ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Energy and Environmental Policy Laboratory

Cyber Security in the Energy Sector: Threat landscape and Policy frameworks

Dominika Helena Giantas

Working Paper 13

January 2019

The contents of this paper are the author's sole responsibility. They do not necessarily represent the views of the Energy and Environmental Policy Laboratory of the University of Piraeus, of any of the Laboratory's members, and/or of the author's other affiliations.

ISBN

xxxx

Introduction

The energy sector is one of the most crucial national infrastructure sectors, correlated to the energy security, but also to the resilience, functioning and the development of the modern state and economy. Due to this fact, the energy ecosystem has become an attractive target and vulnerable sector to several threats and challenges. The latest trend, which introduces new technologies, digitalization and intercorrelation in many aspects of our lives, adds a new dimension to the national energy security, the cyber one. The purpose of this paper is to examine if there is cyber threat in the energy sector in in the digital era and if so, what are some policy recommendations, which could help states worldwide to fortify the energy sector.

First of all, we will try to explore the reasons that make the energy sector vulnerable to cyber risks. Then, we will scrutinize the basic elements of the cyber threat landscape of the energy sector by determining the main cyber threats to the energy systems and infrastructure and then, focusing on the types of the cyber-attacks on the energy sector. Lastly, we will determine how countries should protect the energy sector from cyber threats, by highlighting some strategies introduced worldwide and making policy recommendations for better cyber security in the energy sector, referring to the top level of its management.

Table of Contents

1. Is the energy sector in danger of cyber threat?

1.1 The energy security in cyber era

The energy sector, as it is delineated, comprises all energy extraction, conversion, storage, transmission, and distribution processes with the exception of those that use final energy to provide energy services in the end-use sectors (industry, transport, and building, as well as agriculture and forestry). [1] In other words, energy sector includes all the industries and companies, forming an inter-related and complex network, are involved in the components of the energy supply chain.

Crucial role in the energy sector plays the energy infrastructure. It refers to the fundamental facilities and systems which serve the production, transportation, storage and distribution of energy. The quality, resilience, reliability, efficiency and sustainability both of the energy sector and the infrastructure constitute the backbone for the energy security and policy of modern states and economy.

In the light of the digital era, the energy sector and infrastructure have been pioneers by adopting digital solutions, introducing new technologies and becoming more and more interconnected.

For example, electricity markets are now being monitored and controlled in real time over vast geographical areas serving large numbers of customers. Moreover, oil and gas companies have long used digital technologies to model exploration and production assets, including reservoirs and pipelines, while the industrial sector has used process controls and automation for decades, in order to maximize quality and yields and to minimize energy use. Intelligent transport systems are using digital technologies in all modes of transport to improve safety and efficiency. [2]

From one hand, digital solutions have improved energy efficiency and the reliability of energy supply and propelled the use of smart energy systems and renewable energy sources. This leads to significant cost saving for energy sector. For example, in the electricity sector, it is estimated that the deployment of storage, alongside smart solutions such as demand management and the construction of interconnectors which allow the UK to import and export more electricity from the continent, could to savings of £8 billion a year by 2030.[3]

Moreover, digitalization proves to be the key to optimize the electrical,

[1] (Intergovernmental Panel on Climate Change, 2015) pg. 518

[2] (International Energy Agency, Digitilization & Energy, 2017)

[3] (National Infrastructure Commission, n.d)

gas and oil systems and eventually ensure safety, security of supply and offer more affordable energy services.[4] He stresses that due to digitalization "previous centralized business models structured according to assets and raw materials on the basis of relatively few fixed partnerships has shifted to a decentralized, service-oriented business model with complex crossi-ndustry value creation networks, where the customer has top priority".[5] Thus, digitalization, technological advancement and the increasing implementation of artificial intelligence are also changing markets, businesses and employment. New business models are emerging, while some century-old models may be on their way out.[6]

The digitalization promotes innovative business models that enhance the system's flexibility and incentivise deployment of renewable technologies such as virtual power plants, innovative forms of power purchase agreements and platform business models such as peer-to-peer trading. [7] Moreover, according to IRENA, the shift to renewables combined with digitalization, would result in the loss of 7.4 million jobs in fossil fuels by 2050, but at the same time 19.0 million new jobs would be created in renewable energy, energy efficiency, and grid enhancement and energy flexibility, and thus a net gain of 11.6 million jobs.[8] Bloomberg NEF (BNEF) estimates that annual revenue from digitalization of energy could be $54 billion for the present, while by 2025 it will increase to even $64 billion. [9]

On the other hand, unprecedented challenges and threats arise in the energy sector due to its relentless cyberization. The energy infrastructure and industries become more and more cyber-dependent. They are becoming digital, smart and connected to electronic data, controlled and operated digitally. This increases the vulnerabilities and potential access points for cyber-attacks, data exfiltration, privacy risks or damages to infrastructure.

The digitalization overall, brings a new dimension to the traditional perception of the energy security. The IEA defines energy security as "the uninterrupted availability of energy sources at an affordable price. It has a long-term aspect, which relates to timely investments to supply energy in line with economic developments and environmental needs". Energy security, in the short term, focuses on the ability of the energy system to react promptly to sudden changes in the supply-demand balance. [10]

Today, the energy security needs to include a cyber security dimension. Cyber security is defined as "technologies and processes constructed to protect

[4] (European Commission, Cybesecurity in the energy sector, 2018)

[5] (KPMG International , 2016)

[6] (International Energy Agency, Digitilization & Energy, 2017)

[7] (International Renewable Energy Agency , 2018)

[8] (International Renewable Energy Agency , 2018)

[9] (Bloomberg NEF, 2017)

[10] (International Energy Agency, Energy security, n.d)

computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorist groups and hackers".[11] Not only physical threats but also the cyber-attacks from non-state actors are from now on, a threatening tool to the stable supply of energy sources and the energy security of states.

The risk of cyber threats is changing the way energy policymakers, enterprises and stakeholders view the energy security, the energy infrastructure and supply chain management.[12] A new type of actor occurred as a threat to the energy security and new means of threatening action are added to the definition of energy security. This means that the sources, infrastructure and utilities directly or indirectly involved in energy production and distribution of energy products require enhanced protection in order to secure stable energy supply.

According to the IEA, the core principals of digital energy security should be resilience, cyber hygiene and security by design.

A. Resilience

Potential delays or disruptions in the energy systems and the disturbance of distribution of the commodity can have a longstanding impact on the proper functioning and the development of societies and economies. Due to this fact, it is vital for the energy infrastructure to have the ability to withstand or recover quickly from shocks and threats that originate from the cyberspace and relate to the ongoing process of digitalization of the energy systems. This is called cyber resilience which refers to "the ability to continuously deliver the intended outcome despite adverse cyber events"[13]. The International Energy Agency underlines that although cyber-attacks causing disruptions to the energy sector have been minor, in a short time the attacks will become more common as the digitization and interconnectivity move forward. [14]

B. Cyber hygiene

[11] (Goutam, 2017)

[12] _(World Energy Council, New cyber resilience report : energy sector prime target for cyber-attacks, 2018)

[13] _(Björck, Henkel, Stirna, & Zdravkovic, 2015)

[14] (International Energy Agency, Digitilization & Energy , 2017)

The term refers to a basic set of precautions and monitoring that all ICT users should undertake.[15] In other words, it includes practices and steps that should be followed in order to enhance the cyber security of IT systems. Cyber hygiene keeps devices and data safe, organized and well-protected from cyber-attacks.

Most common cyber hygiene practices include awareness, secure configuration of equipment and networks, keeping software up to date, avoiding giving staff and users unnecessary system privileges or data access rights, and training. [16]

Cyber hygiene is believed to be beneficial mainly for two reasons. Firstly, it secures maintenance of computers and software, so that they can perform at the highest level and be more resistant to cyber security risks. [17] Secondly, cyber hygiene incorporates security and enables the prevention of cyber-attacks.[18]

The energy sector, as more cyber oriented it becomes, the more in need of sound cyber hygiene it will be, in order to secure proper, reliable and sustainable functionality of energy systems, and ward off threats, inherent to the digitalization process.

C. Security by design

The International Energy Agency notices the need for the incorporation of security objectives and standards in the energy sector as a core part of the technology research and design process. [19] Due to growing cyber vulnerability of energy enterprises, infrastructure and systems, it becomes necessary to implement a cyber security architecture, in the energy sector, as an integral part of the Security by Design and a form of protection specifically from cyber threats. By being prepared and having the right systems and technology, the energy sector can prevent attacks, respond quickly to the occurred threats, recover and continue its operations sooner and with less cost.

Full prediction and prevention of cyber-attacks is not feasible. But with the right policy framework, the energy industry can successfully limit the cost, the length and the impact of cyber events on markets, economy and society.

All in all, there is a critical linkage between cyber reality and the domain of energy issues. The energy sector has become one of the most susceptible industries to cyber-attacks. It comes from the fact that digital solutions are

[15] (International Energy Agency, Digitilization & Energy, 2017)

[16] (International Energy Agency, Digitilization and Energy, 2017)

[17] (Brook, 2018)

[18] (Brook, 2018)

[19] (International Energy Agency, Digitilization and Energy, 2017)

welcomed in the energy industry, since they bring many economic benefits, such as efficiency in the supply management and rationalization of the energy consumption. But with the digitalization, the energy sector is also within the scope of cyber-attacks, such as data breaches of DoS attacks. As a result, the issue of energy security cannot ignore the cyber dimension, especially because, as Barrichella mentions, the threat of cyber-attacks is growing. [20]

1.2 Why energy sector is in danger?

Cyber-threats are becoming an ordinary challenge and struggle for the energy sector. It is the new reality, which governments, companies and industries, directly or indirectly associated to the energy production, distribution or/and consumption, face daily. The emergence of cyber threats and actors in the energy sector has surely been sparked by some factors.

First of all, the energy sector is a highly attractive target of cyber malicious activities. Energy commodities and their safe, feasible and cheap extraction, production, processing and distribution to customers plays a vital role in the economic growth, social development and national security. As the survey of World Energy Council, published in 2013 mentions, energy is the main "fuel" [21] which fires every activity.

Energy is directly linked to wellbeing, prosperity. It supports economic growth, social progress, is fundamental for a better quality of life and high standards of living. Barnes, Chalabi, Steeg and Yokobori point out that indeed the availability of abundant and cheap sources of energy have contributed to improvement of living standards, healthcare, technological advancement and prolonged life expectancy.[22]

Indeed, from the simplest human need to the task of national security, energy flows through all of these necessities. For example, heating our homes, lighting, air conditioning, cooking, electrical appliances and water heating are all functions that require energy.

Moreover, among the consumers of energy are also profit-seeking and nonprofit enterprises engaged in commercial-scale activity, such as retail stores, office buildings, government buildings, restaurants, hotels, schools, hospitals, and leisure and recreational facilities.[23] Energy consumption by the commercial sector also includes energy consumption for street and other outdoor lighting, and for water and sewage treatment.[24] Therefore, the main enterprises and institutions of a country need energy for their proper and continuous functioning and providing the users with goods or services on a daily basis.

What is more, energy has great importance for the industrial sector of

[20] (Barichella Arnault, 2018)

[21] (World Energy Council, World Energy Resources, 2013 Survey , 2013)

[22] (Barnes, 2000)

[23] (Government Publications Office, 2016)

[24] (U.S. Energy Information Administration, 218)

each country. Specifically, energy resources such as gas, petroleum and propane constitute the fundament for the development of many industries, including manufacturing, construction, mining, farming, fishing, and forestry. Furthermore, energy is fundamental for the transportation sector. Specifically, road, rail, sea and air transport depend on energy products.[25] Generally, energy is required to meet the basic human needs and is an input for most productive processes in primary sectors, industry and services.

Last but not least, energy sources are fundamental for the national security and defense, since they fuel military forces of each state. In fact, Nuttall, Samaras & Bazilian have examined the interaction which occurs between military issues and defense planning, and the energy issues. They also mention that developments in the energy sector have serious implications for military tactics and strategy. Energy empowers capable operational major vehicles, weapons systems and communications infrastructure at the desired levels of performance, range and readiness when a threat to the national security occurs. [26] All in all, the need to deliver adequate and timely energy supplies to military forces is throughout the course of the history a prerequisite for the success of military campaigns.[27]

In brief, given the importance of energy resources and infrastructure for the stability, development, well-being and high living standards of each country, it becomes clear that this sector has an increasing appeal to cyber threats and constitutes a target of high value. Any interruption, even brief, of the energy supply is highly consequential on several sectors and human activities. For example, interruption of electricity supply can cause major financial losses and create havoc in cities and urban centres.[28]

What is more, energy insecurity and shortages handicap productive activities and undermine consumer welfare.[29] Energy products are absolutely essential for modern lifestyle and proper functioning of states, for human well-being and sustainable development. Therefore, issues such as adequate energy supplies, continuous availability of energy sources, quality of supply are of high importance. Energy insecurity, blackouts and shortages handicap productive activities and so undermine consumer welfare. They also cause inconveniences and difficulties for individuals, enterprises and entities. They could be threatening to the functionality of hospitals and healthcare facilities, industry sector etc.

