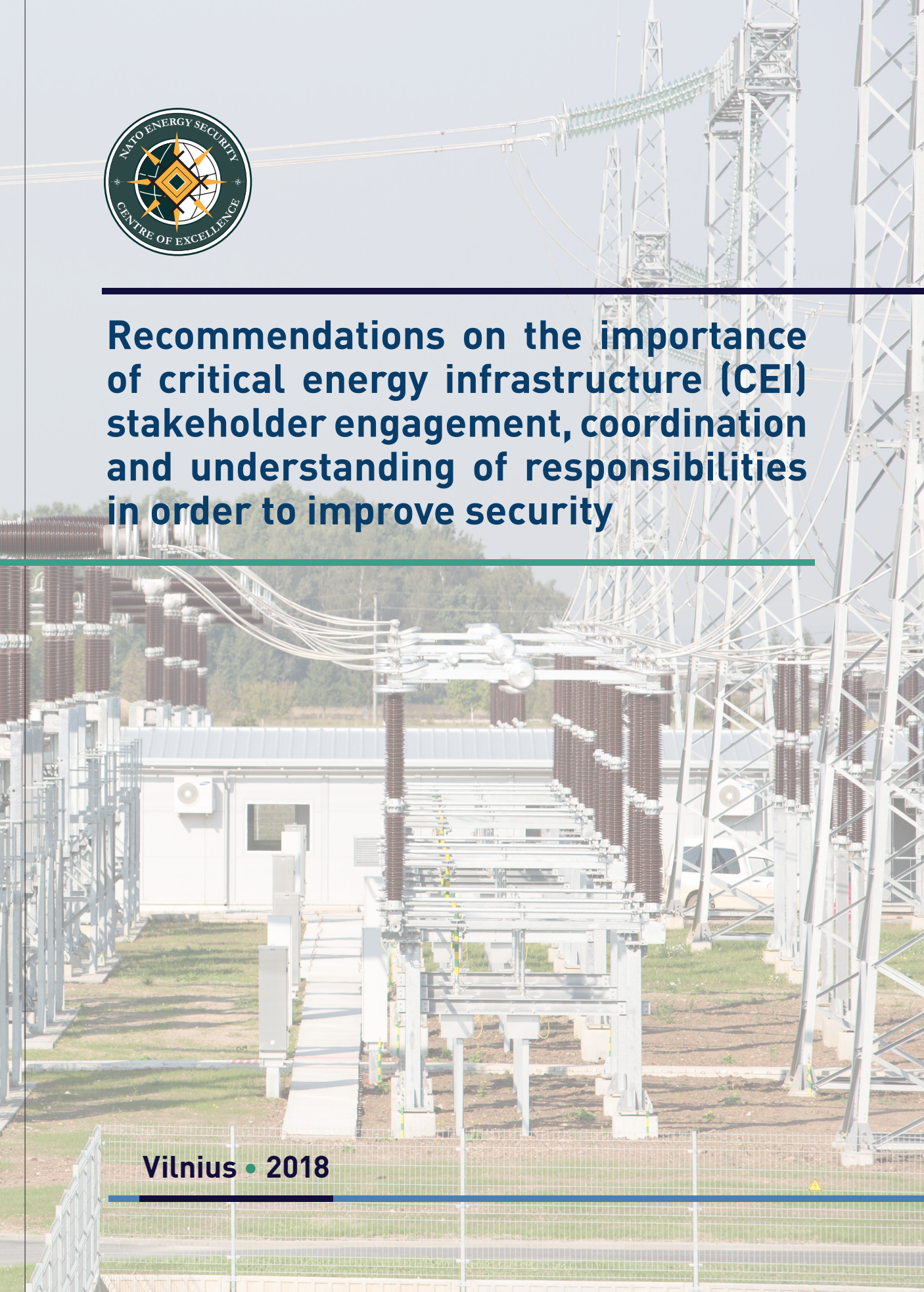

Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security

Vilnius • 2018

Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security

Dr Tiziana Melchiorre
Fellow
NATO Energy Security Centre of Excellence, Vilnius

Special appreciation for professional contribution to:
Amber Grid AB
Elering
Ente Nazionale Idrocarburi (ENI)
Ministry of Economics of Latvia
Snam SpA
Terna

Vilnius • 2018

Contents

List of figures

List of acronyms

AEEGSI	Authority for Electricity Gas and Water
APT	Advanced President Threat
BPCS	Basic Process Control Systems
BEMIP	Baltic Energy Market Interconnection Plan
BMS	Building Management Systems
CCS	Continental Central South
CEIP	Critical Energy Infrastructure Protection
CEF	Connecting Europe Facility
CEL	Central European Line
CEPC	Civil Emergency Planning Committee
CERT	Computer Emergency Response Team
CHP	Combined Heat and Power
CIPI	Critical Infrastructure Protection Information
CIWIN	Critical Infrastructure Warning Information Network
CNAIPIC	National Centre to Protect Critical Infrastructure from IT crimes
CNG	Compressed Natural Gas
CORE 17	Exercise Coherent Resilience 2017
CRC	Crowd and Riot Control
CSE	Continental South East
DCPP	Defense Cyber Protection Partnership
DOTMLPFI	Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability
EU	European Union
ECI	European Critical Infrastructure
ECG	Energy Cooperation Group
ENI	Ente Nazionale Idrocarburi

ENSEC COE	Energy Security Centre of Excellence
ENTSO-E	European Network of Transmission System Operators
EPCIP	European Programme on Critical Infrastructure Protection
GCG	Gas Coordination Group
GIPL	Gas Interconnection Poland-Lithuania
GSE	Gestore dei Sistemi Energetici
HVDC	High Voltage Direct Connection
ICTs	Information and Communication Technologies
IRCSG	Industrial Resources and Communication Services Group
IP	Infrastructure Protection
ICI	Istanbul Cooperation Initiative
ICS	Industrial Control Systems
LNG	Liquefied Natural Gas
MSE	Ministry of the Economic Development
MSU	Multinational Specialized Unit
NATO	North Atlantic Treaty Organization
NEIS	National Energy Independence Strategy
NES	National Energy Strategy
NNP	Nuclear Power Plant
NTN	National Transport Network
RTN	Regional Transport Network
OSCE	Organisation for the Security and Cooperation in Europe
PCIs	Projects of Common Interest
POL	Petroleum Oil and Lubricant
PPPs	Public-Private Partnerships
RTN	Regional Transport Network
SASE	Safe and Security Environment
SCADA	Supervisory Control and Data Acquisition System
SEA	Military Fuel Service
SCPX	South Caucasus Pipeline
SGC	Southern Gas Corridor
SP	Stability Policing
TAL	Trans-Alpine Pipeline
TANAP	Trans-Anatolian Pipeline
TAP	Trans-Adriatic Pipeline
TEN-E	Trans-European Networks for Energy
TTX	Table-Top Exercise
TYNDP	Ten-year Network Development Plan
UGS	Underground Gas Storage
WIT	Weapon Intelligence Team

Introduction

This study, which has been requested to NATO Energy Security Centre of Excellence by Lithuania (the Ministry of Foreign Affairs of Lithuania), aims at providing an analysis of the issues related to Critical Energy Infrastructure Protection (CEIP). The main objective is to give general recommendations to North Atlantic Treaty Organization (NATO) members on how to better coordinate the efforts of public bodies and stakeholders/owners of energy infrastructure (electricity, oil, gas) in order to ensure the protection of critical energy infrastructure. To this aim, this study applies a methodology that can be divided into three main steps. The first step is a theoretical part, which is essentially based on the definition of the concept of critical energy infrastructure and on the necessary measures to protect it. This concept has been deduced by the definitions of critical infrastructure provided by the NATO, the United States (US) and the European Union (EU). The discourse developed in this study is constructed on this concept. The second step is constituted of four case-studies that concretely demonstrate how critical energy infrastructure is protected in different contexts through the coordination of public and private entities. The four case-studies are Estonia, Latvia, Lithuania and Italy. As it is evident, Italy is a completely different case from the others not only for its history and its geographical location, but also for the geopolitical context in which it makes its energy policy and for its territorial size. While including Estonia and Latvia in the study can be considered a natural and logical choice, which stems from the fact that it was requested by the Ministry of Foreign Affairs of Lithuania, the decision to include Italy is essentially due to two elements. First, Italy provides a good example of a big country with a huge energy market, which means that it brings contextual value to the analysis of critical energy infrastructure protection. Second, Italy provides a complex geographical reality as it is located at the centre of the Mediterranean, which means that it is a good example of a state that tries to diversify its energy supplies by importing energy from different geographical areas and by becoming a gas hub in Southern Europe. In order to gather the necessary material to study the three cases, energy companies and ministries

of Estonia, Latvia, Lithuania and Italy have been contacted. A questionnaire has been submitted in order to directly access the necessary information that is often difficult to find on internet and printed material. This has been particularly useful to have a clear idea of how these states try to protect their critical energy infrastructure. In addition to this, energy companies, ministries, organisations and think tanks from other countries have also been approached in order to acquire more knowledge in the field in different contexts. This has been useful especially to formulate recommendations. The third step is an Expert Level Workshop, which was held in the premises of NATO Energy Security Centre of Excellence on the 24th of October 2017 with the aim to create a platform for experts to exchange their knowledge and expertise. This has been an added value to the project because the discussion has focused on the most relevant issues of the topic of this study such as the importance of civilian energy infrastructures to the military defense capabilities, energy security risk assessment programs and cyber security. It was an added value to the project because experts from various countries provided useful and interesting information necessary to its development.

This study is divided into four parts that essentially reflect the methodology described above. The first part discusses the concept of critical energy infrastructure, the measures that are necessary to protect it, the relevance of the Public-Private Partnerships as well as the role of NATO in the field. The second part analyses the four case-studies mentioned above. The third part is a report of the Expert Level Workshop held on the topic in October 2017. Finally, the fourth part focuses on the conclusions stemming from the analysis and on the recommendations to NATO members on how to better coordinate the efforts of public and private entities in order to efficiently protect their critical energy infrastructures.

