YEARBOOK OF UNWE (2021), PUBLISHING HOUSE – UNWE
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2021.2.10

CYBERSECURITY IN THE TRANSPORTATION OF ENERGY RESOURCES

Nadya Parpulova[1], Vladimir Zinoviev[2]
e-mail: Nadya.Parpulova@unwe.bg, e-mail: vzinoviev@unwe.bg

Abstract

Technical constraints in the field of transport of energy resources following the digitization are particularly relevant in the case of critical infrastructure and Industry 4.0. Since all industrial facilities, of the sector like petrochemical pipelines, expensive to build and designed without any particular form of protection against cyber-attacks, followed a plug-in approach: new technologies have been added on top of existing layers to ensure compatibility and as such became exposed to cyber-attacks. Cyberattacks on energy plants and transportation means could become the most serious threat to any country's national security, to the impact on the population and the physical destruction of structures, usually in an extremely wide area.

The paper justifies and sums up some steps that both governments and industry should follow and plan for: a) creating instruments and structures in place for conducting strategic intelligence prior to attacks on the network b) invest in designing programs that will raise the awareness of the potential threats and will map out the weak points c) boost collaboration and industry partnerships to address the increasing convergence of physical and virtual threats.

Key words: transport, energy resources, cyber-security, IoT, intelligent pipelines, cyber-attacks

JEL: O14, F63

Introduction

The paper looks at the issue of cybersecurity in the transportation of energy resources. The paper outlines both conventional and modern means of transport, explores the extent to which these means have "plugged-in" to new technologies to ensure compatibility with the 4.0 industry achievements in the sector.

The paper investigates how this situation has led to the simultaneous co-existence of modern IoT /Internet of Things/ devices and legacy devices. The fact is that legacy devices are deployed when industrial facilities were still considered

[1] PhD student, Faculty of Economy of Transport and Energy, University of National and World Economy

[2] Assoc. Prof., PhD, Faculty of Economy of Transport and Energy, University of National and World Economy

"closed environments" that were difficult to access remotely and were therefore designed without any particular form of protection against cyber-attacks. "Opening up" these infrastructures to the outside world to take advantage of the potential of the IoT therefore exposes potentially vulnerable legacy systems to cyber-attacks.

Finally, the conclusions made call for quick and coordinated actions to provide and secure the transportation of energy resources as a matter of national and international security.

Transport and means of transport

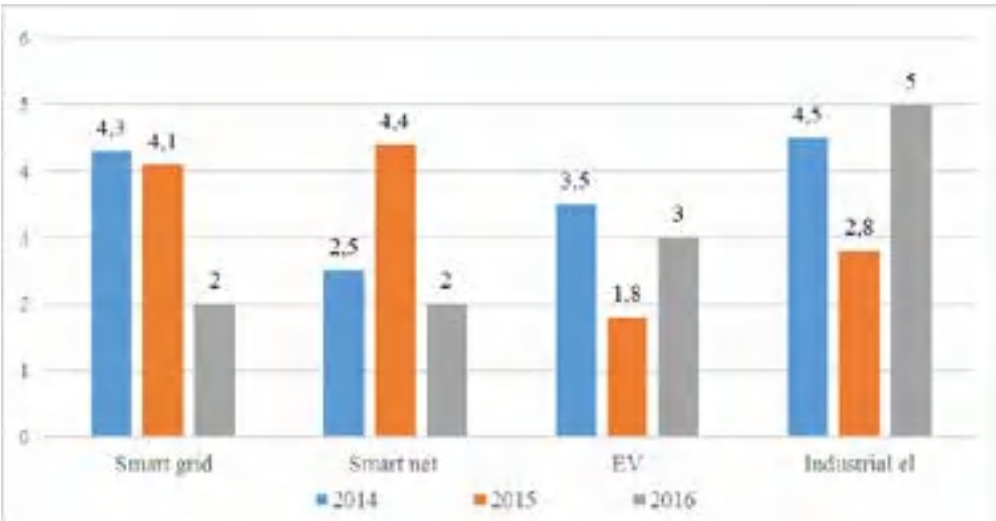
Transport plays an important role in today's economy and has a large impact on growth and employment. The transport industry directly employs around 10 million people on the European continent only and accounts for about 5% of the gross domestic product (GDP) on the same territory.