Taking into consideration the vital role of energy industry in almost every aspect of human activity, it becomes clear that energy sector is a highly attractive target for malicious cyber actors. Specifically, by selecting energy infrastructure or networks as target of a cyber-attack, cyber actors can cause a damage with high social, financial and political impact. They also hit the core,

[25]_(Bergasse , 2013)

[26] (Nuttall, Samaras , & Bazilian , 2017)

[27] (Nuttall, Samaras , & Bazilian , 2017)

[28] (Barnes, 2000)

[29] (Barnes, 2000)

the fundament of economic growth, prosperity, development and security at a national level. Eventually, they do not just manage to fulfill their designated goals (e.g. financial gain, political and ideological motivation), but they do it in the most consequential possible way, with the widespread havoc and insecurity.

Another factor, which sparked the interest of cyber threats for attacks on the energy sector is the growing digitalization and convergence of energy sector and cyberspace. The energy sector evolves into a sphere, which cyber actors and threat have finally access to.

Specifically, the energy industry in no exception to adopting new technologies, innovations and embracing the digital transformation. For example, oil and gas industries could introduce miniatured sensors, fibre optic sensors and smart grids and cables in the production systems. Though this way, they might boost production or increase the overall recovery of oil and gas from a reservoir. [30] Moreover, digital technologies in the coal supply chain such as automated systems, sensors, and robotic or remote mining can improve productivity, enhance workers' safety or/and lower costs. [31] The investments in digital technologies by energy companies have intensified over the last years. According to International Energy Organisation, global investment in digital electricity infrastructure and software in 2017 has grown by over 20% annually since 2014 [32] But, according to a report of International Energy Agency, the greatest opportunity which derives from the digitalization is the ability to overcome boundaries between energy sector and thus, increase flexibility and integration of energy systems. [33]

The energy sector evolves into more interconnected, influenced by the telecommunications and Internet and cyber-dependent. This unfolds a spectrum of benefits and possibilities to explore. On the other hand, energy systems are being progressively exposed to damage originated in the cyberspace. Henceforward, the more technologically driven the energy sector becomes, the more sources of vulnerabilities to cyber-attacks may occur. The targets of possible cyber-attacks may multiply, and the cyber tradecraft can become more sophisticated and effective. Indeed, cyber-attacks are becoming easier and cheaper to organize, whereas digitalized equipment and the growth of the Internet of Things (IoT) are increasing the potential "cyber-attack surface" in energy systems.[34] All in all, malicious cyber actors exploit the deepening linkage between energy sector and digitalization.

Last but not least, the emergence of cyber-attacks in the energy sector could be interpreted as a new possibility of warfare and offense that states and

[30] (International Energy Agency, Digitilization and Energy, 2017)
[31] (International Energy Agency, Digitilization and Energy, 2017)
[32] (International Energy Agency, Digitilization and Energy, 2017)
[33] (International Energy Agency, Digitilization and Energy, 2017)
[34] (International Energy Agency, Digitilization and Energy, 2017)

non-state actors seek. The cyberspace is a global domain, available for anyone who has access to computer and Internet connection. Sigholm further explains [35] that this inevitably means the existence and activity of different actors, with specific needs, goals and motivations each one.

The cyber threats could be seen as a new weapon of choice both for state and non-state actors. The nature of warfare has shifted from physical to online.[36] At the same time information technology and the internet have become a major element of national power. [37] Screier delineates that many states use cyber capabilities, create offensive cyberwar capabilities and develop national strategies, and sometimes they sponsor cyber-attacks and network infiltrations. [38] Given into account the vital role of the energy sector in the state security and prosperity, the exploitation of cyber techniques by states, to damage, sabotage adversaries or gain advantageous position in the terms of geopolitical antagonism, is possible. Cyber-dependent energy sector is used as a theater of state conflict. For instance, some state could sponsor and direct hacking groups to cause disruption of energy services and damage to the energy infrastructure, cables, grids, or control systems of an adversary. In consequence, this puts the stability, economic prosperity, security and well-functioning of the victim-state into real danger.

On the other hand, some cyberattacks on the energy sector are not state sponsored and used instrumentally in the conduct of cyberwarfare. These attempts are driven by other motivations and intentions, compared to the motives of nation-states. Specifically, political ends, ideology, financial gains, desire for revenge or embarrassment, information theft, or public attention and terror can be named as some possible motives for non-state cyber actors. Undoubtedly, digital technologies and the expansion of cyber space to the energy sector have stimulated an increasing role for non-state actors in the international system.

All in all, the topic of cyber energy security is a rising in importance motion and is gaining a serious attention of the policy makers, governments, businesses and academic community worldwide. The vital role of energy in the prosperity, security and economic growth of a state has been clarified and conceptualized by governments long ago. Reliable, uninterrupted, safe and stable and at an affordable price provision of energy sources is one of the main objectives of many states' political agenda. Yet, in today's highly interconnected and digitalized world, the energy security is put in danger, as states and non-

[35] (Sigholm, 2016) pg 9
[36] _(O'Flaherty, 2018)
[37] _(Schreier, 2017)
[38] _(Schreier, 2017)

state actors explore and exploit the new possibilities, which cyber space offers, in order to achieve their defined goals.

1.3 Cyber threats and types of cyber-attacks

1.3.1 Cyber threats

As concluded above, the energy sector is in increasing danger of malicious cyber activity and attacks. At the same time, the cyber threat landscape is dramatically changing. Today's cyber threats are not only persistent, well organized, constantly evolving— and often successful, but also many disguise themselves within the information technology (IT) ecosystem in a manner that is all but impossible to distinguish from legitimate activity. [39] The threats have multiplied and become more sophisticated and so, dangerous to the security of the industrial control systems and networks such as power grids, chemical plants, aviation systems, transportation networks, telecommunication systems or financial systems.

One of the most prominent actors and exploits are hacktivists. Hacktivists are often described as "persons—acting alone or in a group—who seek unauthorized access to computer files or networks in order to further social or political ends."[40] The can also be defined as "politically motivated hackers" but differ from other types of hackers since they are motivated by the pursuit of social change and do not seek profit or intellectual pursuit. [41]

Scott and Spaniel (2016) convey that hacktivists vary in their technical sophistication and they characteristically operate according to political and ideological motivations.[42] What is more, these actors are motivated by ideology in an effort to maximize disruption and embarrassment to their specifically targeted victims and to right the real or imagined social wrongs. [43] With keeping in mind the driving force of their actions, they may conduct distributed denial of service (DDoS) attacks, deface a company's website, or steal and expose private information in an attempt to embarrass the company and gain attention for a cause.[44] So, once a hacktivist has attacked and damaged his opponent, he seeks for public attention, media coverage and recognition.

The energy sector has been greatly targeted by hacktivists. They may

[39]_(PwC, 2013)
[40]_(PwC, 2013)
[41]_(Mikhaylova, 2014)
[42]_(Scott & Spaniel , 2016)
[43] (Bryk , 2016)
[44] (FireEye, 2016)

opportunistically target energy companies in response to perceived controversies [45] and often are invested in some conspiracy theory or environmental cause. [46] The biggest threats to the energy field posed by cyber activists are believed to be stealing "intellectual property" such as a proprietary way to drill a well and cyber-attacks which would disrupt a factory's manufacturing process, causing damage in the real world. [47]

Anonymous, a hacktivist collective launched a cyber-attacks campaign on the energy sector in 2013 as a form of protest against the West's domination of the world's resources and the adoption of US dollars as currency for oil exchange.[48] Paganini claims that the attacks could include distributed Denial-of-Service attacks, theft of sensitive information, defacement of websites and social media platforms or sabotage of the energy systems with malware. [49]

Anonymous was also responsible for a series of attacks on top multinational oil companies to express dissatisfaction with the drilling in the Arctic. According to PwC annual security survey, hacktivists were the second most likely source of security incidents in the energy sector, constituting the 32% of the incidents. [50]

In 2012, a group called "Cutting Sword Justice" launched a persistent cyber-attack on one of the world's largest oil producers, Saudi Aramco. A computer worm was activated on the computer network of the company, replicated itself across more than 35,000 computers and deleted a great amount of data on the hard drives. [51] At the same time, the worm spread into the computers of other energy companies such as ExxonMobil and GasRas. [52]. The group claimed responsibility for the attack, stating "we penetrated a system of Aramco company by using the hacked systems in several countries and then sended [sic] a malicious virus to destroy thirty thousand computers networked in this company"[53]. The group expressed an opposition to the Saudi Aramco's support of the Al Saud royal family's authoritarian regime. "This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression" [54] highlighted the group in a statement. As a consequence of the attack, Saudi Aramco was forced to switch to 1970s

[45]_(FireEye, 2016)

[46]_(Scott & Spaniel , 2016)

[47] (Israel's Homeland Security, n.d)

[48] (Paganini , 2013)

[49] (Paganini , 2013)

[50]_(PwC, 2013)

[51]_(Bronk , 2016)

[52]_(Bronk , 2016)

[53]_(Bronk , 2016)

[54]_(Middleton , 2017)

technology using typewriters and faxes in order to manage the needs od supplies, shipping and contracts with government and business partners[55]

Cyber criminals form another serious threat to the energy sector. Cybercriminals attack systems to generate a profit through the exploitation or auction of victim data[56] Cyber criminals may seek to obtain personal and financial data for fraudulent purposes.[57] According to PwC, opportunistic criminals focus on stealing customer information, identities, payment data, and other sensitive information, which can be quickly converted for financial gain.[58]

The cyber-dependent crimes include techniques and methods such hacking or keylogging to exploit vulnerabilities in computer systems and steal personal data, detailed online searching for personal information and social engineering techniques which enable frauds and phishing emails. [59]

Scott and Spaniel (2016) reveal that in the energy sector, attacks by cyber criminals target at gaining access to customer data or insider knowledge which could impact the investments in the field, or exfiltration and selling confidential information. What is more, they highlight the fact that mercenary cybercriminals may conduct attacks-for-hire against energy organizations on behalf of an unsophisticated nation state, or even terrorist entity.[60] Last but not least, Pwc states that such groups can pilfer funds via unauthorized wire transfers, other "cash-outs," and sensitive corporate secrets.[61] According to Scott and Spaniel (2016) groups such as Desert Falcons or Patchwork APT/Chinastrats which have multiple times attacked energy companies, are associated in the category of cyber criminals.

Desert Falcons is a group of cybermercenaries operating from the Middle East and using a set of methods to hide and operate malware. The cybercriminals are thought to be highly skilled, using sophisticated methods of attacks. The interesting about the group is the range and variety of victims; Kaspersy Lab points out the clear political, geographical and social distinctions between them.[62] Desert Falcons have targeted mainly military and governments of many countries but also energy providers, oil and natural gas organizations, and smart grid operators. [63] It is estimated that the group has comprised around 5000 systems in countries such as Israel, Egypt, Iraq, Kuwait, USA, UAE, Qatar, China, Germany, Canada, Turkey, France and South Korea. [64]

[55] (Pagliery , 2015)
[56]_(Scott & Spaniel , 2016)
[57]_(McGuire & Dowling , 2013)
[58]_(PwC, 2013)
[59]_(McGuire & Dowling , 2013)
[60]_(Scott & Spaniel , 2016)
[61]_(PwC, 2013)
[62]_(Kaspersy Lab , 2015)
[63] (Scott & Spaniel , 2016)
[64]_(Scott & Spaniel , 2016)

The criminals make use of a wide range of tools and techniques. For example, they use social engineering methods, exploiting the victims' trust in social networking forums and the curiosity about news relating to political conflict in their country, spear phishing e-mails, targeted attacks through Facebook chat, cyber espionage, infection with malware, or spyware. [65]

Another prominent group characterized as cybercriminal is Patchwork APT or Chinastrats. As explained by Scott and Spaniel (2016), Patchwork began its activity in 2014 and in 2015, when discovered, infected at least 2,500 victims. [66] The groups targets are mainly government-associated organizations, but also several industries such as aviation and the energy sector. [67] According to Symantec telemetry, targeted organizations are located in dispersed regions. Although approximately half of the attacks focus on the US, other targeted regions include China, Japan, Southeast Asia, and the United Kingdom.[68]

It is essential to note that the group does not make use of sophisticated tools and technologically advanced methods in order to launch successful cyber campaigns. The criminals use Chinese-themed content as bait to compromise its targets' networks[69], copy-pasted codes from malware and malware kits such as Powersploit, Meterpreter, Autolt, and UACME, codes from GitHub and hacking forums and do not develop their own malware or toolset.[70] This, as Scott and Spaniel clarify, signifies that cyber criminalists do not necessarily need to be sophisticated or technological pioneers to be successful. [71]

A common cyber threat that should not be neglected comes from the inside of the energy industry. Many employees- current or former-, contractors, consultants, and other trusted partners have authorized access to information and system management, and so the likelihood to exploit this access to inflict harm, such as industrial espionage, sabotage, or unauthorized disclosure of information. [72]

Some insiders act intentionally, with the knowledge of their actions and the awareness of the consequences. They can also be blackmailed, influenced by other threat actors or just be careless and infect systems with malware unintentionally, by just responding to phishing emails or visiting watering hole sites and so enabling an attacker into systems and networks. Some malicious insiders are trustful and easily manipulated by real attackers and others are just charmed by financial gains or seek revenge. Consequently, malicious insiders do

[65]_(Kaspersy Lab , 2015)
[66]_(Scott & Spaniel , 2016)
[67]_(Hamada, 2016)
[68]_(Hamada, 2016)
[69]_(Hamada, 2016)
[70]_(Scott & Spaniel , 2016)
[71]_(Scott & Spaniel , 2016)
[72]_(PwC, 2013)

not always seek to harm the organization. Often, they are motivated by self-interest.[73] PwC reports that current employees comprise the most cited likely source of security incidents (40%) [74]. Malicious insiders are believed to often be disgruntled, desperate, or disenfranchised employees or contractors and constitute a nuisance or a serious threat for several entities. [75]

Whatever is their motivation, they constitute a weakness of the sector, a means to breach or bypass the defense measures of the industry. It's a cyber-risk, inherent to human nature, and an unsolved issue in cyber security of every industry, including the energy sector.