Finally, another consideration concerns the great contribution given by the energy companies and national authorities of the four case studies taken into consideration in this study as well as of other states that have not been included here but that have given inputs and information that have been very useful for the analysis. It would have been impossible to develop this study without their contribution as well as without the very active participation of high level experts in the workshop and the great interest they have shown in the topic and in the activities of NATO ENSEC COE in the field.

Chapter 1
Critical Energy Infrastructure Protection

INTRODUCTION

This chapter aims at discussing the concept of critical energy infrastructure by trying to provide a clear definition and to highlight its main elements. This is done by first defining the broader concept of critical infrastructure and then by linking it to energy security of which it is a key element. It is shown that the protection of critical energy infrastructure is essential for states because the well-being of their societies depends on its good functioning. An attack on it or a disruption can cause serious problems to the citizens and can jeopardize national security. For this reason, critical energy infrastructure protection is a key issue. In this context, Public-Private Partnerships (PPPs), which are based on the cooperation between the public and the private sectors, are essential. Additionally, critical energy infrastructure protection is also regulated at the EU level through directives although it is a national competence. The sensitiveness of the issue is also demonstrated by the commitment of NATO to support the protection of critical energy infrastructure of the Allies.

These issues are discussed in four sections. The first one analyses the concept of critical infrastructure by linking it to the one of energy. The second section discusses the protection of critical energy infrastructure by describing a method for the risk analysis and by taking into consideration the EU measures aiming at supporting its member states in the field. The EU is a supranational entity whose legislation is transposed into its member states' one (NATO and the OSCE-discussed in the chapter dedicated to the Expert Level Workshop- are international organisations). For this reason it is given much space in this study. The third section discusses the importance of Public-Private Partnerships (PPPs) for an effective protection of critical energy infrastructure. The fourth section focuses on the role of NATO in the protection of critical energy infrastructure showing that the issue has become increasingly relevant over the last decades because it is strictly related to the national security of the Allies.

THE CONCEPT OF CRITICAL ENERGY INFRASTRUCTURE

Although several studies have tried to offer diverse definitions of 'critical infrastructure', a consensual definition does not exist. This study applies the following definition: *critical infrastructure is a system constituted of those facilities, services and information systems that are essential for the maintenance of vital societal functions, health, safety, security, economic and social well-being of people and whose disruption or destruction would have a debilitating impact on national security, national economy, public health, safety and on the effective functions of a government.*

This definition stems from NATO's, the United States' (as it has a substantial and long-term experience in the field) and the EU's ones. According to NATO's definition,"critical infrastructure is those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government" (Jahier, 2014). The US definition stresses the link between the key role played by critical infrastructure and the well-being of citizens as it stipulates that "the nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family" (Department of Homeland Security, 2017). The US identifies 16 critical infrastructure sectors[1] "that compose the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof" (Department of Homeland Security, 2017). The coordinated national effort to manage risks to the nation's critical infrastructure and to enhance the security and resilience of America's physical and cyber infrastructure is led by the National Protection and Programs Directorate's Office of Infrastructure Protection (IP). This office "conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators and State, local, tribal, and territorial partners understand and address risks to critical infrastructure. IP provides information on emerging threats and hazards so that appropriate actions can be taken. The office also offers tools and training to partners to help them manage

[1] **The 16 infrastructure sectors are:1) chemistry; 2) commercial facilities; 3) communications; 4) critical manufacturing; 5) dams; 6) government facilities; 7) defense industrial base; 8) emergency services; 9) energy; 10) financial services; 11) food and agriculture; 12) healthcare and public health; 13) information technology; 14) nuclear reactors, materials and waste; 15) transportation systems; 16) water and wastewater systems. (Department of Homeland Security, 2017)**

the risks to their assets, systems, and networks" (Department of Homeland Security, 2017). Additionally, this office has established strong partnerships across government and the private sector in order to better accomplish its tasks (Department of Homeland Security, 2017).

In the case of the EU's definition, two important documents should be taken into consideration. The first one is the *Green Paper*[2] *on a European Programme for Critical Infrastructure Protection* of 2005, which defines critical infrastructure as including "those physical resources, services, information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of either: a) two or more member states (this would include certain bilateral critical infrastructure, where relevant; b) involve three or more member states (this would exclude all bilateral critical infrastructure)" (European Commission, 2005). The second document is the *Council Directive*[3] *2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection of 2008*.[4] According to this Directive, "critical infrastructure means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Official Journal of the European Union, 2008).The Green Paper, which sets up the bases for the EU Programme on critical infrastructure protection, stresses that this definition of what constitutes an EU critical infrastructure depends on two elements. The first one is the cross-border effect that determines whether an incident can have a serious impact beyond the territory of a member state where the installation is located. The second element is the fact that bilateral cooperation between the member states is a well established and efficient means of dealing with critical infrastructure between the borders of two states. This cooperation would be complementary to the EU Programme on critical infrastructure protection discussed below. On the basis of these two elements, "all those physical resources, services, information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the

[2] "Green Papers are documents published by the European Commission to stimulate discussion on given topics at European level. They invite the relevant parties (bodies or individuals) to participate in a consultation process and debate on the basis of the proposals they put forward. Green Papers may give rise to legislative developments that are then outlined in White Papers", which are "documents containing proposals for European Union (EU) action in a specific area". (Eur-Lex, 2017)

[3] "A directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals". (European Union, 2017)

[4] Directive 2008/114/EC was based upon Article 308 of the former European Community Treaty, which now corresponds to Article 352 of the Treaty on the Functioning of the European Union (TFEU) of 2007. (European Commission, 2012)

health, safety, security, economic or social well-being" of two or more member states (this would include bilateral critical infrastructure) or three or more member states (this would exclude all bilateral critical infrastructure) should be defined as European Critical Infrastructure (ECI) (European Commission, 2005). Critical infrastructure includes: a) energy installations and networks; b) communications and information technology; c) finance (banking, securities and investment); d) health care; e) food; f) water (dams, storage, treatment and networks); g) transport (airports, ports, intermodal facilities, railway and mass transit networks and traffic control systems); h) production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials); i) government (critical services, facilities, information networks, assets and key national sites and monuments) (European Commission, 2005a)

However, it is necessary to stress that none of these definitions can be considered as rigorous because they do not contain any specific information in order to precisely interpret which infrastructures fit the definition. The reason is that every state establishes its own criteria for defining which infrastructure can be considered critical and the list of the national critical infrastructures is normally classified. Additionally, there are many difficulties in determining which assets should be considered 'critical'. Indeed, as infrastructures are characterized by dense interconnections, networks, nodes, links and interdependencies, it is difficult to prioritize. Also, what should be considered 'critical' often changes over time, but "decision-makers are often unwilling to assume the political risk of removing items from a 'critical list', resulting in a waste of resources" (United Nations Security Council, 2017).

However, the *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* establishes general criteria to identify critical infrastructure. The identification and the designation of critical infrastructure is the result of a complex technical-political process stemming from the potential impact that a failure/disruption of an infrastructure can have in terms of sectoral and inter-sectoral relevance. The inter-sectoral evaluation criteria concern the following: a) potential victims (number of fatalities or injuries); b) potential economic effects (financial losses, deterioration of products or services, and environmental effects/damages); c) potential effects on population (impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services) (Official Journal of the European Union, 2008; Montanari and Querzoni, 2014). These criteria are described more in detail in the *Communication from the Commission on a European Programme for Critical Infrastructure Protection* of 2006 discussed in the following section. This document clearly states that the member states should identify and design their na-

tional critical infrastructures according to predefined national criteria that shall take into account specific qualitative and quantitative effects of the disruption or destruction of a particular infrastructure. These are the following: a) scope: the disruption or destruction of a particular critical infrastructure should be rated on the basis of the geographic area that could be affected by its loss or unavailability; b) severity: the consequences of the disruption or destruction of a particular infrastructure must be assessed on the basis of public effect (number of population affected), economic effect (significance of economic loss and/or degradation of products or services), environmental effect, political effects, psychological effects, public health consequences. If these criteria do not exist, the Commission will assist the member state upon request in their development by providing the necessary methodologies; c) establishment of a dialogue with CIP owners/operators; d) identification of geographic and sectoral interdependencies; e) national critical infrastructure related contingency plans where deemed relevant; f) the member states should base their national CIP programme on the common list of critical infrastructures sectors established for ECI[5].

The Council Directive states that critical infrastructures should be identified and designated through a common procedure of the Member States. This is due to the fact that the disruption and the destruction of critical infrastructure can have significant cross-border impacts. For this reason, critical infrastructures should be identified and designated on the basis of a common procedure between Member States (Official Journal of the European Union, 2008). It is in this perspective that *Regulation (EU) N. 347/2013 of the European Parliament and of the Council of 2013* underlines "the need to modernize and expand Europe's energy infrastructure and to interconnect networks across borders, in order to make solidarity between Member States operational, to provide for alternative supply or transit routes and sources of energy and to develop renewable energy sources in competition with traditional sources". The regulation also stresses that all Member States should be connected to the European gas and electricity networks in order to see its energy security ensured by the appropriate connections (*Regulation (EU) No. 347/2013 of the European Parliament and of the Council,* 2013).