Effective transport systems are fundamental for the overall companies' ability to compete in the world economy. Logistics, such as transport and storage, account for 10-15% of the cost of a finished product for the companies, which by itself is an add on factor for researching all potential instruments provided by the new technologies for optimizing the results from the sector and thus increasing the domino effect transport has on economy.

In the past few decades, a fourth industrial revolution has emerged, known as Industry 4.0. Industry 4.0 takes the emphasis on digital technology from recent decades to a whole new level with the help of interconnectivity through the Internet of Things (IoT), access to real-time data, and the introduction of cyber-physical systems (Joshi, 2001), Industry 4.0 offers a more comprehensive, interlinked, and holistic approach to all types of manufacturing.

Speaking of manufacturing transport does not manufacture a product as such. Its product is the service of the movement of people and goods. This is a tangible and measurable result therefore it is a kind of manufacturing and inevitably falls under the broad spectrum of influence of the Industry 4.0.

The transport sector is a very specific sector, it is part of the industrial sector as such and yet there are many features that literally make this sector as important as the blood system in the human body – without it, there is no life. The transport sector holds large quantities of critical information at any time as it depends on strict logistics and coordination. Both logistics and coordination are focused on the protection of devices and networks forming the smart grids, critical infrastructures, Industry 4.0 and services involved, primarily the field of transport of energy resources.



Source: Adapted from the Interstate Natural Gas Association of America ("INGAA")

Figure 1: Investments in IT solutions in the energy sector in the US

The energy sector on the other hand is under vastly growing expectations to secure the wellbeing of humankind. The global energy sector faces a triple challenge in the next 20-30 years:

1. The sector needs to be fundamentally transformed into a low carbon energy supply system in response to climate change mitigation and related policies (e.g. the Paris Agreement under the United Nations Framework Convention on Climate Change), where it needs to rely on the new technologies and industry 4.0 developments.

2. While it needs to adapt to climate change and its effects it also needs to ensure that energy supplies remain secure and reliable. If the energy supplies are interrupted or made scarce this immediately affects the economy and every-day life.

3. Achieving all of the above draws the third pillar of effort – how to cyber-secure all this and prevent it from being misused being it economically or politically.

How do we transport energy resources generally?

Every-day life sectors as well as the heavy industry are using energy recourse extensively:

a) Natural gas, as compressed natural gas and liquefied natural gas, is used in cars, buses, trucks, and ships. Most natural gas-powered vehicles are in

government and private fleets. Natural gas is also used to run compressors to transport natural gas in pipelines.

b) Propane (a liquid hydrocarbon gas) is used in cars, buses, and trucks. Most vehicles that use propane are in government and private fleets.

c) Crude oils are used in many industrial sites.

Crude oil is transported from source to refinery by barges, tankers, overland, pipelines, trucks, and rail. Natural gas is transported by pipelines and liquefied natural gas tankers (Huber, 2001).

Transporting uranium, nuclear fuel and radioactive waste always carries risks. The conventional means of transport are being more and more affected by climate change. For instance: ports and docks depend on the sea level and aim to avoid or at least reduce damage caused by flooding. Sustained periods of extreme heat can lead to deformities in rail tracks and eventually derailment, softening of road surfaces in general, and rutting and bleeding of asphalt surfaces (Library of Congress Online Catalog, 2005).

New technologies are the only hope to achieve the sustainability in supplies

Transport is in the top three sectors regarded as a factor for economic growth. The performance of the transport sector is consequently linked to innovations and the 4.0 Industry. Looking into some of the above mentioned effects of Industry 4.0 on transport it seems that the sector is not only highly influenced by innovations, but it is one of the most susceptible to the implementation of all instruments the 4.0 industry has to offer.

