M. (2009), Cyber Deterrence and Cyber War, Rand Corporation, Santa Monica, CA

Lindsay, J.R. , Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack, Journal of Cybersecurity, Volume 1, Issue 1, September 2015, Pages 53–67, https://doi.org/10.1093/cybsec/tyv003

Lloyd's and University of Cambrige (2015), Business Blackout- the insurance implications of a cyber-attack on the US power grid.

Lötjönen, J. (2018), Cyber Security in robotics, energy and health, JYVSECTEC/JAMK.

Marinos, L. and Lourenço, M. (2019), ENISA Threat Landscape Report 2018.

Markopoulou, D., Papakonstantinou, V. and Paul de Hert, The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, Computer Law &Security Review: *The International Journal of Technology Law and Practice*. 31.09.2019 https://doi.org/10.1016/j.clsr.2019.06.007

Marsh (2014), Advanced cyber-attacks on global energy facilities.

Marsh (2015), Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers

Marsh (2015), UK Cyber Security: the role of insurance in managing and mitigating the risk.

Marsh, UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk

Martin, D.X. and Bector, R. (2015), A new approach to cybersecurity: Leveraging Traditional Risk Management Methods, Oliver Wyman

Maurer. T. and Morgus, R. (2014), Compilation of Existing Cybersecurity and Information Security Related Definitions.

Mayet, R. (2019), Cybersecurity in the energy sector, Directorate General for Energy Deputy Head Security of Supply European Commission.

McAfee (2014), Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic and International Studies.

McCurry, South Korean nuclear operator hacked amid cyber-attack fears, *The Guardian*, 23.12.2014, https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack

Melis, S., Rosiello, A. and Sperzani, S. (2016), Cyber-Risk Management Will Hackers Cause The Next Energy Crisis?, Oliver Wyman.

Monti, A. et al. (2018), Digitalization of the energy system and customer participation: Description and recommendations of Technologies, Use Cases and Cybersecurity, ETIP SNET.

National Institute of Standards and Technology (2014), Framework for Improving Critical Infrastructure Cybersecurity.

NATO Glossary of Terms and Definitions, Edition 2014.

Nye Jr, Joseph S. (2010), Cyber power, Belfer Center for Science and International Affairs, Harvard Kennedy School.

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en

Paravantis, J. (2019), History of Energy Security: A Geopolitical Perspective, Department of International and European Studies , University of Piraeus

Perlroth, N., Sanger, D. and Schmidt M., As Hacking against U.S. Rises, Experts Try to Pin Down Motive, *The New York Times*, 03.03. 2013, https://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?pagewanted=all&_r=0

Pradeep Kumar Kukreja, SRM Karnawat (2012), ONGC, Cloud Computing – Next generation tools for Oil and Gas Companies?, 9th biennial international conference & exposition on petroleum geophysics.

Privacy and Information Security Law Blog (2018), Department of Energy Announces New Efforts in Energy Sector Cybersecurity.

Robert, L., Assante, M. and Conway, T. (2016), Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center & SANS Industrial Control Systems.

Robinson, N. et al. (2013), Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts, Directorate General for internal policies policy department A: economic and scientific policy industry, research and energy.

Sanger, D.E. (2012), Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, New York, Broadway Books.

Schmitt (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, 29-37

Smith, Don C (2018), Enhancing cybersecurity in the energy sector: a critical priority, Journal of Energy & Natural Resources Law, 36:4, 373-380, DOI: 10.1080/02646811.2018.1516362.

State of the Union 2017, Resilience, Deterrence and Defence: Building strong cybersecurity in Europe.

Teplinsky (2013), American University Business Law Review, 300

U.S. Department of Energy, Cybersecurity Strategy 2018-2020

Uzunov, S., Presentation, Smart Grids and Cybersecurity, 23rd Energy Community Electricity Forum Athens, 7 June 2018

Verizon, Data Breach Investigations Report.

Vernacchia, S. (2018), A practical method of identifying cyberattacks, PWC Middle East.

Verton, D., CIA to publish cyberterror intelligence estimate, *ComputerWeekly.com*, 25.02.2004 https://www.computerweekly.com/news/2240054743/CIA-to-publish-cyberterror-intelligence-estimate?amp=1

Vijayapriya, T. et al. (2011), Smart Grid: An Overview, Smart Grid and Renewable Energy, 2, 305-311.

Warren, M.J. (2008), "Terrorism and the Internet," Cyber Warfare And Cyber Terrorism, Information Science Reference, pp. 42-49.

Weber, A.M. (2014), "The Council of Europe's Convention on Cybercrime," 18 Berkeley Technology Law Journal.

Wolff, E. et al. (2016), The global uptake of the NIST Cybersecurity Framework, Cyber Security Law & Practice.

World Energy Council (2016), World Energy Perspective – The road to resilience: managing cyber risks.

Wueest, C. (2014), Targeted Attacks Against the Energy Sector, Symantec Corporation.