Insider threats pose one of the greatest threats to the Energy sector because they can be easily manipulated or directed to bypass security applications, infect energy systems and networks with malware, disable physical controls, or physically alter systems. [76]As a result, they have the potential to cause serious energy disruptions, to cause panic and high economic and social cost. Additionally, cyber terrorists are becoming a real and a serious threat to the energy cyber security. The evolution of technology is partly responsible for the emergence of this treat, since it entails availability of new and often cheaper, faster and easier methods, tools and capabilities of attacks and a wider range of targets, not only in physical world but also in cyber space.

Pollitt (1998, cited in Conway, 2014 cited in Chen, Jarvis & Macdonald, 2014) uses the term "cyber-terrorism" to denominate "the premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non- combatant targets by sub-national groups or clandestine agents." Denning defines cyber-terrorism as a highly damaging computer-based attacks or threats of attack by non-state actors against information systems. Non-state actors launch attacks to intimidate or coerce governments or societies in order to achieve political and social goals. Denning emphasizes that "cyber-terrorism is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act" (Denning, 2006). She notes that cyber-terrorists, instead of turning against individuals or physical property, cause destruction and disruption in cyberspace.

The energy sector is a highly attractive target for cyber terrorists. This comes from the fact that among all the infrastructures, energy networks and systems appear to be the most critical and fundamental for the economic growth and prosperity of societies. In fact, all the industries and human activities rely heavily on the continuous and uninterrupted flow of energy

[73] (Bailey, Kolo, Rajagopalan, & Ware , 2018)

[74]_(PwC, 2013)

[75]_(Scott & Spaniel , 2016)

[76]_(Scott & Spaniel , 2016)

supply.

Terrorist organizations face more and more limited barriers to exert cyber terrorism on the energy sector. For example, groups such as ISIS possess the economic resources and basic knowledge to outsource layers of an attack to mercenary hackers or to hire a sophisticated adversary to develop an easy to use malware on in energy systems. [77]

Furthermore, Scott and Spaniel (2016) indicate that these groups can potentially use malware-as-a-service, ransomware-as-a-service, or SCADA-access-as-a-service to compromise energy systems. Moreover, they can collect confidential and sensitive information. The authors specify that cyber terrorists could steal and use facility information in order to exploit the physical vulnerabilities and loop holes and to conduct a terrorist attack on infrastructure or facility. They could also take advantage of population density information and launch an attack at the prime time, causing more chaos and panic to societies and governments. Lastly, stolen customer information could direct them to funds, needed for their terrorist activities. The potential for surprise in the cyber realm from cyber terrorists may increase in coming years, as energy sector becomes more digitalized and interconnected and depends progressively on digital devices but also as malign actors such as terrorist organizations become more emboldened, sophisticated and better equipped in the use of rapidly evolving cyber capabilities.

Last but not least, cyber practices are believed to be used by nation states as they are exploring new possibilities of warfare in the terms of their geopolitical antagonism. Specifically, an individual or group of individuals are sponsored by nation states and act on behalf of governments in order to launch cyberwarfare campaigns against critical infrastructure — manufacturing plants, power stations, aviation systems, transportation networks, water systems and energy companies and foreign governments. Moreover, they seek information, perform reconnaissance, launch cyber-espionage campaigns, focus on intelligence gathering, or disrupt of services.[78]

The major powers considered as sponsors of cyber-attacks are the United States, Russia and China.[79] They are the most advanced and prolific in terms of cyber capabilities and technology. According to Institute for Critical Infrastructure Technology, the so called Advanced Persistent Threat (APT) groups, as the cyber workforces of nation states, deploy the most sophisticated attack and malware obfuscation techniques, expend significant resources to discover and exploit previously undiscovered vulnerabilities (zero-day exploits)

[77] (Scott & Spaniel , 2016)

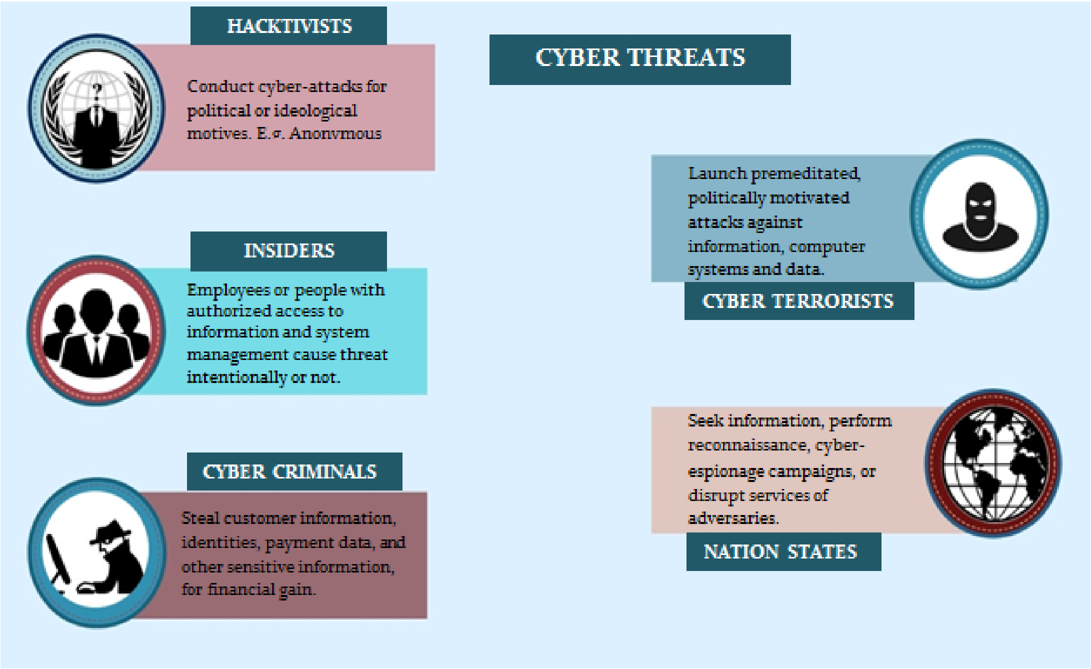
[78] (Garner Jr. , 2017)

[79] (Scott & Spaniel , 2016)

in target systems.[80] Undoubtedly, APT groups are savvy, innovative, sophisticated, continuously engineering new cyber weaponry and creating advanced malware, often customized to their target. For this reason, they can conduct the most successful offensive and defensive cyber-operations on behalf of their sponsors. The state sponsored cyber activities are becoming not only more professional, advanced and effective, but also, they are an accepted and preferred means of warfare. Markedly, cyber capabilities are becoming complimentary to the traditional methods of nation state conflict, a part of strategic planning in the terms of geopolitical antagonism of nation states.

Significantly, they could provide a state with a competitive advantage, fortified power and economic and technological lead in the global arena. As the competition in the energy sector is reinforced, the geopolitical tensions remain high and the cyber space marks a growing worldwide expansion, nation-state sponsored cyber threats may not abate.

The Figure 1.1 depicts the main actors linked to cyber-attacks in the energy sector. Over the past years now, the threats have multiplied and gained high levels of expertise and sophistication. Each of these cyber actors has different motives and philosophy behind the cyber-attacks.



Conduct cyber-attacks for political or ideological motives. E.g. Anonymous

Employees or people with authorized access to information and system management cause threat intentionally or not.

Steal customer information, identities, payment data, and other sensitive information, for financial gain.

Launch premeditated, politically motivated attacks against information, computer systems and data.

Seek information, perform reconnaissance, cyber-espionage campaigns, or disrupt services of adversaries.

Figure 1.1 Cyber threats

[80] _(Scott & Spaniel , 2016)

1.3.1 Types of cyber-attacks

Firstly, cyber actors can use several tools in order to commit a successful cyber-attack on the energy sector. Their cyber capabilities are constantly improving, they gain more experience, sophistication and knowledge. Moreover, they are expanding their weaponry, by creating and using new types of malware or ransomware. The unstoppable process of digitalization brings new opportunities for the cyber actors to explore new, more effective, cheaper and impactful on the targets means of cyber-attack.

One of the main tools in the cyber arsenal is malware. Malware is software specifically designed to disrupt, damage, or gain unauthorized access to an information and communications technology (ICT) system.[81] It constitutes harmful forms of software such as viruses, worms, trojan horses, logic or time bombs.

Malware is usually installed for example by clicking a link to download a file, or by opening an attachment which appears to be harmless, but actually has a malware installer hidden within. [82] Once malware is in a computer, it enables the attacker to have access and steal sensitive information, alter or delete data and files, take control of the device, monitor the user's actions or send emails on his/hers behalf.

Ransomware can also be used as a cyber weapon. Ransomware is "a type of malware that attempts to extort money from a computing device, user or corporation by infecting and taking control of the victim's computer, or the file & documents stored within."[83] The analysis of Institute for Critical Infrastructure Technology's report observes that locking down critical infrastructure such as the energy networks with ransomware does not depend on expertise and knowledge of unique applications or system configurations. The only prerequisite is enough momentary access to the system to install the malware.[84] Ultimately, ransomware installs and governs itself and makes the target negligent or complacent. [85]

The first reported case of an energy utility being victim of ransomware attack was The Board of Water and Light in April of 2016. Its information system was paralyzed was he duration of a week. Speciffically, the company's network was infected by ransomware via a phishing email, which then spread throughout the company's entire network and started encrypting files in all computers on the internal network.[86]

[81] (International Energy Agency, Digitilization & Energy, 2017)

[82]_(Rapid 7 , n.d)

[83] (Loota , n.d)

[84] (Scott & Spaniel , 2016)

[85] (Scott & Spaniel , 2016)

[86] (Sentryo , 2016)

BWL acted immediately by locking down all the corporate systems and closing email servers, accounting services and power and water services. Through this way, the ransomware did not spread into operational or industrial control systems, no customer information was compromised and no utility functionality was lost during the incident. [87]

According to Sentryo, a company focusing on providing cyber security for industrial Internet, ransomware constitutes a modus operandi inevitably on the rise. [88]This proliferation comes from the fact that ransomware attacks have proven effective, causing trouble, disturbances and unprecedented risks to companies in the energy sector.

Moreover, spear phishing or whaling is a common method of cyber-attack used by many cyber actors. Phishing/whaling is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion. [89] According to Boeck from Lockton Companies, phishing refers to sending an email that purports to be a legitimate message from a well-known sender, but in fact, it is sent from a criminal, who tries to obtain confidential and sensitive information, such as usernames and passwords or to insert malware into the victim's computer system.[90]

The types of phishing attack include spear phishing, clone phishing, whaling and smishing as the most consequential threats on the energy sector. Generally, phishing attacks on the energy industry are mostly motivated by the opportunity to create harm and cause damages rather than to achieve financial gains. [91] In the specific sector of energy, cyber threats use this method in order to gain access to computer networks, power grids, generators, operating systems, or other physical or virtual infrastructure.