Transportation companies (be they private or public companies) have a large digital presence these days, whether publicly via the Internet or internally via computer systems to manage internal data and processes. Not being able to effectively protect themselves from the new threats exposes today's businesses to loss of confidential information and negatively impacts their performance. This is where cybersecurity becomes a top priority, especially when it comes to transporting energy resources.

Cybersecurity, by definition, encompasses a group of physical, logical, and administrative measures aimed at protecting organizations, people, and systems (devices, applications, or data) from digital attacks that could compromise confidentiality, availability, or integrity.

Cyber-physical systems equipped with Internet technology require reliable concepts and technologies to ensure security, privacy and protection of knowledge and data. Therefore, reliable and secure communication and sophisticated identity and access management for machines are essential.

Different layers of protection at different levels as well as prevention and resilience are defined and implemented on these assets. Thus, different measures can be combined to effectively prevent and mitigate attacks.

Cybercrime is a growing problem:

- In 2016, a company was the victim of a cyberattack every 40 seconds worldwide. Cyberattacks are expected to become even more common by 2021: Every 11 seconds, a business will be the victim of a cyberattack.
- Global cybersecurity spending is expected to grow at an annual rate of 12% to 15% between 2017 and 2021.
- Cybersecurity Ventures estimates that cybercrime will cost the world $6 billion per year by 2021, equivalent to 1% of the global GDP. Moreover, this is twice as much as in 2015.
- 39% of companies already have cybersecurity training and sensitization programs for their employees. The foreseen world expenditure in information security products and services was worth 124 billion dollars by 2019, 8.7% higher than the 114 billion dollars invested in 2018. Sales of cloud security applications and platforms were expected to rise at a compound annual growth rate (CAGR) of 35.3% between 2017 and 2019 and become a 459-million-dollar market this year.

Security services were forecast to generate a market of 64.2 million dollars in 2019, exceeding the 52.3 million dollars of 2017.

Putting the focus back on the energy sector makes us look at the continuous growth in energy demand. The world population is projected to reach more than 9 billion by 2050 according to the United Nations' World Population Prospects. Population growth, together with urbanization in developing countries and industrialization, will continue to drive the growth of global energy demand and consumption (Paolini, 2011). A broader perspective of it includes a number of activities involved in the supply chain: exploration, extraction, production, transportation, transmission, distribution and consumption, that is to say selling to the final consumer. It is also possible to include offshore activities, as a significant portion of oil and gas production takes place offshore; highly specialized equipment and services are developed for the location, prospection, extraction, production and transportation of energy resources.

When it comes to petroleum trade, pipelines remain the most popular and efficient method of transporting crude oil. Even though pipelines are not financially viable to build, they are an obvious and economical means of transporting large amounts of natural gas in the long term; not to mention that they are considered safe and reliable. Although efficiency is not lost in the pipeline business, there is still room for improvement.

Gathering systems such as the pipelines can be:

- Transportation pipelines
- Distribution pipelines (mostly used to transport natural gas to medium or small consumption units).

Pipelines play a very critical role in the transportation process of energy resources such as (crude oils, gas etc.) There is a process of separation of the crude oils from the natural gas after which the pipelines transport the oil to another carrier or directly to a refinery. Tanker truck, truck, rail tank car, or pipeline are used further to transport the crude oil to the market.

The demand for natural gas constantly increases which inevitably challenges the transportation side and the need for more new pipelines. There are approximately 300,000 miles of natural gas transmission pipelines in the United States. Strategic planning includes determining the shortest and most economical routes on which pipelines should be built, the number of pump stations and natural gas compression stations along the route, and final storage so that oil can be transported from almost any field to any refinery as needed.

As the network of pipelines increases the risks of leakages and environmental and other damages is higher. New technologies come on board to help build more advanced pipelines with adequate and monitoring systems and safety and efficiency parameters installed.

The most important aspect of facilitating the transportation of various types of petroleum products through pipelines is infrastructure, which is not limited to the pipelines themselves. It includes the facilities used for transportation such as compression and metering stations, storage services, and natural gas processing facilities. The development and improvement of current downstream infrastructure is aimed at maintaining the smooth transportation of natural gas from production areas to consumers and meeting public demand.