Furthermore, an important aspect that is necessary to take into consideration is that critical energy infrastructure is a key factor of **energy security**, which is a crucial concept in this study. Energy is defined as the power coming from those sources (e.g. oil, electricity, gas) making a state work. Energy can be of three types: a) primary energy such as coal, crude oil, natural gas, wind or

[5] **The critical infrastructure sectors are: energy, nuclear industry, information and communication technologies, water, food, health, financial, transport, chemical industry, space, research facilities. (European Commission, 2006a)**

sunlight; b) secondary energy, which is primary energy that has been converted into electricity, diesel or kerosene; c) tertiary energy, which is secondary energy converted into a service like transportation, heating and cooling, and lighting (De Jong and Hughes, 2017). Security is defined as those measures that are taken to protect something in order to ensure the absence of threats. Energy security is here defined according to the International Energy Agency's definition as it is the consensual one. According to it, energy security is "the uninterrupted availability of energy sources at an affordable price" (International Energy Agency, 2017). It can be divided into physical security, price security and geopolitical security. Physical security is uninterrupted supply, which means "avoiding involuntary physical interruptions to consumption of energy (i.e., the lights going out or gas supplies being cut off) [but also available, reliable and accessible energy supply] (Månsson, Johansson, Nilsson, 2014). Price security is avoiding unnecessary price spikes due to supply/demand imbalances or poor market operation (e.g. market power). Geopolitical security is avoiding undue reliance on specific nations so as to maintain maximum degrees of freedom in foreign policy" (Chaudry, Ekins, Ramachandran, Shakoor, Skea, Strbac, 2009). This study mainly focuses on physical security as it refers to energy infrastructure as well as on cyber security that is crucial for the well-functioning of infrastructures. In fact, uninterrupted supply means security of supply, which "depends on a chain of well-functioning infrastructure and networks stretching from energy extraction through transportation, transformation, refining and distribution all the way to energy end use" (Johansson, 2013). Additionally, it is necessary to stress that energy security means different things to different countries as it depends on their geographic location, on their economic conditions as well as on their endowment of resources.

In this context, the concept of energy system is crucial. A system is "a group of interacting, interrelated, or interdependent elements forming a complex whole" (American Heritage Dictionary of the English Language, 2017). An energy system "consists of entities linked together forming chains from energy sources to end-users" (De Jong and Hughes, 2017). Entities can be external or internal to the system. External entities supply the system with energy (typically primary or secondary energy) or an energy service demanding tertiary energy from the system. Internal entities are "processes organized into energy chains which convert and transport the energy from its energy suppliers to meet the energy demand of the users of its energy services" (Hughes, De Jong and Qin Wang, 2016). A process is both a producer and a consumer of energy. The energy system of a state is interconnected and complex. Indeed, disruptions in one part of the infrastructure can spread out through the whole system (Yusta, Correa, and Lacal-Arántegui, 2011). Additionally, the critical infrastructure of a state is cross-sector dependent, which means that an outage in one critical

infrastructure sector (e.g. water, telecommunications, transport, etc) can impact other sectors. This is especially true for the energy sector as the others need energy to work. Also, a problem in a certain geographical area can have an impact on other regions or on other states (OSCE, 2013).

THREATS, VULNERABILITIES, RISKS: THE IMPORTANCE OF AN EFFICIENT RISK MANAGEMENT PROGRAMME

Most critical energy infrastructure, and critical infrastructure more generally, is owned by the private sector. In spite of this, it is the government that has the responsibility to regulate it and to some extent to protect it especially where protection is too important to leave to the private sector like in the case of the nuclear facilities (this is one of the reasons for the heavy regulatory system associated with nuclear power) (De Jong and Hughes, 2017).

Protection and security of critical energy infrastructure require the inclusion of every element of the energy infrastructure in the definition and in the implementation of a **risk management programme**. The interdependencies within the energy infrastructure are a major challenge for risk management. The reason is that economies and societies rely on interconnected and interdependent infrastructure systems. This gives rise to the so called 'cascading events', which means that if one disruption occurs, others are likely to follow within the systems and processes that are connected to the infrastructure affected by the initial disruption (OECD, 2008). The relevance of interdependencies is also stressed by the European Commission's Green Paper. This latter suggests that interdependencies should be taken into account in the identification process of ECI because this contributes to assess the potential impact of threats against specific critical infrastructures and to identify which member state would be affected in case of a major critical infrastructure related incident (European Commission, 2005). In particular, this document emphases that "full consideration would be given to interdependencies within and between businesses, industry sectors, geographical jurisdictions and member states authorities in particular those enabled by Information and Communication Technologies (ICTs) (European Commission, 2005).

The risk management programme should incorporate the analysis of the possible threats, the risk assessment, the vulnerabilities, and the implementation of hazard mitigation procedures. A 'threat' is "a possible event with the potential to adversely impact organizational operations". It can be a terrorist, cyber or kinetic attack as well as sabotage, disruption of supply or a natural disaster. 'Risk' is "a measure of the extent to which an [energy system] entity is threatened by

a potential event and is typically a function of the impact of the event and the likelihood of its occurrence" (Hughes, De Jong and Qin Wang, 2016). The term 'vulnerability' refers to "the weakness level of a system to failures, disasters or attacks" (Yusta, Correa, and Lacal-Arántegui, 2011). The degree of vulnerability can be measured in terms of how prepared an entity is to a specific event (Hughes, De Jong and Qin Wang, 2016).

An entity is in its normal state and experiencing the minimum stress when its consumption and production requirements are met. However, if an event changes these conditions, the entity will experience an increased stress and it will enter a new state, either tension or disruption. An entity in the tension state can continue operating although not to the standard of the normal state. Some entities can continue operating when they are in a tension state, passing from a low-tension state to a high-tension state when subsequent events occur. If the stress increases beyond the tipping-point, the entity stops operating and enters the disruption state (Hughes, De Jong and Qin Wang, 2016).

An event can be internal or external. An internal event occurs inside an entity and can be accidental or structural. Accidental events are "erroneous, non-deliberate actions taken by those responsible for the entity", such as misreading a meter, the installation of the wrong software, and the failure to communicate procedural changes. Structural events are "failures of equipment, environmental controls, or software due to ageing, or other circumstances which exceed the entity's expected operating parameters", such as failure of a crude oil pipeline due to corrosion, the failure of a blowout prevention valve, and the failure of sensors to detect a change in stack emissions (Hughes, De Jong and Qin Wang, 2016). There are four types of external events. First, an underproduction of energy event occurs when the demand for energy permanently exceeds the entity's production of energy. Second, an availability event occurs when the energy supply falls below the entity's demand. Third, a policy event occurs when a policy affecting the entity is introduced. Fourth, an environment event originates from a source in the entity's environment. Four types of environmental events exist. An unintentional environmental event is a non-malicious anthropogenic source that affects the operation of the entity by mistake (e.g. a backhoe operator digs a trench, damaging a natural gas pipeline). A resource environmental event occurs in case of a loss of a resource on which the entity depends (e.g. the loss of electricity that powers an oil pipeline's pumping station). A natural disaster event occurs in case of natural disasters from both terrestrial and extra-terrestrial sources which threaten the entity (e.g. a tsunami floods a nuclear reactor's backup generators). An adversarial event occurs when individuals, groups, organisations, or states actively seek to disrupt the functioning of the entity (e.g. a government agency inserts malicious software into a country's oil

pipeline pumping stations, causing them to fail catastrophically) (Hughes, De Jong and Qin Wang, 2016).

The likelihood of an entity entering a new state after the occurrence of the event is the "estimated probability that the threat event will occur" (Hughes, De Jong and Qin Wang, 2016). It can be expressed in terms of the time between events. If the event occurs frequently, which means that the time between events is short, the likelihood or the probability of the event is very likely. If the event does occurs infrequently, which means that the event occurs very rarely, the likelihood of the event very unlikely. If the event occurs periodically, the likelihood that the event occurs falls between very likely and very unlikely (Hughes, De Jong and Qin Wang, 2016).

The likelihood that an event occurs can be determined with a **risk analysis**. The method proposed in this study has been introduced by Larry Hughes, Moniek de Jong and Xiao Qin Wang in their article titled *A generic method for analyzing the risks to energy systems*. The authors discuss an interesting method of risk analysis that can be applied to any entity in an energy system. This method was originally conceived by the National Institute for Statistics and Technology and was used by the United States Department of Homeland Security for determining the risk in cyber-systems. It consists of six steps. The first step is the identification of threat sources, which can be another entity, the entity's environment, an anthropogenic source, or the entity itself. The actualization of a threat is a threat event or just an event that can be either internal or external. In some cases, multiple threat sources can initiate the same threat event. The second step is threat assessment and ranking. In this case, the level of stress should be determined either with qualitative or quantitative values or with both. The third step is vulnerability assessment and ranking. It consists in measuring the degree of vulnerability in terms of how prepared an entity is to a specific event. If the entity is vulnerable to the event, the appropriate countermeasures should be put in place in order to reduce the stress associated to the event to the pre-event stress level. If the event occurs but the countermeasures are not planned or only partially implemented, the entity's post-event stress level will be higher than the pre-event level (Hughes, De Jong and Qin Wang, 2016). Additionally, an element that is necessary to take into consideration is the time that the entity needs to recover from the event. If the time of recovery is very rapid or almost instantaneous, the entity is resilient. If the recovery time increases, the entity's tolerance to the event decreases to the point where recovery becomes intolerably long or impossible. Ideally, events never occur or are rare but, as they become more frequent, they can become intolerable (Hughes, De Jong and Qin Wang, 2016). The tolerance could be used to determine the value of the entity's vulnerability to the event. In order to do so, an assessment scale can be used

with both qualitative and quantitative values. A qualitative value can be obtained from interviews with experts, while a quantitative value could be determined from the ration of the time at which the entity is expected to recover to the time at which recovery is impossible. Therefore, a ratio near zero has a very low vulnerability to the event, whereas a value close to one indicates a high or very high vulnerability. The impact that the event has on the entity can be determined from the threat (the outcome of the event) and from the vulnerability (the entity's response to the threat), which either return the entity to the normal state or put it into a new state of tension or disruption (Hughes, De Jong and Qin Wang, 2016).

Furthermore, another element that is necessary to take into consideration in the risk analysis is the risk, as previously mentioned. Given the definition and the discussion above, risk "can be described as the likelihood of an event resulting in the entity entering a new state, depending on the entity's vulnerability" (Hughes, De Jong and Qin Wang, 2016). When the value of the risk is known, the people responsible for the entity can decide which actions to take in order to improve the entity's tolerance to the event. These actions can be simple countermeasures or countermeasures that change the entity in order to adapt it to the new 'normal' state (Hughes, De Jong and Qin Wang, 2016). It is important to note here that the decision about the kind of countermeasures to take usually depends on a cost-benefit assessment, which stems from the financial losses caused by the impact of the event on the entity. Assessments often concern a specific part of the infrastructure and reflect the requirements of the operators (De Jong and Hughes, 2017). However, the new countermeasures can result in new threats.