The energy sector of Ukraine has been reportedly, and multiple times targeted by phishing campaigns. During 2015, three Ukrainian energy providers lost power for several hours, leading to serious power outages. Specifically, these incidents affected more than 225,000 customers in three different distribution-level service territories of Ukraine and impacted the reliability of the companies' systems and business operations. [92]

Besides thus, Jeffers from the InfoSec Institute underlines that phishing attacks are often perceived as in linkage with terrorism. That is because such attacks allow terrorists to cause panic, havoc and to spread terror inside

[87] (Sentryo , 2016)

[88] (Sentryo , 2016)

[89]_(Shi & Saleem , n.d)

[90] (Boeck , 2015)

[91]_(INFOSEC Institute , n.d)

[92] (Lee, Assante , & Conway , 2016) pg vi

governments and societies. [93] All in all, phishing attacks depend on exploiting human weaknesses, careless or gullibility, in order to gain access to well protected targets, obtain sensitive information, or gain strong foothold in systems and networks for potential attacks in the future.

Furthermore, botnets are being increasingly used by cyber actors. Botnets or robot networks are automated programs that run over the internet.[94] They constitute a collection of "bots" or robots, which create an army of infected "zombie" computers. [95] Some botnets run automatically, while others are controller by the originator and execute commands. In other words, a botnet is a collection of networks or devices which have been infected with a type of malicious software. Once compromised by malware, botnets can be commanded from anywhere in the world and be spread through various countries and be used for illicit purposes. [96]

According to BitSight study of 2015, the utilities industry is struggling, since more than 52% of the companies in this sector experiencing a botnet grade of B or lower. This means that these companies are more likely to experience a data breach than the healthcare, retail or finance sector. Utility systems are often exposed and infected to botnet malware such as TDSS, Carufax, ZeroAccess, Sality, and Banload. [97]

Denial of Service attack, as Kazerooni indicates, is one of the top new risks threatening the energy sector. [98] He further explains that although the DDos have existed since the occurrence of the Internet, they experience a significant revival and boosting due to technological advancements. [99] Distributed Denial of Service is a method of shutting down a host computer system by utilizing multiple computers to flood that host with more traffic than that host can manage resulting in the host's systems resources being depleted and shutting the host down.[100]

During a DoS attack, a hacker floods a computer with more traffic than the host was built to handle and overloads the server with data. This results in loss of functionality of the network and availability for the users. What is more, it potentially means that internal network operations could slow down or halt, payment transactions may no longer be processed, industrial control systems such as SCADA could be disrupted, and the network architecture might be damaged. [101] DoS can in short time and easily impact the functioning of energy

[93] (INFOSEC Institute , n.d)

[94] (International Energy Agency, Digitilization & Energy, 2017)

[95] (Government of Canada, 2017)

[96] (Gassen , Tiirmaa-Klaar , Gerhards-Padilla, & Martini , 2013)

[97] (Kazerooni, 2015)

[98] (Kazerooni, 2015)

[99] (Kazerooni, 2015)

[100] (Garner Jr. , 2017)

[101] (Kazerooni, 2015)

utilities and the delivery of vital commodities

The types of cyber-attacks, showed in the Figure 1.2 , constitute serious and real threats to the energy sector and so, the energy and the national security of states. A successful attack can cause major suffering to large populations, significant power outages, economic damage and consequences on other industries, which depend on the energy distribution such as health services, food production and transport.

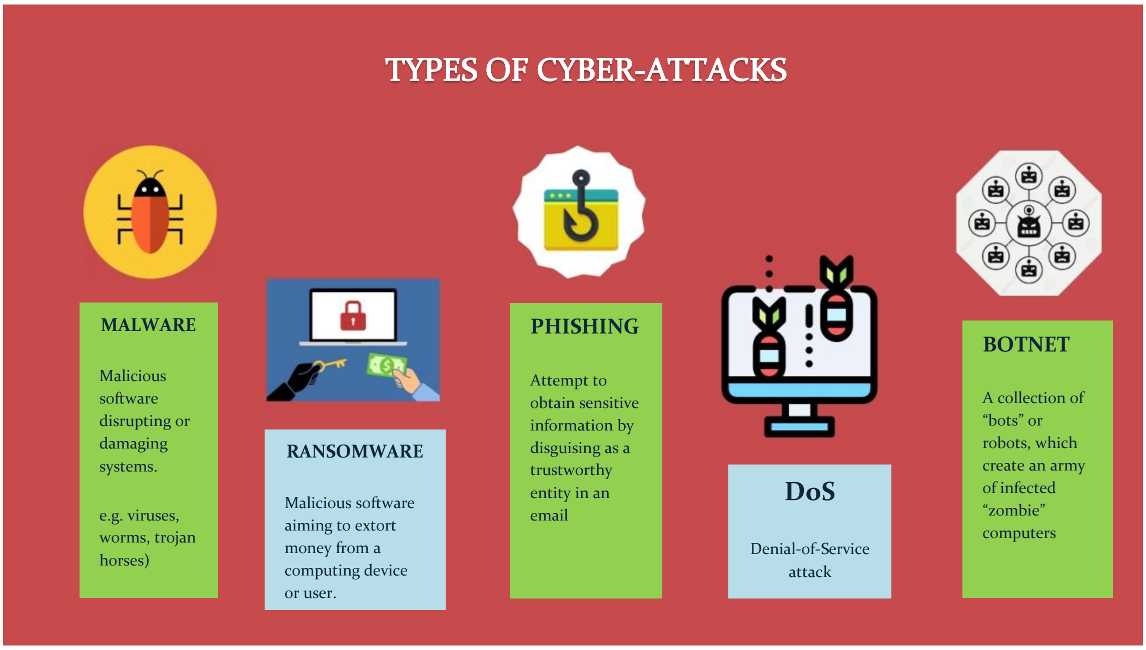

TYPES OF CYBER-ATTACKS
MALWARE
Malicious software disrupting or damaging systems.
e.g. viruses, worms, trojan horses)
RANSOMWARE
Malicious software aiming to extort money from a computing device or user.
PHISHING
Attempt to obtain sensitive information by disguising as a trustworthy entity in an email
DoS
Denial-of-Service attack
BOTNET
A collection of "bots" or robots, which create an army of infected "zombie" computers

Figure 1.2 Types of Cyber-attacks

1.4 Cyber Security Frameworks around the world

The growing threat deriving from the cyber domain has affected deeply the energy cyber security measures and practices of some countries. In this paper we will examine the cyber security strategies of three countries, the European Union, U.S. and Israel. U.S. and Israel are leaders in the national cyber security, while the European Union is making gradual steps towards becoming a significant international actor in the cyber security arena. It is important to note that due to unavailability of sources, the research does not examine the national cyber security strategies implemented in the energy sector by Russia and China, although they constitute influential states in the field of cyber security.

1.4.1 The case of the European Union

The Cyber Security for the Energy sector in the European Union is an answer to the transformations of energy production and distribution, the expansion of intelligent network devices and smart technology. These changes pose a requirement for a coordinated energy cyber security strategy at a European level. A major objective of the EU cyber security strategy is to reduce the vulnerabilities of CI and increase their resilience. [102] As cited in Lester (2016) cyber resilience refers to "the ability to prepare for, respond to and recover from a cyber-attack." He further explains that cyber resilience is not only prevention of a cyber-attack, but it is also the concern for continuous operation during an attack and the ability to adapt and recover.[103]

In 2013, the European Union adopted the Cyber Security Strategy: An Open, Safe and Secure Cyberspace. The five strategic priorities are a) achieving cyber resilience, b) drastically reducing cybercrime, c) developing cyber defence policy and capabilities related to the Common Security and Defense Policy (CSDP), d) developing the industrial and technological resources for cybersecurity and e) establishing a coherent international cyberspace policy for the European Union and promote core EU values. [104] This strategy is bound both for private and public sector of EU-member states. Thus, it obviously includes the key sector of energy.

Moreover, as the Joint Communication states, the task of cyber security involves long and short-term practices and tools, so that each of the member states can tackle cyber-security challenges, but also the overall performance of the EU could be enhanced. [105]

In order to achieve cyber resilience, the Commission of the EU, passed, among others, the Directive on Security of network and Information (NIS Directive). The Directive adopted in July of 2016 provides legal measures to boost the overall level of cybersecurity in the EU. Particularly, for the energy sector, the Directive aims to ensure "a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy". What is more, "businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority."

Furthermore, the Commission took steps in order to enhance ENISA's

[102] (European Parliament Directorate-General for Internal Policies, 2016)

[103] (Lovells, 2016)

[104] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

[105] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

role in building a stronger cyber security in the EU. Particularly, EU asked ENISA to assist member states in developing strong national cyber resilience capabilities, by building expertise on security and resilience of industrial control systems, transport and energy infrastructure. [106] At the same time, ENISA is expected to support Member States to carry out pan-European cyber incidents exercises on a regular basis. [107]This could be seen as a tool which could help utilities in the energy sector to be prepared and ready if a cyber event occurs.

European Union acknowledges that energy sector of its member states is increasingly exposed to cyber threats. This could mean potential damages to a) confidentiality – unauthorized access to or interception of information, b) integrity – unauthorized modification of information, software, physical assets and c) availability – blockage of data transmission and/or making systems unavailable. These threats apply to all generation, transmission and distribution technologies, and to energy market services. [108] Within this context, the European Union established the Energy Expert Cyber Security Platform (EECSP) - Expert Group. Its mission is to "give guidance to the Commission on policy and regulatory directions at European level, addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies as well as nuclear." [109]

Initially, the expert group is committed to analyzing the existing legislation, initiatives, projects and cyber security strategies, which are linked to all parts of the energy sector, and the interplay between various EU legislative instruments applicable to the energy sector such as the NIS Directive and the General Data Protection Regulation At the same time, the group will explore ways to streamline the corresponding obligations impacting the energy sector and propose some possible solutions. [110]

Secondly, based on the first deliverable, the group of experts is bound for developing short-, medium-, and long-term strategy and reinforcing the implementation of the new legal basis of the NIS directive and the GDPR and lastly, to provide input for legislative acts, adopted in the future. [111]Finally, the group will focus on regular monitoring of the various findings in line with the implementation of relevant legislation and the evolution of risks, threats and

[106] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

[107] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

[108] (European Commission Directorate-General for Energy, n.d)

[109]_(European Commission, Energy Expert Cyber Security Platform (EECSP) - Expert Group (E03341), 2017)

[110] (European Commission Directorate-General for Energy, n.d)

[111] (European Commission Directorate-General for Energy, n.d)

vulnerabilities in the energy sector.[112]

The European Union also established the European Energy - Information Sharing & Analysis Centre. EE-ISAC helps utilities to improve the cyber security and resilience of their grid by enabling trust-based data and information sharing. EE-ISAC is a joint initiative of 4 major European utility companies together with universities, governmental bodies and technology providers. The participants get the chance to share security data and analysis, to exchange experiences about cyber incidents and compare security solutions. [113] The Cyber Security Strategy of 2016 notes that the scale of the threat to energy cyber security is massively increasing as energy systems develop ubiquitous intelligence and communications capabilities throughout their operations.[114]

What is more, the report includes some of the public and private projects that are driving innovation in energy cyber security and some information-sharing platforms and initiatives. For example, the European Smart Metering Industry Group represents smart energy solution providers and publishes frameworks and standards aimed to ensure efficient integration of new energy management systems. Sparks refers to Smart Grid Protection Against Cyberattacks project, which is EU-funded and conducts analysis of smart grid security measures, publishes standards and develops technological tools, such as an intrusion detection mechanism for SCADA systems. As for information-sharing bodies, we can mention European Reference Network for Critical Infrastructure Protection, (ERNCIP), a network established to improve the protection of critical infrastructures in the EU[115] or Thematic Network on Critical Energy Infrastructure Protection (*TNCEIP), which* allows operators to exchange information on threat assessment, risk management, cyber security, and other related topics.[116]

In September of 2017, the European Union updates its 2013 Cyber Security Strategy, intended to improve the protection of Europe's critical infrastructure and boost the EU's digital self-assertiveness towards other regions of the world.[117] According to the EU's cyber security factsheet, published in 2018, cyber incidents and attacks are reportedly on the rise. Since 2016, every day there are more than 4,000 ransomware attacks and have increased by 300% since 2015. [118]"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks

[112] (European Commission-Directorate General for Energy, n.d)
[113] (European Energy - Information Sharing & Analysis C, 2019)
[114]_(European Commission, Protection of critical infrastructure, n.d)
[115] (Joint Research Center , 2018)
[116] (European Commission, Protection of critical infrastructure, n.d)
[117] (Bendiek , Bossong , & Schulze , 2017)
[118] (European Commission, 2017)

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"[119] highlighted the European Commission President Jean-Claude Juncker in his State of the Union speech September 2017. Whilst the EU's 2013 Cyber Security Strategy remains in place, the updated version introduces an extensive package of new measures. Particularly, the 2013's Cyber Security Strategy's goal to foster a reliable, safe and open cyber ecosystem, remains valid. But the continuously evolving and deepening threat landscape calls for more action to withstand and deter attacks in the future. [120]

Cyber Security Strategy of 2017 aims to build greater resilience and strategic autonomy and boost capabilities in terms of technology and skills. The prerequisite for this are structures eligible to build strong cybersecurity and to react when needed, with the full involvement and galvanization of all key actors, the EU, Member States, industry and individuals. This approach also aims to enhance deterrence of cyber incidents, the detection, tracing and accounting those responsible. Lastly, it would promote international cooperation, recognizing the global dimension of cyber security issues and the aim of EU leadership on cyber security. [121]

The main pillars of the updated Cyber Security Strategy of the EU are

1) Building resilience to cyber-attacks,

1) Creating effective EU cyber deterrence and

1) Strengthening international cooperation on cyber security

As in EU's Cyber Strategy of 2013, building cyber resilience is still a fundamental objective of EU Cyber Strategy. It requires robust and effective structures to promote cybersecurity and to respond to cyber-attacks in the Member States but also in the EU's own institutions, agencies and bodies. What is more, it needs a more comprehensive, cross-policy approach to building cyber-resilience and strategic autonomy, with a strong Single Market, major advances in the EU's technological capability, and far greater numbers of skilled experts.[122]

One of the most important measures, which aims to enhance EU's cyber resilience is a reform proposal of ENISA. Particularly, it includes a permanent mandate for the agency. Through this way, ENISA can provide support to each

[119] (European Commission, 2017)

[120] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[121] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[122] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

of the Member States, EU institutions and businesses in key areas, such as the implementation of the NIS Directive. [123] What is more, ENISA will have a stronger advisory role on policy development and implementation, enhance the European preparedness by organizing yearly pan-European cybersecurity exercises, support EU policy development on information and communications technology (ICT) cybersecurity certification and play an important role in stepping up both operational cooperation and crisis management across the EU. Lastly, the agency will also serve as a focal point for information and knowledge in the cybersecurity community.