Pipelines are an efficient and safe means of transporting materials – many of which are flammable or toxic. To increase efficiency and reliability and to reduce costs, pipeline owners and operators leverage information technology (IT) and operational technology (OT) extensively in their day-to-day operations. In today's evolving threat environment, the inherent vulnerabilities in these IT and OT systems can present high-consequence opportunities for foreign adversaries, hackers, and other malicious actors to exploit.

Millions of miles of pipelines responsible for transporting oil, natural gas, and other energy resources are an important factor in any national and economic security. With the advancement of 4.0 industry instruments such as (ICT / information and communication technology/, OT /operations technology/ and IT) to drive automation, the operators of the pipelines should also implement security measures to protect pipelines from evolving and emerging cyber risks. The

integration of ICT devices into critical pipeline systems creates vulnerabilities that ill-intentioned cyber actors can exploit.

Pipeline cybersecurity risks

Pipeline infrastructure is critical to national security. It is the main means of transport for the energy sector that affects all sectors of the economic life. Pipeline operations depend on and affect many other critical infrastructure sectors such as: water and wastewater systems, chemical systems, and transportation systems.

In addition, they are among the 55 National Critical Functions (NCFs):

- disruption of pipeline operations,
- corruption, or dysfunction would have a debilitating effect on security,
- national economic security,
- national public health or safety.

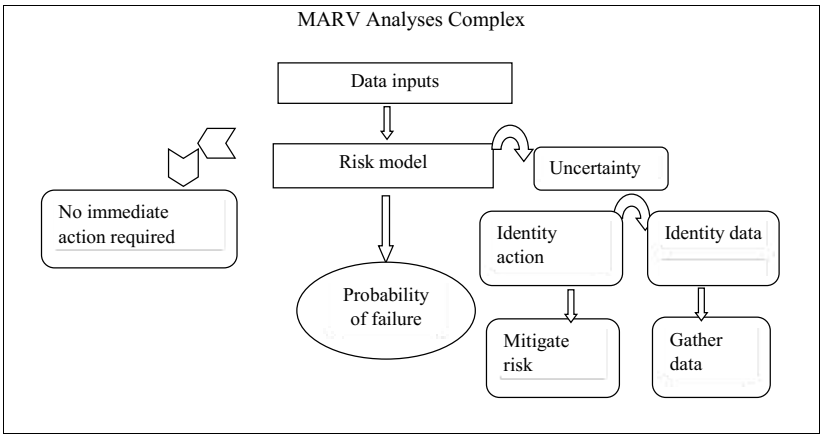
A cyberattack on a pipeline system could result in explosions and leaks, sabotage, equipment malfunctions and unanticipated shutdowns, intellectual property theft, and supply chain disruptions to midstream and downstream operations of other NCFs. The consequences of an attack could affect supplies of fuel, natural gas, and certain chemicals; cause power shortages; harm the environment; and hinder production in all sectors (CISA, 2020).

Improving pipeline cybersecurity

Cybersecurity assessments are vital to enable the operators to understand better the cybersecurity environment of pipelines OT and IT. The assessments, being a more in-depth reviews provide technical experts the opportunity to review network architecture design, system configuration and protocols, and network traffic and make recommendations on how owners and operators can improve their cybersecurity. The understanding of the overall risk is critical for the future functioning of the systems (DHS, US 2021).

There are many private companies and researchers marking a good progress on pipelines' cyber security like MARV analyses complex.

Below is assembled a logical framework of action on cybersecurity risks adapted from the MARV analysis complex.



Source: Adapted from the MARV analysis complex: a tool for multi analysis of variants

Figure 2: Logical framework of action on cybersecurity risks adapted from the MARV analysis complex

Preliminary tasks following from the MARV analysis:

- Analyze pipeline infrastructure to identify vulnerabilities;
- Engineer solutions to reduce the likelihood of a potential damaging cyber-attack;
- Prepare a roadmap for improving pipeline cyber resilience.