The method discussed above is generic. Therefore, each entity must deal with its specific set of threats and must be associated with the countermeasures necessary in their specific case (Hughes, De Jong and Qin Wang, 2016). In general, it is possible to say that risk management helps government to identify key security assess, assess risks, set up the priorities and implement the necessary strategies to mitigate those risks. Private operators play a key role in all these activities. Also, an efficient method is essential for the protection of critical infrastructure because it enhances its resilience. Infrastructure resilience is "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. Absorptive capacity is the ability of the system to endure a disruption without significant deviation from normal operating performance (...). Adaptive capacity is the ability of the system to adapt to a shock to normal operating conditions (....). Recoverability is the ability of the system to recover quickly— and at low cost— from potentially disruptive events" (US National Infrastructure Advisory Council, 2009).

Furthermore, an aspect that should be taken into consideration in relation to the protection of critical energy infrastructure and of critical infrastructure more generally is that governments make 'infrastructure-related discriminatory investment policies' in order to protect critical infrastructure. They can take three forms. The first one is blanket restrictions, which means banning foreign entities from reaching a threshold of ownership and control. They take the form of an absolute ban in some cases. The second form is sector-specific licensing provisions, which are licenses or contractual arrangements between the government and private entities. The third form is trans-sectoral measures including investment approval procedures that are trans-sectoral measures used 'to block infrastructure investments that are deemed to pose threats to essential security interests' (OSCE, 2008; Moore and Shenoi, 2010).

Additionally, the EU is also very much committed to improve the protection of critical infrastructures on its territory. To this aim, in 2005 the European Commission adopted the Green Paper mentioned above whose main objective is "to receive feedback concerning possible European Programme on Critical Infrastructure Protection (EPCIP) policy options by involving a broad number of stakeholders". The Green Paper states that "the effective protection of critical infrastructure requires communication, coordination, and cooperation nationally and at EU level among all interested parties-the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public" (European Commission, 2005). The Green Paper was the basis for the European Programme for Critical Infrastructure Protection (EPCIP) that was adopted by the European Commission in 2006. The Green Paper sets up the principles guiding the implementation of the Programme that are contained in the EPCIP itself and that are the following: a) subsidiarity, which means that the Commission may provide support to member states concerning national critical infrastructures where requested and taking due account of the Commission's competences and resources; b) complementarity, that is to say that the Commission shall avoid duplicate existing efforts at EU, national or regional level if these have proven to be effective in protecting critical infrastructure; c) confidentiality, which means that Critical Infrastructure Protection Information (CIPI) must be classified appropriately and access granted only on a need-to-know basis; d) stakeholder cooperation, which means that all relevant stakeholders (including the owners/operators of critical infrastructures designated as ECI and public authorities and other relevant bodies) should be involved in the development and implementation of EPCIP; e) proportionality, which means that measures should be proposed only when a need has been identified after an analysis of the existing security gaps and must be proportionate to the level of the risk and of the type of the threat concerned; f) sector-by-sector approach, which means

that the EPCIP will be developed on a sector-by-sector basis because various sectors possess particular experience, expertise and requirements with critical infrastructure protection (European Commission, 2005; European Commission, 2005a). On the basis of this principles, the aim of the EPCIP is to improve the protection of and to increase the resilience (against all threats and hazards) of critical infrastructures in the EU.[6] The underlying rationale is that "disruption to infrastructures providing key services could harm the security and economy of the EU as well as the well-being of its citizens" (European Commission, 2012). It is co-financed by the Community Programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013. In 2012, the EPCIP was reviewed by the Commission in close cooperation with the member states and other stakeholders. The review process revealed that the EPCIP did not give enough consideration to the links between critical infrastructures in different sectors. Consequently, a new approach was needed in order to build the resilience of critical infrastructures and to properly protect them (European Commission, 2013). The review process confirmed that the framework of the EPCIP consists of five elements. The first one consists of measures designed to facilitate the implementation of EPCIP. These measures are the following. An Action Plan sets out the actions to be achieved along with relevant deadlines and is updated regularly. It is implemented on the basis of sector specificities involving other stakeholders as appropriate.[7] The second element is the Critical Infrastructure Warning Information Network (CIWIN), which provides 'a platform for the exchange of best practices in a secure manner (...) and for the exchange of rapid alerts linked to the Commission's ARGUS system'.[8] The third element is the use of critical infrastructure protection (CIP) expert groups at EU level, which are established 'to address clearly precise issues and to facilitate public-private dialogue concerning critical infrastructure protection'. The fourth element is the CIP information-sharing process and the

[6] The need to ensure high degree protection of the EU infrastructures and to increase their resilience is stressed in the Stockholm Programme of 2009 and in the EU Internal Security Strategy of 2011. (European Commission, 2013). The Stockholm Programme underlines the need to reduce the vulnerabilities of the EU critical infrastructure is an essential objective. It also invited the Council, the Commission, the European Parliament, and the member states to draw up and implement policies aiming at improving the necessary measures for the protection, security preparedness and resilience of critical infrastructure. It also emphasized the importance of the including additional policy sectors through the analysis and the review of Directive 2008/114/EC. The EU Internal Security Strategy highlights that the EU should continue designating critical infrastructure and put in place plans to protect those assets because they are essential for the functioning of the society and of the economy. The Strategy also emphasizes that efficiency and coherence of the infrastructure should be increased through the improvement of long-standing crisis and disaster management practices. (European Commission, 2012)

[7] The Action Plan organizes CIP related activities around three work streams: 1) the strategic aspects of EPCIP development of measures horizontally applicable to all CIP work; 2) the activities dealing with ECI that are implemented at a sectoral level; 3) support provided to the member states in their activities concerning national critical infrastructures. (European Commission, 2006)

[8] ARGUS is a system linking all specialized systems for emergencies and a central crisis centre bringing together all relevant Commission services during an emergency. (European Commission, 2017)

identification and analysis of interdependencies. The CIP information-sharing process means that stakeholders should take the appropriate measures to protect information concerning the issues related to the protection of critical information. The identification and analysis of interdependencies, both geographic and sectoral, is an important element to improve critical infrastructure protection in the EU. The fifth element is the support of member states concerning national critical infrastructures. This means that the Commission helps the member states to protect their critical infrastructure where this is requested. The sixth element is contingency planning, which is a key element of the CIP process as it helps minimize the potential effect of disruption or destruction of critical infrastructure. The seventh element is the external dimension of critical infrastructure protection. Its importance is due to the fact that threats such as terrorism, other criminal activities, natural hazards and other causes are not constrained by national borders. As today's economy and society are interconnected by nature, a disruption outside the EU's borders can have a detrimental impact on the Community and its member states. The eighth element is the EU programme on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks' for the period 2007-2013, which provides funding for CIP-related measures. The programme will stimulate, promote and develop measures aiming at preventing and reducing security risks (in particular those related to terrorism through prevention, preparedness and consequence management (European Commission, 2006).

Furthermore, while increasing and improving the protection of critical energy infrastructure, the EU aims at integrating its energy market in order to meet its energy and climate goals.[9] Also, "an interconnected European grid will help deliver the ultimate goals of the Energy Union[10] to ensure affordable, secure and sustainable energy to all Europeans" (European Commission, 2017b).

[9] In the context of the 2030 Framework for climate and energy, the EU members have agreed "to help the EU achieve a more competitive, secure and sustainable energy system and to meet its long-term 2050 greenhouse gas reductions target". The targets are the following: "a) a 40% cut in greenhouse gas emissions compared to 1990 levels; b) at least a 27% share of renewable energy consumption; c) at least 27% energy savings compared with the business-as-usual scenario". (European Commission, 2017a)

[10] The Commission launched the Energy Union strategy in 2015 to "ensure that Europe has secure, affordable and climate-friendly energy". It is made of five dimensions: 1) security, solidarity and trust, aiming at diversifying energy supplies and at ensuring energy supplies through solidarity and cooperation between member states; 2) a fully-integrated internal energy market, aiming at securing supply and at giving consumers the best energy deal through a free flow of energy throughout the EU through adequate infrastructure and without any technical and or regulatory barriers; 3) energy efficiency, aiming at reducing the dependence of member states on energy imports, at reducing emissions and at driving jobs and growth; 4) climate action-decarbonising the economy, aiming at implementing an effective climate policy necessary to creating an Energy Union; 5) research, innovation and competitiveness, aiming at driving the transition of the energy system and improve competitiveness through breakthroughs in low-carbon and clean energy technologies by prioritising research and innovation. (European Commission, 2017c)

It is in this perspective that the Commission has launched the Trans-European Networks for Energy (TEN-E) strategy. The aim is to fund new energy infrastructure projects all over Europe because not all investments are commercially viable. The TEN-E strategy should be seen in the context of the European Energy Security Strategy[11] of 2014 whose aim is "to ensure a stable and abundant supply of energy for European citizens and the economy". In particular, the TEN-E strategy serves two of the eight key pillars of the European Energy Security Strategy, namely building a well-functioning and fully integrated internal market and diversifying external supplies and related infrastructure. The European Energy Security Strategy clearly states that accelerating the construction of key interconnectors is crucial to create a truly integrated and competitive internal market. The European Energy Security Strategy also stresses that "a truly integrated and competitive internal energy market not only needs a common regulatory framework but also significant development of energy transport infrastructure, in particular with the development of cross-border interconnections between member states" (European Commission, 2014). According to the Commission, around 200 billion are needed during the current decade to update the existing Europe's infrastructure. The Regulation on the Guidelines for trans-European energy networks of 2007 and the Connecting Europe Facility (CEF), which "is a key EU funding instrument to promote growth, jobs and competitiveness through targeted infrastructure investment at European level" (European Commission, 2017g), ensure the timely implementation of the key projects Europe needs by identifying 12 priority corridors and areas. The Projects of Common Interest (PCIs) are drawn up by the Commission every two years. They "are key infrastructure projects, especially cross-border projects, that link the energy systems of EU countries. They are intended to help the EU achieve its energy policy and climate objectives: affordable, secure and sustainable energy for all citizens, and the long-term decarbonisation of the economy in accordance with the Paris Agreement"[12] (European Commission, 2017d). In order to become a PCI[13], "a project must have a significant impact on energy markets and market integration in at least two EU countries, boost competition on energy markets and help the EU's energy security by diversifying sources,

[11] The European Energy Security Strategy, which "sets out areas where decisions need to be taken or concrete actions implemented in the short, medium and longer term to respond to energy security concerns". It is based on eight key pillars: 1) immediate actions aimed at increasing the EU's capacity to overcome a major disruption during the winter 2014/2015; 2) strengthening emergency/solidarity mechanisms including coordination of risk assessments and contingency plans; and protecting strategic infrastructure; 3) moderating energy demand; 4) building a well-functioning and fully integrated internal market; 5) increasing energy production in the European Union; 6) further developing energy technologies; 7) diversifying external supplies and related infrastructure; 8) improving coordination of national energy policies and speaking with one voice in external energy policy. (European Commission, 2014)

[12] The Paris Agreement was signed by 195 states with the aim to set out a global plan "to avoid dangerous climate change by limiting global warming to well below 2° C". (European Commission, 2017e)

and contribute to the EU's climate and energy goals by integrating renewables" (European Commission, 2017d).