What is more, Commission proposed an EU cyber security certification framework. As the Joint Communication mentions, the Framework would lay down the procedure for the creation of EU-wide cybersecurity certification schemes and would cover several products, services and systems which adapt the level of assurance to the use involved (whether it's critical infrastructures or consumer devices).[124] At a later stage, Commission aims to involve stakeholders and have them focused on cyber security of essential services such as the energy sector, which is becoming increasingly digital and interconnected.[125]

At the same time, the Commission recognizes the need to implementing the NIS Directive in full and developing its fullest potential in key sectors. Citing the Joint Communication, "The Directive on the Security of Network and Information Systems (the "NIS Directive") is the first EU-wide cybersecurity law. It is designed to build resilience by improving national cybersecurity capabilities; fostering better cooperation between the Member States; and requiring undertakings in important economic sectors to adopt effective risk management practices and to report serious incidents to the national authorities." The NIS Directive is at the heart of the EU cyber resilience, so the acceleration to the implementation process is necessary for key sectors such as energy, due to its increasingly globalized, digitally-reliant and interconnected nature and the essential role in the national security.

Another important point of the EU Cyber Security Strategy of 2018, relevant to the energy sector, is the swift implementation of the blueprint for cross-border major incident response. The Blueprint presents objectives and modes for fast and effective operational response at Union and Member-State

[123] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[124] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[125] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

level to the cyber security incidents and crisis. [126] In regard to the energy sector, this initiative is of a high importance, since it provides a crisis mechanism, which could be used to secure the continuous, uninterrupted energy supply in the EU and the functionality of economies and societies. It will also allow each Member State to seek support at the EU level to tackle with a cyber incident in its energy sector and mitigate the attack's impact.

The updated EU Cyber Strategy focuses also on "cyber hygiene" and awareness as a way to enhance the cyber resilience in several sectors, including the energy. The human factor is often involved in cyber security incidents, either intentionally or not. The EU Strategy acknowledges that cyber security is everyone's responsibility, beginning with the personal level and ending up on the national and EU Member-State level.

The second pillar of the EU Cyber Strategy of 2018 is creating an effective EU cyber deterrence. At the center of this objective is a more effective law enforcement and framework of measures focusing on detection, traceability and prosecution of cyber criminals. [127] This initiative increases the ability of the EU and its member states to identify malicious cyber actors, to promptly investigate cyber-attacks and to bring perpetrators to justice, in every sector that potentially is attacked by a cyber threat, including the energy sector.

The last pillar of the new EU Cyber Strategy refers to the goal of strengthening the international cooperation on cyber security. Specifically, this refers to a strategic framework for conflict prevention and stability in cyberspace, a new Capacity Building Network to support third countries' ability to address cyber threats and EU Cybersecurity Capacity Building Guidelines to better prioritize EU efforts and lastly, further cooperation between EU and NATO, including participation in parallel and coordinated exercises and enhanced interoperability of cybersecurity standards.[128] All of these steps aim to enhance cyber security in several sectors of EU interest, featuring the energy sector too. Nowadays, the cyber security in the energy sector is a priority at the EU level. On 16th October of 2018, European Distribution System Operators' Association for Smart Grids (EDSO) and the European Network for Cyber Security (ENCS) hosted Smart Grid Cyber Security event. During the technical workshop, which was organised in Brussels, explored the growing challenges of smart grids cyber security and the increased responsibilities placed on electricity distribution system operators (DSOs). The Secretary General of EDSO Roberto Zangrandi underlined that cyber security and digital safety is a

[126] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[127] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

[128] (European Commission, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017)

major responsibility for stakeholders, citizens and the industry itself. He also stressed that the great challenge ahead of us is to define a socially responsible digitalization in our sectors and notes that cybersecurity and digital safety will be the new Civil Right for the citizens. [129]

In the light of this, EDSO and ENCS have agreed to jointly take active leadership in the sector, committing to together: a) take responsibility for grid security requirements and testing, and assuring that certification delivers an improved level of grid security, b) provide dedicated security training and exercises, and to develop and expand this training portfolio in line with threat landscape developments and c) establish a research agenda covering the needs and priorities of European DSOs, and collaborate on Horizon 2020 security call applications. [130]

All in all, the EU has shared competences in the field of energy along with the Member States. This means that EU countries exercise their own competence where the EU does not exercise, or has decided not to exercise, its own competence. [131]

What is more, many of the proposals on the EU level, a voluntary character and a subsidiary role in the aim of cyber security in the energy sector. Many Members States, such as France and Germany, have developed their own national cyber security strategy and tools to prevent and respond to cyber incidents. In other words, the Member States of the EU have the responsibility of securing their energy sector from cyber threats. On a collective level of the EU, its institutions can assist, support, develop guidelines and proposals, provide tools and funds, and promote coordination and cooperation among Member States.

At the same time, due to the potential or actual borderless nature of the cyber risks, an effective national response would often require EU-level involvement. Thus, the EU will seek to establish a coherent international cyberspace policy for the European Union and promote EU core values of human dignity, freedom, democracy, equality, the rule of law and the respect for fundamental rights. [132] Lastly, the Commission and the High Representative, in cooperation with Member States, will work towards a coherent EU International cyberspace policy to increase engagement with key international

[129] (EDSO, 2018)

[130] (EDSO, 2018)

[131] (EU-Lex, n.d)

[132] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

partners and organizations, to mainstream cyber issues into CFSP, and to improve coordination of global cyber issues. [133]

1.4.2 The case of USA

A. Cyber Security Strategy 2018-2020

One of the core priorities for the Department of Energy is the cyber security of Federal systems and networks. It has prepared the Cyber Security Strategy 2018-2020, as a plan for an effective, collaborative, enterprise-wide cybersecurity posture and defense. The plan leverages diverse perspectives and experience from across the Energy Enterprise, establishing a common understanding and a culture of accountability.

The Strategy identifies four Principles of Success, crosscutting and interlinked. The first on is "One team, One fight". As declared by the DOE itself, cyber security is a top priority. Consequently, the DOE's leadership must focus on integrating policies, activities and operations of the Department to fulfill the derived goal. [134] This principle stresses the need for coordination, integration and cooperation on a daily basis to secure the Department as "One Team. One fight". The second principle of the strategy is Employment of risk management methodology. Given the fact that the cyber security landscape is constantly evolving, and threats are dynamic, insidious and becoming more sophisticated and complex, the Department of Energy must focus its efforts on conducting sound risk management, calculating and evaluating incidents and modifying and constantly calibrating its cybersecurity defense-in-depth and defense-in-breadth posture.[135]

Third pillar of the Cyber Security Strategy 2018-2010 for the energy sector is the Prioritized Planning and Resourcing. Cyber security must be integral part of DOE's task such as planning risk management, budgeting and execution of plans. This means that cybersecurity must receive resource allocations and focus commensurate with its priority status.[136] Through this way, as it is mentioned in the Cyber Security Strategy, adverse results such as harm and loss of stakeholder trust, can be avoided. What is more, the leaders must be accountable for their failures in prioritizing cyber security needs. Finally, the third principle of Cyber Strategy 2018-2020 is linked to the implementation of the Executive Order 13800: Strengthening the Cybersecurity

[133] (European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace , 2013)

[134] (U.S Department of Energy , 2018)

[135] (U.S Department of Energy , 2018)

[136] (U.S Department of Energy , 2018)

of Federal Networks and Critical Infrastructure, which order several Federal agencies, among others DOE, to examine how Federal authorities and capabilities can support cyber risk management. [137]

The last principle of the strategy prepared by DOE is Enterprise-wide Collaboration. In order to meet the goal of cyber security, the Department needs a holistic approach to cyber security issues to cover all the sites, departments, laboratories and partners, each of which has unique missions, goals and needs. Evenly challenging is the stake of sound cyber security defense. It relies on a collaborative approach and customer engagement. To achieve this, the Department must understand the customers' needs, solicit customer feedback, address the cyber security issues in a clear manner and keep customers informed and interested. These actions are substantive to achieving the principle "One Team. One fight."

The Department aims to apply these four principles across four IT Strategy goals: The first one is the delivery of high-quality IT and cybersecurity solution. Secondly, the aim is to continuously improve the cybersecurity posture. Thirdly, the transition from IT owner to IT broker is set for better customer focus. The last goal is the Excellence as stewards of taxpayer dollars.

Within those four goals, the Cybersecurity Strategy identifies seven objectives. Each of the cyber security objectives is matched to a particular DOE's IT Strategy goals, as mentioned above. Specifically

In accordance to the first IT Goal, the Department sets the objective to secure and reliable access to mission essential systems, networks, and information resources.

What is more, the objective for second IT Goal tracks each function of NIST's Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. The Framework intends to enhance organizational capabilities in order to implement risk management measures and ensure that cybersecurity risk management processes are aligned with strategic operational and budgetary planning processes. Guidelines and tools such as the Cybersecurity Capability Maturity Model, Cybersecurity Evaluation Tool, and Electricity Subsector Cybersecurity Risk Management Process to enhance cyber security hygiene, to strengthen internal controls, to adopt universal standards and processes for cyber security functions. Furthermore, the Framework puts attention to protection.

Particularly, it makes provision for the development and implementation of enterprise controls, embraces standards and best-practices. Through this way, the Department intends to ensure confidentiality, integrity, and availability of its information resources and reduce risks, cost and increase resilience. Besides this, the framework promotes enterprise security awareness

[137] (U.S Department of Energy , 2018)

through workforce development and training. Specifically, the Department puts emphasis on training, education acquisition of skills and behaviors which foster a cyber security culture, improve the efficiency in the fields of identification, evaluation and risk management.

At the same time, the Department discusses the task of protection as an integral part of its Framework. To be more specific, the Framework welcomes several tools and processes to accelerate cyber threat detection, notification, and response across the enterprise. [138] For example, this includes the involvement of Joint Cybersecurity Coordination Center (iJC3), which consolidates disparate cybersecurity functions and streamline information sharing enterprise-wide. [139]. Lastly, the task of responding is essential for a successful cybersecurity framework and stipulates a rapid analysis of, and response to, anomalies and suspected events.[140] This goal entails the maturation of the cybersecurity Incident Management Program within DOE, expanding analytical forensics and response tactics, utilizing automated tools to streamline information technology security, improving incident management capabilities, and delivering training to frontline operators, on time and with precision.[141]

The third IT Goal, namely "Transition from IT owner to IT broker for better customer focus" is linked to customer focused cybersecurity. For example, the Department could inject customer requirements into information flow for the Department's IT, Information Resources Management, and Cybersecurity governance process or/and develop and implement iterative process for soliciting customer input/feedback and determining and understanding customer requirements and challenges. [142] The goal is to keep the customers informed, aware, and engaged in a collaborative partnership for more successful cyber security measures.

Finally, a risk-based approach is needed for the forth IT Goal. This approach is needed in all phases of the Department's IT project planning, execution, management, and procurement and at the same time requires a group of owners trained, equipped and aware of the value of employing cyber security measures. These owners are actual acceptors, or holders of risk but also customers. Lastly, the process should include several components of the DOE's ecosystem, such as the departments responsible for intelligence and counterintelligence, enterprise assessments, privacy, and physical, personnel,

[138] (U.S Department of Energy , 2018)
[139] (U.S Department of Energy , 2018)
[140] (U.S Department of Energy , 2018)
[141] (U.S Department of Energy , 2018)
[142] (U.S Department of Energy , 2018)

and information security.[143] Obviously, a more holistic approach is necessary for the success of DOE's mission.