Building long-term resiliency

Protecting the nation's pipeline network depends on a unified effort of the private industry through coordination councils assembling: pipeline owners, operators, and other key stakeholders – to share timely information and ensure actionable mitigation strategies are put in place. Such collaboration builds a national culture of pipeline safety and resilience and strengthens economic and national prosperity.

As the world searches for clean and efficient alternative energy sources to reduce greenhouse gas emissions and combat global warming, the shift to using natural gas has come into focus around the world. Not surprisingly, as the demand for natural gas increases, so does the demand for safe and affordable transportation and storage options.

According to a recent study by the global strategy consulting firm Mckinsey (Eiden, Goraieb, Nobels, and Wallance, 2021), global gas demand is expected to grow by 0.9% per year between 2018 and 2035. Since liquefied natural gas (LNG) is considered the best method for transporting and storing natural gas as it is cooled to -260°F, global LNG demand is expected to grow by 3.6% per

year between 2018 and 2035, the study added. The study, titled "The Growing Importance of LNG Market" points out that the role of gas pipelines has declined in recent decades, from 73% of total volumes transported in 2000 to 65% in 2020**.**

LNG pipelines are used to transport natural gas from liquefaction facilities to storage facilities, from storage facilities to tankers, and from tankers to regasification facilities. The biggest challenge with LNG pipelines, besides the high cost, is the difficulty in construction. This is because LNG requires certain temperatures to keep its contents in a liquid state. To maintain this temperature level and prevent re-vaporization, pipelines must be insulated with a combination of mechanical insulation.

This complex insulation system for building LNG pipelines is more expensive and difficult than that of standard pipelines. Transporting LNG via ships or carriers is always the way to go for exporting natural gas on an intercontinental scale as they can carry large volumes of natural gas. LNG carriers are among the strongest, safest and most technologically advanced ships in the world. They are equipped with sophisticated monitoring and control systems. LNG shipping is an economical and efficient method as long as the freighters are larger (Wallance, 2021).

Some regulations and codes have been established by international organizations to organize the transportation process, especially by ship. In addition, certain standards have been established for seating, design, construction, equipment, and fire safety requirements for facilities and terminals.

According to the BP report (British Petroleum, 2020), Egypt exported 4.5 billion cubic meters (bcm) of LNG in 2019, up 2.6 bcm from 2018 (EOG-Newspaper, 2020). Accordingly, interest in the safe storage and transportation of LNG is growing. An LNG expert, who preferred anonymity, stated that improving LNG transportation means, such as increasing the number of trains and using the latest technology applications, will increase the quality of the overall LNG process in Egypt and the Middle East. Technical constraints may be the consequence of the digitization of previously isolated systems.

This is particularly relevant for critical infrastructure and Industry 4.0.

Since industrial facilities, especially large ones such as petrochemical plants or power plants, are expensive to build and maintain, their development typically follows an incremental, plug-in approach: new technologies have been added on top of existing layers to ensure backward compatibility with equipment that could not be changed.

They are outfitted with sophisticated gas and fire detection and suppression systems.

Another article written by David Pendleton (Pendleton, 2020), suggests that the majority of the world's LNG cargo fleet and terminals are equipped with SSL

technology /*stands for: Secure Sockets Layer*/. SSL is a secure protocol developed for sending information securely over the Internet /a system for communicating emergency shutdown (ESD) signals/ (Electrostatic discharge (ESD) is the sudden release of electricity from one charged object to another when the two objects come into contact).

The LNG Expert stressed on the importance of conducting safety sessions for the employees, pointing out that monitoring practices can prevent any incidents before happening.

Smart infrastructure goes along with:

- Centralized control;
- Monitoring of pipelines and its component;
- Control of bridges and tunnels for loads and wear and tear;
- Intelligent pipeline: It is characterized by comprehensive and unified data, perceptual interaction and visualization, system integration and interconnection, precise matching of supply and demand, intelligent and efficient operation, and predictive analytics for early warnings.