Consequently, the TEN-E strategy helps reduce the isolation of the less-favoured, island, landlocked or remote regions by strengthening the territorial cohesion of the EU and promotes sustainable development, especially by improving the links between renewable energy production installations and using more efficient technologies. In so doing, the environmental risks associated with the transportation and transmission of energy will be reduced (Eur-Lex, 2007).

Finally, in 2009 the EU established the European Network of Transmission System Operators (ENTSO-E) that was given legal mandate by the EU's Third Legislative Package for the Internal Energy Market in 2009, which aims at further liberalising the gas and electricity markets in the EU. The objective of ENTSO-E is to "set up the internal energy market and ensuring its optimal functioning, and of supporting the ambitious European energy and climate agenda. One of the important issues on today's agenda is the integration of a high degree of Renewables in Europe's energy system, the development of consecutive flexibility, and a much more customer centric approach than in the past. ENTSO-E is committed to develop the most suitable responses to the challenge of a changing power system while maintaining security of supply. Innovation, a market based approach, customer focus, stakeholder focus, security of supply, flexibility, and regional cooperation are key to ENTSO-E's agenda" (ENTSOE, 2015). It represents 43 electricity transmission system operators from 36 states across Europe.

In short, the protection of critical energy infrastructure is a key issue that states and the EU are very committed to deal with in order to ensure the well-functioning of the society. It requires taking into consideration every element of the energy infrastructure in order to efficiently implement a risk management programme. Although the protection of critical energy infrastructure is a national competence, legislation and instruments have been put in place at the EU level.

[13] As part of the TEN-E strategy nine priority corridors and three thematic areas have been identified. The priority electricity corridors are four: 1) North Seas offshore grid (NSOG-North Sea, Irish Sea, English Channel, Baltic Sea and neighbouring waters); 2) North-south electricity interconnections in western Europe ('NSI West Electricity'- Mediterranean area including the Iberian peninsula); 3) North-south electricity interconnections in central eastern and south eastern Europe ('NSI East Electricity'); 4) Baltic Energy Market Interconnection Plan in electricity ('BEMIP Electricity'). The priority gas corridors are four: 1) North-south gas interconnections in Western Europe ('NSI West Gas'); 2) North-south gas interconnections in central eastern and south eastern Europe ('NSI East Gas'); 3) Southern Gas Corridor ('SGC'- Caspian Basin, Central Asia, Middle East and eastern Mediterranean Basin); 4) Baltic Energy Market Interconnection Plan in gas ('BEMIP Gas'). The priority gas corridor are the oil supply connections in central eastern Europe. The priority thematic areas related to the entire EU are: 1) smart grids deployment; 2) electricity highways; 3) cross-border carbon dioxide network. (European Commission, 2017f; Official Journal of the European Union, 2013)

THE PUBLIC-PRIVATE PARTNERSHIP: CHALLENGES AND OPPORTUNITIES FOR THE PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE

The broad definition of Public-Private Partnership that this study applies is the one contained in Article 15.41 of the EU Regulation 549/2013, namely "Public-Private Partnerships (PPPs) are long-term contracts between two units, whereby one unit acquires or builds an asset or set of assets, operates it for a period and then hands the asset over to a second unit. Such arrangements are usually between a private enterprise and government but other combinations are possible, with a public corporation as either party or a private non-profit institution as the second party" (Official Journal of the European Union, 2013a). PPPs are therefore contractual agreements between a public agency or public sector authority and a private sector entity that allow a private-sector entity to participate in the delivery of public services, or in developing an environment that improves the quality of life for the general public (Witters et al., 2012). The PPPs do not just fund projects but they require full commitment from all partners for the entire undertaking (Witters et al., 2012). In particular, the importance of PPPs lies on the fact that the cooperation between the public and the private sectors is crucial to efficiently respond to the escalating worldwide threats in order to protect infrastructures. PPPs are indeed seen as a key instrument to mitigate the threat (Carr, 2016). This practice is however not a new one as it can be traced back to the ancient times. For instance, in the 4th century BC in the city-state (polis) of Athens prominent citizens financially contributed to public festivals and religious events and to build public festivals and monuments. Some centuries later, in the Roman empire, civilians worked hand-in-hand with the Roman army to build the necessary infrastructure (Witters et al., 2012).

However, the PPPs practice intensified only after 1990 when the privatization of critical infrastructure was considered as beneficial for the state from an economic perspective, freeing up capital and drawing more heavily on the efficiencies and business practices of the private sector (Carr, 2016). Another reason for the intensification of the PPPs practice is the progressive specialization in modern societies, which means that performing tasks requires highly specific expert knowledge. As a consequence, the division of labor, which is seen as essential in modern societies, blurs the lines between the public and the private sector. Therefore, many tasks that were previously performed by the state are today handled by specialized companies (Dunn-Cavelty and Suter, 2009). The last decade in particular has seen a marked increase in cooperation between the public and the private sectors as a "direct result of efforts to increase the quality and efficiency of public services, insufficient public sector financial re-

sources to cover investment needs coupled with spending restrictions and a desire to access private sector efficiencies" (European Commission, 2003).

In this context, two considerations should be done. The first one concerns the fact that critical infrastructure protection is unequivocally strictly linked to national security. This raises the question about to what extent the state renounces to its authority as well as to its responsibility for national security. Indeed, as ensuring security for the citizens is a core task of the state, to pass on its responsibility in the area of critical infrastructure protection is a delicate matter for the government. Therefore, as Madeline Carr puts it, "this raises questions about how well the state is equipped to provide national security in this context and about how existing policies and practices of national security are being challenged by this new threat conception" (Carr, 2016). The second consideration pertains to the two phenomena that the technological development characterizing the last decades have triggered, namely an increasing privatization and internationalization (or globalisation). These two trends become manifest in the form of PPPs (Carr, 2016; Dunn-Cavelty and Suter, 2009). As for the increasing privatization, the development of the Information and Communication Technology (ICT), which is predominantly privately owned and operated and on which many other sectors depend, has complicated the situation. This has led to question who is the real authority. Quoting De Bruijne and Van Eeven, Christer Pursiainen states that "government authorities may have, formally or informally, the overall responsibility for the reliable provision of services, but they lack authority and resources to actually fulfil that responsibility. Central governments bodies and policy makers involved in CIP to a large extent lack the technical expertise and the means to monitor or control CI operation" (Pursiainen, 2009). For what concerns globalization, it is worth noting that it has made the situation more complex from the perspective of the government control. In fact, national critical infrastructure depends not only on other sectors but also on other states because no state is immune to the effects suffered from serious infrastructure disruptions from its neighbours (Pursiainen, 2009).

The PPPs legal construction can include three types of arrangements, which are clearly identified by Louis Witters. He argues that the first one "can be used to introduce private-sector ownership into state-owned businesses through a public listing or the introduction of an equity partner". The second type is "a private finance initiative, where the government takes advantage of private-sector management skills by awarding long-term franchises to a private-sector partner, which assumes the responsibility for constructing and maintaining the infrastructure and for providing the public service". The third type "can cover the selling of government services to private-sector partners, which can better exploit the commercial potential of public assets" (Witters et al., 2012). In these

cases the private-sector consortium forms a special company called 'special purpose vehicle' (SPV) whose aim is to develop, build, maintain, and operate assets for the contracted period. Wherever the government has invested in the project, it is usually allotted an equity share in the SPV. Also, within the PPP it is the SPV that signs the contract with the government and the subcontractors to build the facility and to maintain it (Witters et al., 2012). However, in more general terms, the identification and classification of PPPs often takes place within a framework of authority and responsibility. In particular, it is possible to identify two broad categories. First, horizontal, non-hierarchical arrangements characterized by consensual decision-making. Second, hierarchically organized relationships with one party in a controlling role. The true partnerships are of the first category.

Furthermore, it is necessary to emphasize that private-sector owners of critical infrastructure accept to make their system secure only to the point that it is profitable, which means to the extent that the cost of dealing with an outage would cost more than preventing it. Also, they tend to distinguish between protecting against low-level threats such as individual hackers and protecting against an attack on the state (that is a national security issue). This distinction is at the core of the tension of the PPPs. The rational is that neither partner can achieve its objectives on its own. Consequently, either each needs the other to achieve its own goals or there must be a financial arrangement that makes the partnership attractive to both parties (Carr, 2016).