B. National Cyber Strategy

In September of 2018, the White House published the National Cyber Strategy, first fully articulated cyber strategy for the United States since 2003, based on three pillars: I) Protect the American People, the Homeland, and the American Way of Life, II) Promote American Prosperity, III) Preserve Peace through Strength and IV) Advance American Influence.

The Administration acknowledges that evolution of cyberspace is inseparable component of America's financial, social, government, and political life. The rise of the Internet and the expansion of digital services in several facets of the modern life is believed to correspond with the rise of the United States as a superpower. [144] At the same time the United States is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks. For example, states such as Russia, China, Iran, and North Korea are believed to exploit the cyberspace and cyber capabilities to pose strategic threats to U.S. prosperity and security. [145] This means that economy, democracy and its virtues, intellectual property or infrastructure of the United States are vulnerable and under serious danger. In the light of this, Donald Trump highlighted that "We will continue to lead the world in securing a prosperous cyber future." and thus, unveiled America's first Cyber Security Strategy in 15 years.

What is more, the National Security Council staff will coordinate with several departments, agencies and the Office of Management and Budget (OMB) on an appropriate resource plan to implement this Strategy, while the involved departments and agencies will execute their missions following the strategic guidance.[146]

The Pillar I focuses on the objective of Protecting the American People, the American Way of Life, and the American interests, as the forefront of the National Security Strategy. It alludes to management of cybersecurity risks, the security of Federal networks and information, critical infrastructure, combating cybercrime, and improvements in incident reporting. These are steps to increase the security and resilience of the Nation's information and information systems.[147]

[143] (U.S Department of Energy , 2018)
[144] (The White House, 2018)
[145] (The White House, 2018)
[146] (The White House, 2018)
[147] (Grant, 2018)

The Pillar II namely “Promote American Prosperity” describes the effort to “preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency.”

The Pillar III of the National Cyber Strategy relates to the promotion of peace and stability through responsible state behavior, attribution of disruptions and destabilizing factors in cyberspace, and the imposition of costs on malicious cyber actors and the growth of the national power. [148]

Finally, the last Pillar of the National Cyber Strategy is a commitment of the United States to maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace.[149]

According to the official report of Trump’s administration, this means that it will take care of maintaining on a long-term basis openness, interoperability, security, and reliability of the Internet and the freedom online expression and activity. What is more, the last pillar describes the goal of international cyber capability, which would allow United States’ partners to defend themselves and to along with the United States address common threats and serve mutual interests. [150]

All in all, Trump emphasizes his commitment to strengthening America’s cybersecurity capabilities and securing America from cyber threats. At the same time, he stresses the need for action of Americans and companies in order to enhance the national cybersecurity. He concludes by saying “We will continue to lead the world in securing a prosperous cyber future”.[151]

The new cyber strategies reflect the changes in the political, technical, and institutional environment over the last years. In that time, the cyber threat has evolved significantly. For example, the cyber-attacks, such as the WannaCry in 2017 and notPetya and serious concerns about hostile cyber actions of other states on critical infrastructure or intellectual property of U.S describe the escalating danger in the cyber domain. The U. S strategy describes a more aggressive, active, offensive and proactive stance towards the cyber threats and foresees conducting of operations against nation states and criminal groups in the cyber domain. The administration of Donald Trump acknowledges that the ongoing expansion of cyber space and digitalization need a higher degree of attention, determination, coordination, and steps towards protection, security and defense.

What is more, this move coming from the biggest super power in the

[148] (The White House, 2018)
[149] (The White House, 2018)
[150] (The White House, 2018)
[151] (The White House, 2018)

world illustrates that decision and policy makers perceive the cyberspace as the new domain of antagonism between states and a new arena of international relations.

1.4.3 The case of Israel

According to the Global Cyber Security Index [152] of 2017, Israel is classified into the category of counties in the maturing stage of cyber security and overall, holds the 20th place in over 150 countries in the Global Rank. Particularly, maturing stage refers to those countries which have scored between the 50% and 89%, have developed complex commitments, and are engaged in cybersecurity programs and initiatives. [153] Israel has become one of the world leaders in cybersecurity and has one of the world's lowest cybercrime rates.[154]

Israel has been at the forefront of hi-tech and internet infrastructure and services development for the past decade. [155] Technology, innovation and cyber capabilities have been the core of the national security concept of Israel, as it sought to gain and maintain a qualitative edge over its Arab enemies, which are more populated, gifted and benefited for example by geography. Moreover, the country puts a lot of emphasis on technological and scientific innovation, in order among others, to enhance the security if its critical infrastructure against cyber-attacks.

As Cohen, Freilich and Siboni mention, Israel is a state which relies heavily on cyber technology and constitutes a primary target of cyber threats.[156] For example in 2015, cyber-attacks increased by 38% with an average of 161,927 per day and Security incidents cost businesses an average of $3.8 million per year.[157] The Energy Minister of Israel, Steinitz said that Israel's Electric Authority was targeted by a "severe cyber-attack" but at the same time succeeded in mitigating the attack by shutting down systems to prevent virus from spreading.[158]

In response to the threats and potential attacks, Israel has invested resources to upgrade its cyber capabilities, both offensive and defensive. At the

[152] Is a reference of International Telecommunications Union which measures the commitment of countries to cybersecurity at a global level to raise awareness of the importance and different dimensions of the issue along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation – and then aggregated into an overall score. Retrieved from: (International Communications Union, n.d)

[153] (International Telecommunications Union , 2017)

[154] (Ouwendijk, n.d)

[155] (Housen-Couriel, 2017)

[156] (Cohen , Siboni , & Freilich , 2016)

[157] (Kletzkine, n.d)

[158] (Staff, 2016)

same time, it runs research and development programs for a better and more effective cyber defense strategies and technologies and constitutes a center for prominent foreign cyber security companies such as IBM, Cisco, Deutsche Telekom or Microsoft. [159]

Israel established a national cyber strategy in 2011 under the title" Advancing National Cyberspace Capabilities". The strategy incorporates measures which promote Israel's leadership in cyber security at a global level. Besides this, the strategy establishes the first national advisory and fortified body responsible for cyber security of Israel, National Cyber Bureau (INCB).

Specifically, the National Cyber Bureau is an advisory body for the Prime Minister, the government and its committees regarding cyberspace. Furthermore, it has some administrative duties such as preparation of meetings and discussions and follow-up on implementation of decisions. Moreover, the Bureau has the task to guide and keep informed all the relevant bodies regarding cyber security policies decided by the Prime Minister and the government. Besides this, the Bureau holds the responsibility for the conducting of national and international exercises and developing a plan for effective national response to emergency situations in cyberspace. Last but not least, the Bureau is engaged in the task of education and raising awareness of public regarding the cyber security issues such as practices of cyber hygiene and promoting the R&D and the development of domestic cyber solutions and technologies.

Further to the Government Resolution No. 3611 of August 7, 2011, regarding "Advancing the National Capacity in Cyberspace" the Government of Israel formulated the Resolution 2443 entitled Advancing National Regulation and Governmental Leadership in Cyber Security.[160] The Resolution advances the task of integrating new cyber security regulations within the already-established purview of existing government ministries and other regulators.[161] Additionally, as cited in NATO Cooperative Cyber Defence Centre of Excellence's report, the Resolution 2443 "sets out the authority and capacity for the INCB's regulation of the market for cyber security professionals, services and products" [162]

A new Resolution of Israel's Government, No. 2444 of February 15, 2015 titled "Advancing the National Preparedness for Cyber Security" established the National Cyber Security Authority. The unit's mission is to defend cyberspace and more detailed, to "conduct, operate and implement, as needed, all the operational defensive efforts in cyberspace at the national level, from a holistic

[159] (Kletzkine, n.d)

[160] (The Government Secretary, 2015)

[161] (Housen-Couriel, 2017)pg 12

[162] (Housen-Couriel, 2017)

perspective, for the purpose of providing a complete and continuous defensive response to cyber-attacks, including handling cyber threats and incidents in real time, formulating an ongoing situational awareness, consolidating and analyzing intelligence, and working with the defense community." [163]

Among other responsibilities, the National Cyber Security Authority operates the CERT of Israel, namely the "Israel's civilian center for addressing Information Security and Cyber events". [164] Thus, the National Cyber Security Authority contributes to CERT's activities such as the investigation and response to cyber security incidents and/or providing information and recommendations to public.

Another task of the NCSA, of great importance, is to build and enhance the cyber resilience of the market. This can be achieved through for example preparedness, training and exercises, regulation, licensing, standardization in the market.[165] Last but not least, the Resolution 2444 envisages the establishment of the National Cyber Directorate or Ma'arach, which consists of the two institutions, the National Cyber Bureau and the National Cyber Security Authority. However, the two bodies remain independent auxiliary units in the Prime Minister's Office. [166]

The cyber security policy of Israel involves several other bodies, such as the mentioned CERT-IL or the Israeli Defense Forces (IDF). The IDF is the national army in which young male and female Israelis are obliged to serve for a period between 2.5 and 3 years. [167] The IDF's goal is to defend the existence of the State of Israel, its independence and the security of the citizens and residents of the state. [168]

The IDF has not neglected the innovation, technological innovations and cyber capabilities, although it has initially been engaged in military services, defense and training. In 2015, Chief of Staff Lt. Gen. Gadi Eisenkot decided to bring some structural changes in the IDF. He highlighted: "establishing this arm will enable the IDF to perform better on the [cyber] fronts…and will utilize the technological and human advantages already existing in Israel." [169]

Due to unprecedented challenges that the IDF face in the cyber realm and the growing importance of cyber capabilities as a component of military strength and offensive operations and defense strategies, it was decided to establish a cyber command, which would lead the IDF's activities in the

[163] (The Government Secretary, 2015)pg.1
[164] (IL-CERT, n.d)
[165] (The Government Secretary, 2015)
[166] (The Government Secretary, 2015)
[167] (Ouwendijk, n.d)
[168] (Israeli Defense Forces, n.d)
[169] (Elran & Siboni , 2015)

cyberspace. As Elran and Siboni note,[170] as a preliminary stage, the cyber branch would be established within the Military Intelligence Directorate (DMI) and the C4I Telecommunications Directorate of the IDF.[171]

Lastly, it is worth mentioning that the state of Israel invests heavily in human capital, as an inseparable piece of the national cyber security puzzle. Israel sees people and their skills, experiences and ambitions as a driving force and substantial ingredient in cyber defense. [172] This is the reason why the governments in deeply engaged in welcoming cyber education early in the middle school or/and promoting trainings, university programs and research activities.

All in all, Raska emphasizes that "Israel is developing "a national cyber defensive envelope"" He explains that Israel develops a cyber security strategy with multiple layers, evolves among others computerized systems, professional human capital, early warning and both a passive and active defense.[173]

1.5 Policy Recommendations

The strategies and good practices which have been developed and implemented worldwide illustrate some necessary measures and procedures to enhance cyber security in the energy. It is necessary to highlight that, while there are generally three levels of management, in this paper we refer to the top level of the pyramid, namely the level characterized by the formulation and implementation of energy policies. [174] The policy recommendations discussed as detailed below do not apply to the two remaining levels, the middle and the lower levels of management.

First of all, the energy sector needs to be aware that the human factor is often linked to cyber threats in the energy sector. Humans are inherently complex and multi-faceted creatures with their own agendas, influences, faults, beliefs, and priorities.[175] Thus, cyber security is not only about IT, technological defense, networks and systems. It is also about people, as the users and operators of technological devices. As long as, the human factor is integral part of the energy supply chain, cyber dangers such as social engineering cannot be excluded.

To mitigate the risks which derive from lack of cautiousness, careless

[170] (Elran & Siboni , 2015)
[171] (Elran & Siboni , 2015)
[172] (Press, 2017)
[173] (Raska, 2015)
[174] (Department of Energy Republic of South Africa , n.d)
[175] (Australian Computer Society, 2016)

behavior and human mistakes, the energy sector should prioritize training and cyber security awareness programs. Through rigorous and constantly up to date training, digital literacy and education of security staff and employees in the energy companies, they develop the capabilities necessary to understand the complexity of cyber security as a constantly and quickly evolving field, to recognize and evaluate threats and interpret the changing landscape. At the same time, educational trainings can provide staff with knowledge on privacy, data protection and security measures which can be very useful in protecting themselves from cyber threats and counterbalancing their vulnerabilities. All in all, the energy companies can build a group of trusted, highly educated, trained and equipped professionals that contribute to the cyber security if the energy sector.