Access to energy resources equals economic and social development. Lack of access deprives society from normal living. Over 1.2 billion people in the world still do not have access to affordable modern energy, losing the opportunity for equal development. Helping this group of people have equal access to energy is an important part of achieving the Sustainable Development Goals (SDGs) of the United Nations.

As described above the energy and transportation sectors pushed by the realities have been actively adopting 4.0 industry achievements. Instruments like the Dream Cloud platform covering exploration and development, collaborative research, operation management, logistics, transportation and other businesses like:

- Intelligent refinery: Its operational management control and analysis decision-making capabilities were consistently improved.
- Intelligent pipeline: It is characterized by comprehensive and unified data, perceptual interaction and visualization, system integration and interconnection, precise matching of supply and demand, intelligent and efficient operation, and predictive analytics for early warnings.

Egypt is a case in point. Egypt has become one of the leading producers of natural gas. According to the BP report, Egypt exported 4.5 billion cubic meters (bcm) of LNG in 2019, up 2.6 bcm from 2018. Accordingly, interest in the safe storage and transportation of LNG is growing (Shearer, Tusiani, 2016).

An LNG expert, who preferred anonymity, stated that improving LNG transportation means, such as increasing the number of trains and using the latest technology applications, will increase the quality of the overall LNG process in Egypt and the Middle East.

Technical constraints may be the consequence of the digitization of previously isolated systems. This is particularly relevant in the case of critical infrastructure and Industry 4.0. Since industrial facilities, especially large ones such as petrochemical plants or power plants, are expensive to build and maintain, their development typically follows an incremental, plug-in approach: new technologies have been added on top of existing layers to ensure backward compatibility with equipment that could not be changed.

The piling up of layer on layer has led to the co-existence of modern IoT /Internet of Things/ devices and legacy devices. Certainly the industrial facilities were considered "closed environments" and difficult to access remotely when the legacy devices were deployed. They were designed without any particular form of protection against cyber-attacks. "Opening up" these infrastructures to the outside world to harness the potential of the IoT therefore exposes potentially vulnerable legacy systems to cyber-attacks.

New technologies mean unforeseen vulnerabilities. Understanding the potential security vulnerabilities that new technologies bring is a challenge in itself. It is difficult to detect from the outset where the technical vulnerabilities might exist. In addition, tracking an event and its cause, such as an attack on a system and its exploited vulnerability, may be a much more difficult task if the new technology inherently introduces more complex systems (Annoni et al., 2018; Brundage et al., 2018; Svenmarck et al., 2018).

The most common driver for malicious activity in the cyber world is money

Since no ICT system can be regarded to be completely secure, the question that should be asked regarding security is not whether a system could be compromised, but rather "when, how, and with what consequences". As for "when", it is of course impossible to give an answer a priori without relying on new technologies.

The range of impact of attacks driven by ideologies or (political) agendas rather than money is wide. It ranges from targeted cyber espionage activities threatening corporate intellectual property, to cyber-attacks on critical energy infrastructure with potentially dramatic effects on the physical world, the economy, or even the use of cyber capabilities in a military conflict to support regular warfare. One such example of a cyberattack is the attack on Ukraine's electricity infrastructure that resulted in the temporary disruption of power to over 225,000 consumers in December 2015 (Styczynski, Beach-Westmoreland and Stables, 2016).

Ukraine was affected by a series of attacks aimed at rendering some essential services unusable for a certain period of time. This new type of attack makes it difficult to detect and attribute attacks, so there is no longer a way to quickly

build a defense against the original threat actor. Increasing the attack surface provides threat actors with the opportunity to increase the variety of targets and threat tools.

One such trend is shown in Table 1, based on findings from ENISA's annually published Threat Landscape Report (ENISA, 2019c; 2012; 2013; 2015; 2016b; 2017).

Table 1: Top 15 cybersecurity breaches according to ENISA Threat Landscape Reports

TOP 15 THREATS			
Ransomware	Cyberespionage	Crypto jacking	
Malware	Web-based attacks	Phishing	Web application attacks
Spam	Denial of service	Identity theft	Data breach
Insider threat	Botnet	Physical manipulation, damage, theft and loss	Information leakage

Source: Adapted from European Agency for Cybersecurity (2021).