In this context, the dilemma of common good becomes relevant. The governments expect that the private sector makes considerable investments beyond its cost-benefit calculations. De Bruijne and Van Eeven argue that the governments have two options, namely providing the necessary resources itself with the public budget or increasing regulation. According to them, the first option is mostly impossible because of financial resource reasons. The second option would oblige the private sector to invest more resources to deal with the protection or the resilience of the systems they own or operate. De Bruijne and Van Eeven argue that increasing state regulation would mean coming back from liberalization to state regulation. However, they also argue that when governments have two options, most CIP strategies do not propose any of them. Instead, national CIP strategies are often confined to the status quo by stressing the need for awareness raising and best practice exchange (Pursiainen, 2009). In this context, information sharing is particularly important. In fact, in order to have a proper security strategy, it is important that the private and the public sectors share all the necessary information and techniques related to risk assessment, the identification of weak spots, plans and technology to prevent attacks and disruptions, and plans for recovering from them (Pursiainen, 2009). However,

there are a number of obstacles to sharing information from both government's and private sector's perspectives. For instance, according to the private sector it is not always easy to immediately distinguish between some kinds of technical problems, a low-level attack and a large-scale sustainable attack. In addition, sometimes reporting vulnerabilities is against their commercial interests, especially if understanding and rectifying a problem before competitors become aware of it offers an advantage on the market. Also, if a private security firm shares information with the government about a threat (e.g. a cyber attack), this information could be shared with its competitors. For private security firms their business relies on obtaining, holding and selling information, not on sharing them (Carr, 2016). A reason for this is that private companies often fear that sensitive information on past security incidents that is shared with the government is not treated with the necessary confidentiality causing damage to their reputation (Dunn-Cavelty and Suter, 2009). At the same time, the public sector also has some limitations in sharing information. Indeed, classified information cannot be exchanged with individuals that have not an adequate security clearance. Sometimes, even those working in the private sector can't use classified information because to take action on it would mean to expose it. In addition, there is high expectation that the information that the government shares with the private sector is accurate. For this reason, the processes of review and revision are quite extensive and stringent. This delays the release of time-critical information. Finally, personal relationships are a key element for an effective information sharing process, which means that people are more inclined to share information with colleagues with whom they had previously had a strong personal and/professional bond (Carr, 2016). This shows that information exchange requires strong mutual trust as it involves the exchange of extremely sensitive information. Trust is very difficult to establish. The main problem is that trust can only be established through cooperation that depends on trust. As Dunn-Cavelty and Suter puts it, "the establishment of public-private information exchange is therefore an example of the chicken-and-egg paradox or in other words, a classic assurance problem. For this reason, information exchange between public and private partners usually only succeeds in a small framework with selected partners who have already established a certain degree of trust or in cases where such trust can be established reasonably easily" (Dunn-Cavelty and Suter, 2009).

Therefore, it is possible to state that the involvement of governments in the practical efforts in protecting critical infrastructure of the private sector is quite limited. An important factor to stress here is that the private sector determines the investments to protect critical infrastructure on the basis of its business interests. The underlying logic is the one of the market liberalization for which it is important to keep prices low for consumers although the vulnerabilities of

infrastructures increase. In order to achieve this goal, the funds available for the investment in and for the maintenance of key assets are reduced. Additionally, as the majority of companies operates internationally, they are only partially interested in national cooperation. Therefore, international approaches would be much more attractive and interesting for transnational businesses (Dunn-Cavelty and Suter, 2009).

In conclusion, PPPs are not only sensible but also necessary in order to protect critical infrastructures. In spite of this, these partnerships are not easy ones for a number of factors that are mainly related to the fact that the interests of the public and of the private sectors not always coincide as well as to the information sharing issue.

THE ROLE OF NATO IN CRITICAL ENERGY INFRASTRUCTURE PROTECTION

Although critical infrastructure protection is a national competence, international organizations are involved in work concerning it, too. The reason is the crucial importance of the issue for the national security of the international organisations' member states.

NATO supports the protection of critical energy infrastructure of the Allies, which is one of its three main activities in the field of energy together with enhancing strategic awareness of the security implications of energy developments and enhancing energy efficiency in the military.[14] NATO tries to increase its competence in supporting critical energy infrastructure protection recognizing that attacks on it by hostile states, terrorists or hacktivists can have repercussions across regions because infrastructure networks extend beyond borders (NATO, 2016).

NATO's interest in the protection of critical energy infrastructure and in critical infrastructure more broadly began in 2001. The reason behind NATO's interest were the terrorist attacks of 11/9 in 2001, when some militants associated with the Islamic extremist group al-Qaeda hijacked four airplanes and carried out suicide attacks against several targets in the United States. Over time, NATO's interest in the issue has been consolidated in several documents

[14] NATO tries to raise awareness in the field of energy security as energy security developments (e.g. supply disruptions) can have serious consequences on the security of the Allies. The activities of NATO in the field include consultations on energy security among the Allies and the partner countries, intelligence sharing, and organising specific events like workshops, table-top exercises and briefing by external experts. Enhancing energy efficiency in the military focuses on reducing the energy consumption of military vehicles and camps and on minimising the environmental footprint of military activities. In this sector, NATO's work mainly focuses on bringing together experts to examine existing national endeavours, exchanging best practices, proposing multinational projects, studies on the behavioural aspects of saving energy in exercises and operations, and developing common energy-efficiency standards and procedures (NATO, 2016).

and programmes. For instance, Riga Declaration of 2006 recognises that the security interests of the Alliance can also be affected by the disruption of the flow of vital resources. For this reason, this document stresses the importance of "a coordinated, international effort to assess risks to energy infrastructures and to promote energy infrastructure security" (NATO 2014). Also, the Strategic Concept of 2010 states that the Alliance must "develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning" (NATO, 2010). In 2004, the Programme of Work on Defense Against Terrorism aimed at developing new or adapted technologies to detect, disrupt and defeat terrorists for the armed forces of the Allies and at providing rapid response capabilities for the protection of civilian populations and infrastructure (NATO, 2004). Moreover, at the Bucharest Summit of 2008 the Allies decided that NATO must engage itself in several fields concerning energy security, namely the protection of critical energy infrastructure, information and intelligence fusion and sharing, projecting stability, advancing international and regional cooperation in the sector, and consequence management support. Additionally, the document emphasizes that the Alliance would continue "to consult on the most immediate risks in the field of energy security" and would "ensure that NATO's endeavours add value and are fully coordinated and embedded within those of the international community, which features a number of organisations that are specialised in energy security" (NATO, 2008).

In addition to this, it is important to mention the three documents issued in 2017 by the **Industrial Resources and Communication Services Group (IRCSG)**, which is part of the Civil Emergency Planning Committee (CEPC) of NATO. The first document is titled 'Recommendations and best practices on the protection of electricity, gas and oil critical infrastructure (Critical Energy Infrastructure Protection CEIP)" (IRCSG, 2017). This document designs the best practices "to support national policy makers and relevant authorities in their efforts to review their national sectoral arrangements". It also stresses that while recognizing that resilience of energy supply is crucial to both national and Alliance collective security and that it requires a combination of civil preparedness and military capacity, "NATO has been primarily concerned with aspects of national planning that address continuity of government, continuity of essential services to the population and civil support to military operations" (IRCSG, 2017). Additionally, this document emphasizes the key role that the IRCSG can play as a "transatlantic forum to conceptualize the threat environment, establish generic best practices, check lists, non-binding guidelines and conduct seminars and training events" in order to support national authorities to protect their critical infrastructures (IRCSG, 2017). The second document is "Guidance on improving

resilience of national and cross-border energy networks". This report discusses the vulnerabilities in the energy supply networks and addresses the new trends like the security implications of the digitalization of the energy industry. This report also "describes how the energy sector threat landscape has evolved as a result of enhanced cross-border connectivity and application of new technologies to remotely control physical systems, such as electricity networks and energy pipelines" (IRCSG, 2017a). The report recommends that CEPC guides and assists the Allies in planning to mitigate the risks to and enhance the resilience of national and cross-border energy networks. Additionally, it also recommends that **NATO Energy Security Centre of Excellence (ENSEC COE)**[15] creates a database focusing on the Allies' energy production, in-country stocks and imports and dependencies on third country supply (IRCSG, 2017a). The third document is "Evaluation criteria on resilience", whose aim is to assist the Allies in conducting national self-assessment of their resilience. It provides recommendations on the necessary measures that the Allies should apply to increase the resilience of their energy infrastructure like ensuring that key stakeholders have developed and implemented contingency plans and continuity management arrangements for the provision of those networks and services, and identify alternative supply options to mitigate energy vulnerabilities and implement multiple supply arrangements to ensure energy redundancy and diversity. Other important recommendations in the context of this study concern the development of national arrangements to assess energy usage and critical cross-border interdependencies, putting in place a mechanism to notify the appropriate NATO body of attacks on energy systems which may impact on NATO operations, and the establishment of a national platform with government and private sector participation to assess and coordinate network functionality and maintain situational awareness (IRCSG, 2017b).

Furthermore, it is worth mentioning the Izmir NATO Headquarters Directive 080-02 on the Infrastructure Assessment for Land Operations of 2016. The aim of this directive is "to provide a direction on the preparation, conduct, output and dissemination of Infrastructure Assessments within the framework of the Critical National Infrastructure assessment of a Host Nation's Infrastructure as an intrinsic part of the Operations Planning process" (Izmir NATO, 2016). The directive clarifies that it does not include Force Deployed Infrastructure. This directive identifies the critical national infrastructure that is important for military operations because its maintenance and protection is crucial for the success of such operations. National infrastructure is defined as "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery

[15] **NATO ENSEC COE was accredited by NATO in 2012 and is located in Vilnius, Lithuania. It "currently operates as a widely recognized international military organization with the aim of providing qualified and appropriate expert advice on questions related to operational energy security". (NATO Energy Security Centre of Excellence, 2016)**

of essential services upon which daily life in the country depends" (Izmir NATO, 2016).