Secondly, a fundament for cyber security in the energy system is effective and systematic cyber hygiene. As mentioned above, this refers to all the steps and procedures of a company/ utility which, when regularly implemented, can dramatically increase the cyber security of the energy systems and networks. Most simple practices include complex passwords changed regularly, which can prevent malicious activities and data breach, updating of software and upgrading aging hardware and systems, back up data to a secondary source, or/ and limit to the number of users with access. An effective cyber hygiene requires routine and repetition and is on-going responsibility of the energy sector.

Thirdly, cyber security can be enhanced through risk analysis management. Particularly, a good starting point in the risk assessment and management is to define the critical infrastructure, assess the capabilities and identify the assets of the company, which require protection and should be prioritized. In the next place, the company must recognize its vulnerabilities and pathways for malicious actors to reach critical operational systems. Lastly, it is important to identify threats or warning signs or potential risks. To sup up, cybersecurity risk management can help in identification of serious security vulnerabilities of each company and actor involved in the energy sector and in application of some solutions that will keep the systems and networks protected.

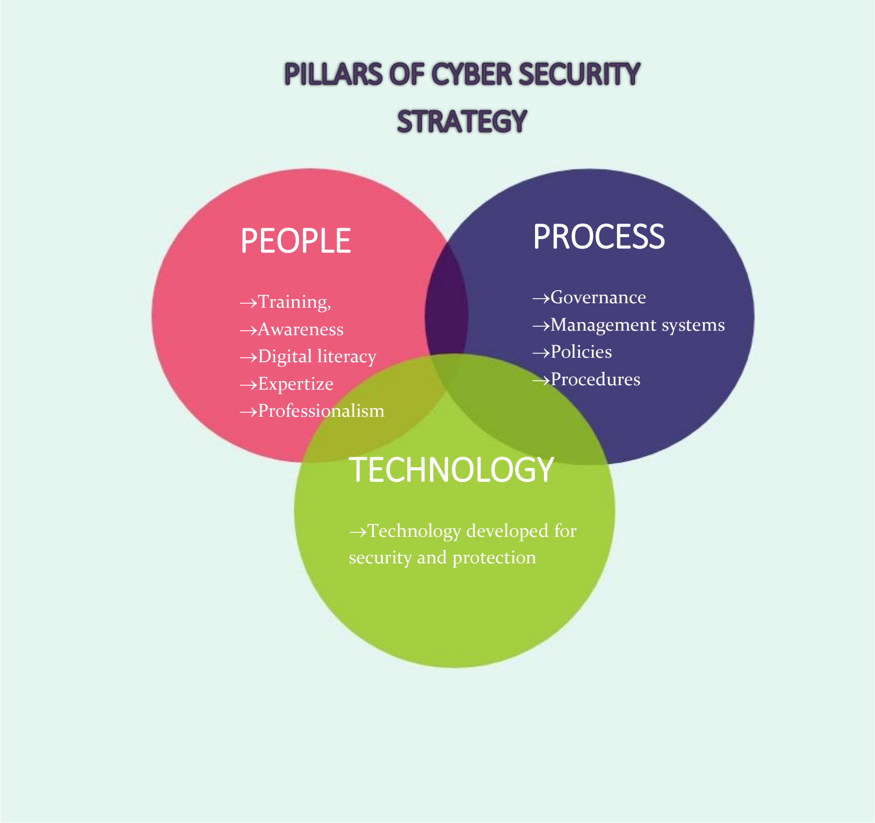
Furthermore, a company should introduce a comprehensive cyber crisis management plan to respond, minimalize the impact and recover quickly from the cyber incident. No matter how accurate and consistent an energy company/utility is in the implementation of all the cyber security procedures and practices, it may still get attacked by a malicious cyber actor and suffer a cyber incident menacing the continuous flow of energy products and services. This is the reason why a company should develop a response plan, which laid out right in time can allow it to close vulnerabilities, limit the damage of a breach and introduce repair measures.

At the same time, cyber security requires continuous modifications and so does the cyber security strategies in the energy sector. It should include periodic reviews, annual reports, regular updates, reorganizations modifications and reforms, if necessary.

The energy sector should not rely only on an efficient reactive behavior in order to overcome a cyber incident and mitigate its impact on the energy sector and the sectors which are directly or indirectly linked to it. The energy sector should put emphasis on prevention. Particularly, tools which cement a proactive stance and a high level of preparedness should be developed and regularly used. For instance, companies should conduct routine exercises, monitor for early warnings, and gather threat intelligence. As a result, an energy company can substantially build cyber resilience ability.

Lastly, promotion of R&D, research programs of security tools, development of new legal framework for punishment of cyber criminals, data and good practices exchange, communication and coordination between the utilities and industries involved in energy supply chain, cooperation between private and public sector, all are not the cyber security panacea, but surely some important steps that could be taken on the high level of management towards better cyber security in the energy sector. All in all, cyber security is constantly evolving, requires new approaches and tools, is an active and on-going process, just like the threats which aims to combat.

What is more, it relies on a multidisciplinary and a multidimensional approach, bridging people, policies and ICT. So, as shown in the Figure 1.5.1 beneath, the cyber security strategy should combine three pillars, People, Technology and Policies and procedures. The energy sector needs proper processes to implement cyber security strategies, and trained and specialized staff, who possesses the qualifications and capabilities to use the technology developed for security and protection. Each of the tree pillars is irreplaceable and necessary for an all-rounded strategy. The process of digitalization and integration of technology in our lives will not abate. That is why, our defense and security measures must be upgraded, reinforced and wedded with innovation.



1.5.1 Figure: The Three Pillars of Cyber Security Strategy

1.6 Concluding Remarks

Cyber threats are highly consequential on every sector of human activity. This derives from the fact that no human enterprise is confined only to physical world. Moreover, the cyber dependency of modern societies and governments is growing, the use of technology has become an inextricable part of our everyday life. Besides this, more and more individuals, governments and other actors conduct their transactions and activities electronically. In fact, cyber space has become a significant component of human involvement.

Thus, cyber-attacks are associated with serious social, political and economic cost.

All of these relate to the energy sector, since it is turning to more and more digitalized and cyber dependent. At the same time, the role of energy sector is becoming even more important and vital due to the global trends of growing energy demand, rapid population growth and economic development. The goal of securing energy needed for growth, activities and proper functioning of states and societies is becoming challenging. Rising demand requires more energy resources and a better management of the energy supply chain. At the same time, the protection of the energy sources, infrastructure and systems has evolved into a more complex task, since their security must be guaranteed not only in the physical world, but gradually in the cyber space too. Cyber security is turning into a priority of policies and agendas for security and defense, as it appears to be a category of risk, stubbornly opaque and resistant to attempts to manage, monitor, and measure.[176]

Thus, the interruptions of energy supply can seriously impact our modern lifestyle. For example, they would jeopardize the functioning of hospitals, public transportation, water systems and other infrastructure, which are critical to the security of the individual, the communities and states. What is more, interruptions can create havoc in cities and cause major financial losses for businesses.

Due to the acceleration of digitalization and the rising value of energy sector and products, they have become an attractive target for cyber actors, such as cyber terrorists or state sponsored actors. There is a wide range of malicious actors behind cyber incidents. They are using several cyber weapons and techniques, developing new tools and increase their sophistication. They can attack industrial control systems and networks, such as power grids, transportation systems or chemical plants for plenty of different reason and motives. It is important to note that attacks on energy infrastructure, such as the cyber-attack on Georgian government in 2008, during the Russia-Georgia war, the Stuxnet worm which harmed Iran's nuclear enrichment program, the attack on German steel mill in 2014 or on Ukraine in 2015 when 230,000 people lost power when 30 sub-stations in Western Ukraine were shut down, firstly indicate that the landscape of war is changing and, from now on attacks can be launched remotely, indirectly and discreetly and secondly, that the weapon of choice for states and non-state actors may not be the army or/and guns, but a keyboard and a computer with Internet access.

In the light of this, energy sector and companies must be aware that, as a key part of the critical national infrastructure and thus, constitute a highly attractive and valuable target for state and non-state threats, they likely be targeted more often than before. Moreover, traditional cyber security measures are inadequate and so, companies must introduce new solutions to be one step ahead and stay prepared for cyber threats. [177] From now on, this is an added challenge that energy sector faces.

The pervasive and covert nature of the cyber threats has surely affected the architecture of strategies and measures that governments have shaped

[176] _(IBM I Sales and Distribution, 2012)

[177] (MWR InfoSecurity, n.d)

worldwide. For example, U.S introduced new cyber strategies, first time since more than a decade. The EU is taking steps towards a more comprehensive approach towards the cyber security of the energy sector of its Member States, by introducing the NIS Directive or establishing the Energy Expert Cyber Security Platform.

The frameworks which are introduced worldwide depict some measures which constitute the fundament of an efficient cyber security strategy constructed by the top level of energy industry management. For example, measures which close the knowledge and skills gaps, enhance cyber hygiene and awareness, a comprehensive plan of prediction, response, recovery after a cyber-attack, crisis management, and the promotion of R&D, innovation and development of policies and tools could be the basic pillars of a cyber security strategy for the energy sector and companies. The energy cyber security strategy should be constructed on three substantial pillars: People, Technology, Procedures and Processes. At the same time, it should combine both a reactive and proactive approach towards cyber security issues.

All in all, it is important to remember that the digitalization and ICT facilitate and accelerate many human activities, among other the energy production and distribution and for provide new opportunities more efficiency, less costs, better productivity and even more security. Concurrently, these processes create new vulnerabilities and thus, potential risks, which derive from actors operating in the cyber domain. Once we achieve to cope with the malicious cyber activity, we could gain many profits from the opportunities which technology gives and accomplish a higher quality of services and life.

Bibliography

Australian Computer Society. (2016, November). *Cybersecurity - Threats Challenges Oportunities.* Retrieved from https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

Bailey, T., Kolo, B., Rajagopalan, K., & Ware , D. (2018, September). *Insider threat: The human element of cyberrisk.* Retrieved from McKinsey & Company: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

Barichella Arnault. (2018, February). *Cybersecurity in the Energy Sector: A Comparative Analysis between Europe and the United States.* Retrieved from Ifri Centre for Energy : https://www.ifri.org/sites/default/files/atoms/files/barichella_cybersecurity_energy_sector_2018.pdf

Barnes, A. (2000). *Energy Security.* Retrieved from World Energy Assessment and its Sustainability,(Chapter 4): http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.463.774&rep=rep1&type=pdf

Bendiek , A., Bossong , R., & Schulze , M. (2017 , November). *The EU's Revised Cybersecurity Strategy Half-Hearted Progress on Far-Reaching Challenges.* Retrieved from Stiftung Wissenschaft und Politik German Institute for International and Security Affairs : https://www.swp-berlin.org/en/publication/revised-cybersecurity-strategy/

Bergasse , E. (2013, February). *The relationship between energy and economic and social development in the southern Mediterranean.* Retrieved from MEDPRO Technical Report No. 27: https://www.files.ethz.ch/isn/161565/MEDPRO%20TR27%20Bergasse%20Energy%20Supply%20and%20Demand%20Policies%20and%20Development%20rev.pdf

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015, January). *Cyber Resilience – Fundamentals for a Definition.* Retrieved from https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition

Björck, H. S. (2015). *Cyber Resilience – Fundamentals for a Definition*. Retrieved from https://www.researchgate.net/publication/283102782_Cyber_Resilience_-_Fundamentals_for_a_Definition

Bloomberg NEF. (2017 , November 9). *Digitalization of Energy Systems.* Ανάκτηση από https://about.bnef.com/blog/digitalization-energy-systems/

Boeck , B. (2015 , December). *Phishing: The Biggest Cyber Threat Today* . Retrieved from Lockton Companies : https://www.vanbreda.be/vrb-custom/uploads/2015/12/Lockton_whitepaper_phishing.pdf

Bronk , C. (2016). *Cyber Threat: The Rise of Information Geopolitics in U.S. National Security* . Santa Barbara : ABC-CLIO.

Brook, C. (2018, December 5). *What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More.* Retrieved from https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

Bryk , J. (2016, April 12). *CSO* . Retrieved from Defining the threat in the energy sector: https://www.csoonline.com/article/3052260/techology-business/defining-the-threat-in-the-energy-sector.html

Cohen , M., Siboni , G., & Freilich , C. (2016, August). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*.