Ethical challenges

There are of course ethical challenges when cybersecurity risk management is involved. Extensive monitoring and pervasive risk-prevention with the help of AI can be highly intrusive and coercive for people, whether employees or citizens. AI can also be so powerful that people feel that their sense of being in control is taken away.

They may get a false sense of security too. Deep-learning AI is, as of today, not transparent in how it reaches a decision from so many data points, yet an operator may blindly trust that decision.

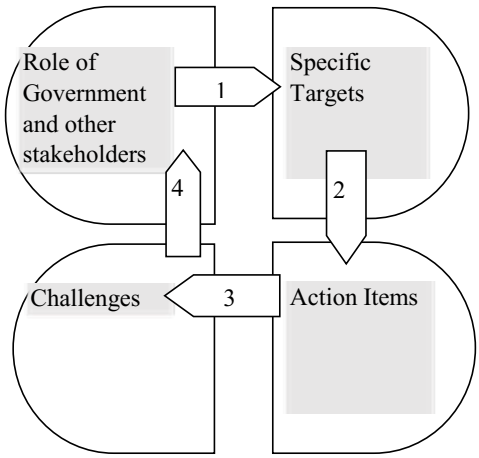
Provision of cybersecurity tools in the transportation of energy resources

The common reason behind the cyber-attacks on the means of transportation and distribution of energy resources is their strategic reach, potentially weakening national security.

As far as market structure and key players are concerned, cybersecurity markets vary from monopolistic to competitive and fragmented structures. In China, the cybersecurity market is dominated by large monopolies with links to the national security apparatus. In Japan the role of the Ministry of Economy, Trade, and Industry (METI), as well as a long-established practice of top-down policymaking have also contributed to the slow speed of growth in the cybersecurity sector. In the United States there is a plethora of companies marketing their cybersecurity programs.

In Europe markets are fragmented between a few large players and several small firms. Such structures are to a large extent shaped by the fact that national governments intervene on the basis of national security concerns. In this respect, in European countries, cybersecurity suppliers developed through a close relationship to military and government buyers. The downside is a degree of national institutional dependency (ACCIO Strategic and Competitive Inteligence Unit, 2019).

Investments in Digital Energy Solutions



Source: Authors' own idea

Figure 3: Key items and inter-cooperation cycle for successful digitalization strategies in the transport and energy sector

In conclusion

Cyberattacks on energy plants and transportation means could become the most serious threat to any country for the impact on the population and the physical destruction of structures in an extremely wide area. Cybersecurity in these sectors is a matter of national security and therefore it demands common efforts both from the governments and the industry.

There are different measures that could be used to tackle the challenges, some of them though appear to be key:

- **Creating instruments** and structures in place for conducting strategic intelligence prior to attacks on the network. National and international organizations must implement a forward-thinking approach to cybersecurity, especially when transportation of energy resources is concerned.

The infrastructure investments are so high that leaving the systems vulnerable is the least to say irresponsible. In the last decade, adversaries (both governments' and industry's) and strategic competitors have developed and experimented with a growing capability to shape and alter data and systems which the transport and energy sector rely on. Cyber espionage has been conducted with years now to collect intelligence and keep on target critical infrastructure. Such attempts are becoming more adept at even using social media. As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information, leading to more open access to any business or national channel, including energy plants and transportation systems.