The discussion conducted above shows that NATO is committed to support the Allies to protect critical energy infrastructure. This practically happens mainly through training and exercises. In this context, the Table-Top Exercise (TTX) entitled 'Exercise Coherent Resilience 2017' (CORE 17) that ENSEC COE and the Ministry of Energy and Coal Industry of Ukraine with the support of US Naval Postgraduate School organized in Kiev on 16-20 October 2017 is a very good example. CORE 17 was funded by NATO ENSEC COE and by NATO's programme Science for Peace and Security.[16] Its aim was to support the Ukrainian authorities in building the resilience of their critical energy infrastructures by improving their emergency preparedness, planning, prevention, and threat response, as well as to strengthen their capability to protect electricity-related critical energy infrastructure. At the same time, the exercise aimed at contributing to developing NATO's competence in supporting the protection of critical energy infrastructure. The fictional setting of the exercise was the conflict between Russia and Ukraine on the Ukrainian borders with Russia, which was based on the real conflict between the two states in 2014. The exercise consisted of four stages: 1) concept specification and development, which consisted in the explanation of the main concepts and of the presentation of the scenario to be used in the exercise; 2) planning and product development, which consisted in the planning of the exercise and in the explanation of how it should be conducted and developed; 3) operational conduct, which consisted in the Academic Seminar and Scenario-based discussions (this latter was divided into three phases, namely the discussion of critical energy infrastructure protection in a) pre-conflict, b) conflict, and c) post-conflict situations); 4) analysis and reporting, which consisted in the evaluation of the results of the exercise by taking into consideration its main aims. The exercise was very useful as it helped the Ukrainian authorities to better understand the vulnerabilities of the critical energy infrastructure of the state and to better face the challenges coming from them. Additionally, the participation of experts from several states (e.g. Belgium, Lithuania, Italy, Latvia, Ukraine, United Kingdom, USA, Georgia, Germany, Czech Republic, Ireland) was an added value as they shared their knowledge and experiences, which made the discussions more valuable and interesting.

However, this TTX is not the only one that NATO ENSEC COE has organized. The first one on 'Critical Energy Infrastructure' was held in December 2014 in Vilnius.

[16] **The Science for Peace and Security (SPS) Programme promotes dialogue and practical cooperation between NATO member states and partner nations based on scientific research, technological innovation and knowledge exchange. The SPS Programme offers funding, expert advice and support to tailor-made, security-relevant activities that respond to NATO's strategic objectives. (NATO, 2017)**

35 experts from 9 states participated. The purpose of the table top exercise was to collect and share information and experience from senior civil emergency planners and crisis management officers from NATO member countries and Istanbul Cooperation Initiative (ICI) partners on protection of critical energy infrastructure and present an overview of the existing challenges. The analysis and the overview of these challenges contributed to comprehensive solutions for energy security education and training for the mid and long term. The chosen method was initial plenary lectures followed by syndicate discussions on three different threats to critical energy infrastructure and the presentation of findings and recommendations. The purpose was to ensure a result with maximum participation by all mentors, stakeholders and Subject Matter Experts (SMEs). Senior civil emergency planners and crisis management officers from NATO member countries and ICI partners exercised three scenarios, which included Liquefied Natural Gas (LNG) shipment incidents, terrorist and cyber risks to energy-related port infrastructure, as well as strategic communications challenges, all affecting the transportation of energy resources. After the lectures and initial training, the exercise participants were split into three Syndicates – Emergency Response Planning Teams that discussed the Terrorism-based scenario, the Cyber-attack-based scenario and the STRATCOM-based scenario. The TTX enhanced participants' competence in supporting the protection of critical energy infrastructure through the sharing of information and experience. Furthermore, the exercise encouraged the participating NATO and partner nations and stakeholders of critical energy infrastructure to update their CEIP strategies in light of new emerging threats.

The second TTX was organized in Vilnius in 2016. The NATO Energy Security Centre of Excellence organized and conducted The Table Top Exercise on Critical Energy Infrastructure Protection - 2016 (TTX CEIP 2016) with the support of the NATO Emerging Security Challenges Division. The TTX sought to gather together experts from NATO, regional NATO member nations and partners, civil emergency planners (including NATO), law enforcement units, military (J2,J5) from NATO and other nations, intelligence and security services, the private sector, operators, representatives from related ministries (Interior, Defence, Foreign Affairs, Energy etc.), NGOs and think tanks. 68 experts from 11 states participated. The Table Top Exercise served as an opportunity for stakeholders to assess and develop their plans and procedures, share information and best practice, increase awareness, and enhance coordination between all responsible institutions. The TTX was based on the Skolkan Scenario (Skolkan 1) Geo-Strategic Situation which was developed by the Joint Warfare Centre used in the exercise as a background of the main scenario event lists. In accordance with the theme of the exercise the incidents related to critical energy infrastructure injected in order to raise the crisis. In total, 27 incidents injected based on the

scenario. The TTX was conducted in three phases. During the first phase, the experts delivered their conceptual understanding of critical energy infrastructure protection and the processes, as well as the best practices concerning critical energy infrastructure. During the second phase, the training audience was divided into syndicates based on identified manmade threats, terrorism, sabotage, cyber-attack, and information warfare. The participants discussed prevention and protection measures, and developed solutions on how to respond to defined incidents in the scenario to recover or mitigate effects. The third phase was dedicated to evaluation and distinguished visitor day (DVD) activities. The table top exercise identified the emerging security issues for future research and studies as well as training objectives of future exercises on the issue of critical energy infrastructure protection and enhanced the competences of the participants in the field.

In short, NATO is very much committed to increase the expertise of its members and partners in the field and in sharing information about the issues related to critical energy infrastructure protection. In spite of the fact that NATO is committed to support the Allies in protecting their critical energy infrastructure, the action of the Alliance is not sufficient because a clear strategy does not exist.

CONCLUSION

The protection of critical energy infrastructure, which is subject to both the EU and national law, is a priority for states because a disruption or the destruction of a part of it can have a negative impact on several other sectors of critical infrastructure within an economy. In spite of this, a consensual definition of the concept does not exist. For this reason, this study has tried to provide one on the basis of the EU and NATO ones. However, the main elements that must be taken into consideration in the protection of critical energy infrastructure are very clear. These elements have been discussed in the context of a method that could be used for risk assessment in order to protect critical energy infrastructure and critical infrastructure more generally. However, a good method is not sufficient to efficiently protect critical energy infrastructure. PPPs are also necessary. In spite of this, the public and the private sectors have often different interests. Indeed, while the former sees critical energy infrastructure protection in terms of national security, the latter sees it in business terms. The fact that states consider the issue as crucial for their national security is the reason why NATO is committed to support the Allies in protecting their national infrastructures. In order to do so, NATO organises trainings and exercises, which are valuable to increase awareness and information sharing among the Allies as well as in its partner countries.

BIBLIOGRAPHY

American Heritage Dictionary of the English Language. (2017). *System*. Boston, MA.: Houghton Mifflin Company. Retrieved from https://www.ahdictionary.com/word/search.html?q=system

Carr, M. (2016). *Public-private partnerships in national cyber-security strategies*. International Affairs. Oxford: John Wiley and Sons Ltd

Chaudry, M., Ekins, P., Ramachandran, K., Shakoor, A., Skea, J., Strbac, G. (2009). *Building a resilient UK energy system. Working Paper 31 March.* London: UK Energy Research Centre

De Jong, M., Hughes, L. (2017). *Critical Energy Infrastructure: Identification and Protection.* Energy Security: Operational Highlights. Issue 11

Department of Homeland Security. (2017). *What is critical infrastructure?* Retrieved from https://www.dhs.gov/what-critical-infrastructure

Dunn-Cavelty, M., Suter, M. (2009). *Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection.* International Journal of critical Infrastructure Protection. Issue 2

ENTSOE. (2015). *Who is ENTSO-E.* Retrieved from https://www.entsoe.eu/about-entso-e/Pages/default.aspx

Eur-Lex. (2017). *Green paper. Glossary of Summaries.* Retrieved from http://eur-lex.europa.eu/summary/glossary/green_paper.html

Eur-Lex. (2007). *Decision No 1364/2006/EC* of the European Parliament and of the Council of 6 September 2006 laying down guidelines for trans-European energy networks and repealing Decision 96/391/EC and Decision No 1229/2003/EC. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l27066&from=EN

European Commission. (2003). *Guidelines for successful public-private partnerships.* Retrieved from http://europa.eu.int/comm/regional_policy/sources/docgener/guides/PPPguide.htm

European Commission. (2005). *Green Paper on a European Programme for Critical Infrastructure Protection.* COM(2005) 576 final. Brussels

European Commission. (2005a). *Communication from the Commission to the Council and the European Parliament of 20 October 2004-Critical Infrastructure Protection in the fight against terrorism* [COM(2004)702 final]. Brussels

European Commission. (2006). *Communication from the Commission on a European Programme for Critical Infrastructure Protection*. COM (2006) 786 final. Brussels

European Commission. (2006a). *The European Programme for Critical Infra-*

structure Protection (EPCIP). Retrieved from http://europa.eu/rapid/press-release_MEMO-06-477_en.htm

European Commission. (2012). *Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP).* SWD(2012) 190 final. Brussels

European Union. (2013). *Regulation (EU) No. 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No. 1364/2006/EC and amending Regulations (EC) No. 714/2009 and (EC) No. 715/2009.* Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0347&from=EN

European Commission. (2013). *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure.* SWD(2013) 318 final. Brussels

European Commission. (2014). *EU Energy Security Strategy.* Retrieved from https://ec.europa.eu/energy/sites/ener/files/publication/European_Energy_Security_Strategy_en.pdf

European Commission. (2017). *ARGUS-a general European rapid alert system*. Retrieved from https://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/argus_en

European Commission. (2017a). *2030 Energy Strategy.* Retrieved from https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/2030-energy-strategy

European Commission. (2017b). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Communication on strengthening Europe's energy networks.* COM(2017) 718 final

European Commission. (2017c). *Priorities. Energy Union and Climate.* Retrieved from https://ec.europa.eu/commission/priorities/energy-union-and-climate_en

European Commission. (2017d). *Energy. Projects of Common Interests*. Retrieved from https://ec.europa.eu/energy/en/topics/infrastructure/projects-common-interest

European Commission. (2017e). *Climate Action.* Retrieved from https://ec.europa.eu/clima/policies/international/negotiations/paris_en