COMMISSION RECOMMENDATION of 22 January 2014. (2014, 1 22). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:039:0072:0078:EN:PDF

Department of Energy Republic of South Africa . (n.d). *Module 5: Organisational Structure for Energy Management* . Ανάκτηση από Industrial Energy Management Training Course: http://www.energy.gov.za/EEE/Projects/Industrial%20Energy%20Management/IEM%20Training/Modules/IEMTCModule5_final.pdf

EDSO. (2018, October 16). *PRESS RELEASE: EDSO and ENCS host Smart Grid Cyber Security event.* Retrieved from https://www.edsoforsmartgrids.eu/press-release-edso-and-encs-host-smart-grid-cyber-security-event/

Elran , M., & Siboni , G. (2015, July 8). *Establishing an IDF Cyber Command.* Retrieved from INSS Insight No. 719,: https://www.files.ethz.ch/isn/192725/No.%20719%20-%20Meir%20and%20Gabi%20for%20web.pdf

EU-Lex. (n.d). *Division of competences within the European Union .* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aai0020

European Commission. (2013 , February 7). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace .* Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2013, February 7). *Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace.* Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2017). *Cybersecurity Factsheet.* Retrieved from State of Union 2017: https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

European Commission. (2017, December 11). *Energy Expert Cyber Security Platform (EECSP) - Expert Group (E03341).* Retrieved from http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3341

European Commission. (2017, September 13). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=en

European Commission. (2018, October 11). Retrieved from Cybesecurity in the energy sector: https://ec.europa.eu/info/events/cybersecurity-energy-sector-2018-oct-11_en

European Commission Directorate-General for Energy. (n.d). *Energy Expert Cyber Security Platform (EECSP) Terms of Reference (EECSP) & Call for Experts (EESCP-Expert Group).* Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf

European Commission. (n.d). *Protection of critical infrastructure.* Retrieved from https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

European Commission-Directorate General for Energy. (n.d). *Energy Expert Cyber Security Platform (EECSP) Terms of Reference (EECSP) & Call for Experts (EESCP-Expert Group).* Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf

European Energy - Information Sharing & Analysis C. (2019). *ISAC?* Retrieved from http://www.ee-isac.eu/home

European Parliament Directorate-General for Internal Policies. (2016 , October). *Cyber Security Strategy for the Energy Sector* . Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf

EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT (TE-SAT) 2016. (2017, Ιανουάριος 10). Retrieved from European Police Office (Europol): https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016

FireEye. (2016). *Cyber Threats to the Energy Industry* . Retrieved from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-energy.pdf

Garner Jr. , M. (2017 , December). Retrieved from NATION STATE THREAT ACTIONS AGAINST CRITICAL ENERGY INFRASTRUCTURES : https://search.proquest.com/openview/154afe40506d09a0e58bf5e013f13fd6/1?pq-origsite=gscholar&cbl=18750&diss=y

Gassen , J., Tiirmaa-Klaar , H., Gerhards-Padilla, E., & Martini , P. (2013). *Botnets.* London : Springer Science & Business Media.

Goutam, R. (2017, February). Importance of Cyber Security. *International Journal of Computer Applications , Volume 111- No 7.* Retrieved from https://pdfs.semanticscholar.org/5cfb/7a5bd2e6c181e8a69ebd49b1dadb795f493b.pdf

Government of Canada. (2017 , Otober 20). *Common threats to be aware of.* Retrieved from https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-en.aspx

Government Publications Office. (2016). *International Energy Outlook 2016: With Projections to 2040.* Washington D.C: Government Printing Office.

Grant, S. (2018 , September 20). *National Security and Defense* . Retrieved from President Trump Unveils America's First Cybersecurity Strategy in 15 Years: https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/

Hamada, J. (2016 , July 25). *Symantec.* Retrieved from Patchwork cyberespionage group expands targets from governments to wide range of industries: https://www.symantec.com/connect/blogs/patchwork-cyberespionage-group-expands-targets-governments-wide-range-industries

Housen-Couriel, D. (2017, March). *National Cyber Security Organisation: Israel.* Retrieved from NATO Cooperative Cyber Defence Centre of Excellence: https://ccdcoe.org/sites/default/files/multimedia/pdf/IL_NCSO_final.pdf

IBM I Sales and Distribution. (2012, August). *Best practices for cyber security in the electric power sector* . Retrieved from Energy and Utilities: https://www-935.ibm.com/services/multimedia/WR928534SF-Best_practices_for_cyber_security_in_the_electric_power_sector.pdf

IL-CERT. (n.d). *IL-CERT- Israeli CERT* . Retrieved from https://il-cert.org.il

INFOSEC Institute . (n.d). *Phishing Attacks In The Energy Industry.* Retrieved from https://resources.infosecinstitute.com/category/enterprise/phishing/the-phishing-landscape/phishing-attacks-by-demographic/phishing-attacks-in-the-energy-industry/

Intergovernmental Panel on Climate Change. (2015). *Climate Change 2014: Mitigation of Climate Change: Working Group III Contribution to the IPCC Fifth Assessment Report.* New York : Cambridge University Press.

International Communications Union. (n.d). *Global Cybersecurity Index.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

International Energy Agency. (2017, November 5). *Digitilization and Energy.* Retrieved from: https://www.iea.org/digital/

International Energy Agency. (2017). *Digitilization & Energy* . Retrieved from https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf

International Energy Agency. (n.d). Retrieved from Energy security: https://www.iea.org/topics/energysecurity /

International Renewable Energy Agency . (2018). *Global Energy Transformation: A roadmap to 2050.* Ανάκτηση από https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2018/Apr/IRENA_Report_GET_2018.pdf

International Telecommunications Union . (2017). *Global Cybersecurity Index (GCI) 2017.* Retrieved from Global Cybersecurity Index (GCI) 2017: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Israel's Homeland Security. (n.d). *Energy under Hacktivism threat.* Retrieved from https://i-hls.com/archives/63698

Israeli Defense Forces. (n.d). *Code of Ethics and Mission* . Retrieved from https://www.idf.il/en/minisites/code-of-ethics-and-mission/

Joint Research Center . (2018, May 31). *European Reference Network for Critical Infrastructure Protection ERNCIP Handbook 2018 edition.* Retrieved from https://erncip-project.jrc.ec.europa.eu/documents/erncip-handbook-2018-edition

Kaspersy Lab . (2015, February). *The Desert Falcons Targeted Attacks* . Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064309/The-Desert-Falcons-targeted-attacks.pdf

Kazerooni, S. (2015, December 2). *The Growing Threat of Denial-of-Service Attacks.* Retrieved from Electric light & Power: https://www.elp.com/articles/powergrid_international/print/volume-20/issue-2/features/the-growing-threat-of-denial-of-service-attacks.html

Kletzkine, J. (n.d). *Israel: A Global Center for Cyber security.* Retrieved from Start-Up Nation Central: https://www.startupnationcentral.org/wp-content/uploads/2017/09/Start-up-Nation-Central-Cybersecurity-Brief.pdf

KPMG International . (2016, January). *Innovative interconnections Digitalization: energy, quo vadis? Energy & Natural Resources.* Ανάκτηση από https://www.res4med.org/wp-content/uploads/2017/05/innovative-interconnections-digitalization-energy-quo-vadis.pdf

Lee, R., Assante , M., & Conway , T. (2016 , March 18). *Electricity Information Sharing and Analysis Center E-ISAC* . Retrieved from Analysis of the Cyber Attack on the Ukrainian Power Grid: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Loota , S. (n.d). *Intel Security Group* . Retrieved from Emerging Cyber Threats and How to Stay Safe: Ransomware : https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwil6uXRsO_eAhUhgHMKHQHrAEAQFjADegQICBAC&url=https%3A%2F%2Fwww2.gov.bc.ca%2Fassets%2Fgov%2Fbritish-columbians-our-governments%2Fservices-policies-for-government%2Finfor

Lovells, H. (2016 , March). *Cyber security: A growing threat to the energy sector – An Australian perspective.* Retrieved from https://www.hoganlovells.com/en/knowledge/topic-centers/cybersecurity-solutions/~/media/c14b2cc829b04a6e841237f66882b2df.ashx

McGuire , M., & Dowling , S. (2013 , October). *Cyber crime: A review of the evidence* . Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf

Middleton , B. (2017). *A History of Cyber Security Attacks: 1980 to Present.* Boca Raton: CRC Press .

Mikhaylova, G. (2014 , December). *THE "ANONYMOUS" MOVEMENT: HACKTIVISM AS AN EMERGING FORM OF POLITICAL PARTICIPATION.* Retrieved from https://digital.library.txstate.edu/bitstream/handle/10877/5378/MIKHAYLOVA-THESIS-2014.%20pdf?sequence=1

MWR InfoSecurity. (n.d). *Industry review.* Retrieved from https://www.mwrinfosecurity.com/work/industries/energy/

National Infrastructure Commission. (n.d). *The impact of technological change on future infrastructure supply and demand.* Ανάκτηση από National Infrastructure Commission report: https://www.nic.org.uk/wp-content/uploads/2905991-NIC-TECHNICAL-v0_5-ACCESSIBLE.pdf

Nuttall, W., Samaras , C., & Bazilian , M. (2017, November). *Energy and the Military: Convergence of Security, Economic, and Environmental Decision-Making*. Retrieved from Energy Policy Research Group University of Cambridge: https://www.eprg.group.cam.ac.uk/wp-content/uploads/2017/11/1717-Text.pdf

O'Flaherty, K. (2018, May 3). *The Forbes*. Retrieved from Cyber Warfare: The Threat From Nation States: https://www.forbes.com/sites/kateoflahertyuk/2018/05/03/cyber-warfare-the-threat-from-nation-states/#540bdab11c78

Ouwendijk, H. (n.d). *Israel Cybersecurity & homeland security in Israel.* Retrieved from Rijksdienst voor Ondernemend Nederland: https://www.rvo.nl/sites/default/files/2017/06/israel-cyber-homeland-security.pdf

Paganini , P. (2013, June 24). *Security Affairs* . Retrieved from Anonymous and state-sponsored hackers threaten energy sector: https://securityaffairs.co/wordpress/15517/hacking/anonymous-and-state-sponsored-hackers-threaten-energy-sector.html

Pagliery , J. (2015 , August 15). *The inside story of the biggest hack in history.* Retrieved from https://money.cnn.com/2015/08/05/technology/aramco-hack/index.html

Press, G. (2017, July 18). *6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry.* Retrieved from The Forbes : https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#3bd7483d420a

PwC. (2013 , February). *Embedding cyber security into the energy system* . Retrieved from https://www.pwc.com/gx/en/oil-gas-energy/publications/assets/pwc-embedding-cyber-security-into-the-energy-ecosystem-pdf.pdf

Rapid 7 . (n.d). *Common Types of Cybersecurity Attacks.* Retrieved from https://www.rapid7.com/fundamentals/types-of-attacks/

Raska, M. (2015, January). *Confronting cybersecurity challenges: Israel's evolving cyberdefense strategy.* Retrieved from S. Rajaratnam School of

International Studies, Policy Report: http://www.michaelraska.de/download/Israel%27s_Evolving%20Cyber%20Strategy_Raska.pdf

Schreier, F. (2017). *On Cyberwarfare.* Retrieved from DCAF HORIZON Working Paper No. 7: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf

Scott, J., & Spaniel , D. (2016 , August 24). *The Energy Sector Hacker Report.* Retrieved from Institute for Critical Infrastructure Technology : https://icitech.org/wp-content/uploads/2016/08/ICIT-Brief-The-Energy-Sector-Hacker-Report.pdf

Sentryo . (2016, November 16). *The Lansing Board of Water & Light falls victim to a ransomware attack.* Retrieved from https://www.sentryo.net/lansing-board-of-water-light-victim-ransomware-attack/

Shi , J., & Saleem , S. (n.d). *Phishing.* Retrieved from https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5-final/report.pdf

Sigholm, J. (2016 , November 23). *Non-State Actors in Cyberspace Operations.* Retrieved from https://doi.org/10.1515/jms-2016-0184

Staff, T. (2016, January 26). *Steinitz: Israel's Electric Authority hit by 'severe' cyber-attack.* Retrieved from Times of Israel: https://www.timesofisrael.com/steinitz-israels-electric-authority-hit-by-severe-cyber-attack/

The Government Secretary. (2015, February 15). *Government Resolution No. 2443 of February 15, 2015* . Retrieved from https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202443%20-%20Advancing%20National%20Regulation%20and%20Governmental%20Leadership%20in%20Cyber%20Security.pdf

The White House. (2018, September). *National Cyber Strategy of the United States of America.* Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

U.S Department of Energy . (2018). *Cyber Security Strategy 2018-2020* . Retrieved from https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-

003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf

U.S Department of State. (n.d). *U.S Department of State.* Retrieved Απρίλιος 30, 2017, from Treaty Between The United States Of America And The Union Of Soviet Socialist Republics On The Elimination Of Their Intermediate-Range And Shorter-Range Missiles (INF Treaty): https://www.state.gov/t/avc/trty/102360.htm

U.S. Energy Information Administration. (218, May 3). *FREQUENTLY ASKED QUESTIONS: How much energy is consumed in U.S. residential and commercial buildings?* Retrieved from https://www.eia.gov/tools/faqs/faq.php?id=86&t=1

World Energy Council. (2013). *World Energy Resources, 2013 Survey* . Retrieved from https://www.worldenergy.org/wp-content/uploads/2013/09/Complete_WER_2013_Survey.pdf

World Energy Council. (2018). *New cyber resilience report : energy sector prime target for cyber-attacks*. Retrieved from https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyber-attacks/