- **The design of programs** that will raise the awareness of the potential threats must be taken forwards. This will help to reduce geographic and operational gaps in communications, since when we speak of the pipeline network it usually crosses different states and jurisdictions. A well-functioning utility security apparatus should be aligned to ensure a robust process in place to report potential vulnerabilities and emerging incidents. Experts are united that countries that share common energy and transport infrastructure should actively discuss cyber resilience strategies. As digital transformation and hyper-convergence create unintended gateways to risks, vulnerabilities, attacks, and failures – cyber resiliency strategy helps reduce risks, negative financial impacts and reputational damages. It should be recognized as a common effort not as a one player – task.
- **Industry partnerships** and wide collaboration is needed to address the increasing convergence of physical and virtual threats. Since most changes and innovations start within the industry sector, there should be a regular dialog on how to secure the delicate connections between physical and virtual infrastructure, as well as IT and operational technology (OT) networks. Industry invests a lot in artificial intelligence (AI): from self-driving cars and drones to virtual assistants and software that translate or invest. Impressive progress has been made in AI in recent years, driven by exponential increases in computing power and by the availability of vast amounts of data, from software used to discover new algorithms used to predict anything from economic expectations to our cultural interests. Minding what is at stake with a vulnerable energy and transport infrastructure new policy lines should create the right environment and motivations to boost industry partnerships. This is critical in terms of cybersecurity in the energy and transport sectors.

4.0 Industry is the way forward – better and more efficient use of resources that are already quite scarce. Being plugged-in though makes the systems far more vulnerable than ever.

Targeted cybersecurity technologies and specifically tailored policies are a must in order to utilize all the benefits of new achievements.

References

ACCIO Strategic and Competitive Intelligence Unit, Barcelona. (2019). Cybersecurity in Catalonia, Technological report of the Security Center of Catalonia [online], available at: http://catalonia.com/.content/documents/2019/cybersecurity-in-catalonia.pdf

Annoni et al., (2018); Brundage et al., (2018); Svenmarck et al., (2018), The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, published by Cornell University.

British Petroleum. (2020). Statistical Review of World Energy, edition 69, available at: https://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html

Cybersecurity and Infrastructure Security Agency (CISA). (2020). National Critical Functions, available at: https://www.cisa.gov/national-critical-functions

DHS, US Department of Homeland Security's Transportation Security Administration (TSA). (2021). Pipeline cybersecurity, available at: https://www.cisa.gov/pipeline-cybersecurity-initiative

Eiden, K., Goraieb, E., Nobels, K., Wallance, D. (2021). The Latin American energy sector: How to address cybersecurity, available at: https://www.mckinsey.com/business-functions/risk/our-insights/the-latin-american-energy-sector-how-to-address-cybersecurity

Energy Information Administration (EIA). (2020). Energy use for transportation – data, available at: https://www.eia.gov/energyexplained/use-of-energy/transportation.php

EOG Newspaper (2020). Successful mix of growth and stability, Issue December, available at https://egyptoil-gas.com/wp-content/uploads/2020/12/EOG-Newspaper-December-2020-Issue-.pdf

European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape report – 2020, available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

Huber, M. (2001). Tanker Operations, a Handbook for the Person-in-Charge (PIC), 4th edition, Centreville, MD: Cornell Maritime Press, 23.

Interstate Natural Gas Association of America ("INGAA"). (2020). Statistics, available at: https://www.ingaa.org/

Joshi, N. (2001). Industry 4.0 – Shaping the future of AEC industry, available at: www.linkedin.com›pulse›industry-40-shaping-future-aec-nilay-joshi

Library of Congress Online Catalog. (2005). Modes of transportation in Oil and Gas Industry: A Research Guide, available at: https://guides.loc.gov/oil-and-gas-industry/midstream/modes

MARV analysis complex (2017). Tool for multi analysis of variants, originally a tool for genome-wide multi-phenotype analysis of rare variants, available at: https://bmcbioinformatics.biomedcentral.com/articles/10.1186/s12859-017-1530-2

Paolini, S. (2011). Increase mobility and reduce Emissions – Transport 2050, iss

Pendleton, D. (2020). LNG bunkering: ESD systems vital for safety and visibility, available at: https://www.rivieramm.com/news-content-hub/news-content-hub/lng-bunkering-esd-systems-vital-for-safety-and-visibility-61825

Shearer, G., Tusiani, M. D. (2016). LNG: Fuel for a Changing World, A Nontechnical Guide, 2nd edition, published by Pennwell Books.

Styczynski, Beach-Westmoreland and Stables. (2016). Undestanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to do about it, available at: https://core.ac.uk/download/pdf/189476459.pdf