European Commission. (2017f). *Trans-European Networks for Energy.* Retrieved from https://ec.europa.eu/energy/en/topics/infrastructure/trans-european-networks-energy

European Commission. (2017g). *Connecting Europe Facility.* Retrieved from https://ec.europa.eu/inea/en/connecting-europe-facility

European Union. (2017). *Regulations, Directives and other acts.* Retrieved from https://europa.eu/european-union/eu-law/legal-acts_en

Hughes, L., De Jong, M., Qin Wang, X. (2016*). A generic method for analysing the risks to energy systems.* Applied Energy. Issue 180

International Energy Agency. (2017). *Glossary.* Retrieved from http://www.iea.org/about/glossary/e/#tabs-2

IRCSG. (2017). *Recommendations and best practices on the protection of electricity, gas and oil critical infrastructure (Critical Energy Infrastructure Protection CEIP).* AC/331-D(2017)0001. NATO. Brussels

IRCSG. (2017a). *Guidance on improving resilience of national and cross-border energy network.* AC/98-D(2017)0005. NATO. Brussels

IRCSG. (2017b). *Evaluation criteria on resilience.* Document PO(2017)0094(INV). NATO. Brussels

NATO. (2016). *Izmir NATO Headquarters Directive 080-02 on the Infrastructure Assessment for Land Operations*. Izmir

Jahier, Khan. (2014). *Critical Infrastructure Protection within NATO*. Civil-Military Planning and Support Section, Operations Division. Retrieved from http://www.cipre-expo.com/wp-content/uploads/2014/02/Khan-Jahier-NATO-CIP-within-NATO.pdf

Johansson, B. (2013). *A broadened typology on energy and security.* Energy. Elsevier

Montanari, L. Querzoni, L. (2014). *Critical Infrastructure Protection: Threats, Attacks and Countermeasures.* Rome: Centre of Cyber Intelligence and Information Security, University of Rome 'La Sapienza'.

Moore, T., Shenoi, S. (2010). *Critical Infrastructure Protection IV: Fourth Annual IFIP WG11.10 International Conference on Critical Infrastructure Protection*. Washington. March 15-17

Månsson, A., Johansson, B., Nilsson, L. J. (2014). *Assessing energy security: An overview of commonly used methodologies.* Energy. Elsevier

NATO. (2004). *NATO's Defence Against Terrorism Programme.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_10/20151029_141007-dat-prog.pdf

NATO. (2008). *Bucharest Summit Declaration.* Retrieved from https://www.nato.int/cps/ua/natohq/official_texts_8443.htm

NATO. (2010). *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North At¬lantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon*

19-20 November 2010. Retrieved from https://www.nato.int/cps/ua/natohq/official_texts_68580.htm

NATO. (2014). *Riga Summit Declaration.* Retrieved from https://www.nato.int/cps/en/natohq/official_texts_37920.htm

NATO. (2016). *NATO's role in energy security.* Retrieved from https://www.nato.int/cps/ic/natohq/topics_49208.htm

NATO. (2017). *Science for Peace and Security.* Retrieved from https://www.nato.int/cps/en/natolive/78209.htm

NATO Energy Security Centre of Excellence. (2016). *About.* Retrieved from https://enseccoe.org/en/about/6

US National Infrastructure Advisory Council. (2009). *Critical Infrastructure Resilience Final Report and Recommendations.* Washington

OECD. (2008). *Protection of 'critical infrastructure' and the role of investment policies relating to national security.* Paris

Official Journal of the European Union. (2008). *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Brussels

Official Journal of the European Union. (2013). *Regulation (EU) No 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC and amending Regulations (EC) No 714/2009 and (EC) 715/2009.* Brussels

Official Journal of the European Union. (2013a). *Regulation (EU) No 549/2013 of the European Parliament and of the Council of 21 May 2013 on the European system of national and regional accounts in the European Union.* Brussels

OSCE. (2013). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.* Vienna

Pursiainen. C. (2009). *The Challenges for European Critical Infrastructure protection.* Journal of European Integration. Issue 31. N.6

United Nations Security Council. (2017). *Physical Protection of Critical Infrastructure Against Terrorist Attacks*. CTED TRENDS REPORT

Yusta, J., Correa, G., Lacal-Arántegui, R. (2011). *Methodologies and applications for critical infrastructure protection: State-of-the-art.* Energy Policy. Issue 39

Witters, L., Marom, R., Steinert, K. (2012). *The Role of Public-Private Partnerships in Driving Innovation.* The Global Innovation Index 2012. WIPO.

Chapter 2
Case studies: Estonia, Italy, Latvia, Lithuania

INTRODUCTION

This chapter illustrates four case studies, namely Estonia, Italy, Latvia and Lithuania in order to provide concrete examples of how critical energy infrastructure is protected in various states. As already stated in the Introduction, Italy is a different case from the other three that are taken into consideration here and that belong to the same geographical area. The reason is that Italy adds value to the analysis for its geopolitical, economic, and historical characteristics.

This chapter is divided into four sections, each of which is dedicated to a case study. Each case study first focuses on an overview of the energy system of the state and then on the main measures adopted to protect critical energy infrastructure. These latter are essentially based on the questionnaires that have been submitted to the energy companies and national authorities of the four states. The first section is dedicated to Estonia that is a special case within the EU because of the predominance of oil shale in its energy sector. The second section focuses on Italy that provides an interesting example of a big state with a huge energy market. The third section analyses the Latvian case showing that it's trying to become more independent from Russia especially through the liberalization of its energy market and through the reinforcement of its connections with Estonia, Lithuania and the other northern states. The fourth section focuses on Lithuania that is making progress in improving its electricity and gas infrastructure.

Estonia

The report of the International Energy Agency of 2013 on Estonia says that "Estonia is unique among European Union (EU) member states in that its

energy sector is dominated by one primary source of energy, oil shale. The country is one of the largest producers of oil shale in the world and its domestic energy sector relies heavily on this source, from which the bulk of its electricity is produced" (International Energy Agency, 2013). Estonia holds significant reserves of oil shale and its industry in the field is the most developed in the world. This provides Estonia with a high degree of energy security. Indeed, Estonia is largely self-sufficient in energy terms. For instance, the use of oil shale reserves for the production of electricity and heat allows Estonia to have a high level of energy autonomy. This is why priority is given to the use of oil shale for electricity and heat generation over the production of more profitable oil shale (International Energy Agency, 2013).

In Estonia there are four companies operating in the sector, namely Eesti Energia, Oil (a subsidiary of Viru Keemia Grupp [VKG]), Narva Oil Plant (Eesti Energia Õlitööstus AS, a subsidiary of Eesti Energia) and Kiviõli Keemiatööstuse OÜ. Among them, Eesti Energia is the largest oil shale processing company in the world, using around 15 Mt of trade oil shale per year in Estonia for electricity and heat generation (International Energy Agency, 2013). Owing to oil shale energy production, Estonia has been the most energy independent state in the European Union in recent years (Eesti Energia, 2017).

There are two oil shale-fired power plants in Estonia. One is the Estonian Power Plant (Eesti Elekrijaam) that is located roughly 20 km west-south-west of Narva and has an installed capacity of 765 MW. The plant was built between 2012 and 2015 (Merko, 2017). The other one is Baltic Power Station (Balti Elektrijaam) and is located 5 kilometres (3 mi) south-west of Narva and was built between 1959 and 1965. It has a design capacity of 1615 MW. They are both owned and operated by AS Narva Elektrijaamad, a subsidiary of Eesti Energia (Global Energy Observation, 2011). These two plants together "provide over 90% of the electricity produced in Estonia, supply heat to the entire city of Narva, and export electricity to the Baltic countries and also to the Nordic countries via the Estlink undersea cable" (Eesti Energia, 2017). However, the most efficient and newest power plant owned by Eesti Energia is Auvere Power Plant that was launched in 2015. It is located near Narva in north-east Estonia close to the Russian border and to the other two plants. It consists of the delivery of a 300 MW steam power plant to Estonian state-owned utility company Eesti Energia, via its subsidiary Narva Elektrijaamad. It was connected to the power transmission network for the first time in May 2015. The new plant supplies the majority of the country's domestic electricity consumption in full compliance with the latest and upcoming stringent EU emission directives (Alstom, 2017). In 2016, the majority of oil shale was consumed in power plants, and over 80% of electricity was generated from oil shale (Statistics Estonia, 2017).

Estonia is interconnected to the EU **electricity market** through the Estlink 1 and Estlink 2 interconnectors with Finland (see Figure 1). These two projects, that connect Estonia with Finland, are included in the priority projects of the European Union and aim to improve cross-border power infrastructure, reduce blackouts and help create more efficient power markets in Europe. Estlink 1, which goes from Harku in Estonia to Espoo in Finland and is 105 km long, was built by ABB Ability group and began operating in 2007 (ABB, 2018). Estlink 2 is the second high voltage direct current (HVDC) connection between Estonia and Finland going from Anttila in Finland to Püssi in Estonia and is 171 km long. It was built by the Estonian and Finnish TSOs Elering and Fingrid. It began operating in 2014. Like EstLink 1, Estlink 2 was acquired by Elering AS and Fingrid Oyj at the end of 2013. Estlink 2 is increasing the security of electricity supply in the Baltic Sea region therefore playing a key role both in the integration of energy markets between the Baltic and the Scandinavian states and in the effective functioning of the EU electricity market (Elering, 2017). These projects are important to desynchronize the Estonian electricity system from the Russian one.

Figure 1 Estlink 1 and Estlink 2
Source: Fingrid
https://www.fingrid.fi/kantaverkko/suunnittelu-ja-rakentaminen/arkisto/estlink-2/

As for the **gas sector**, Estonia has no gas production and it only imports it from Russia and Lithuania. Estonia has two interconnections with the Russian natural gas network (Värska and Narva) and an interconnection with Latvia (Karksi). The Inčukalns natural gas storage facility in Latvia, which is used to supply Estonia in winter, is filled with Russian gas. However, the limited capacity of the connection between Estonia and Latvia creates border bottlenecks. This has a negative impact on the electricity markets of Estonia and other Baltic States (European Commission, 2014a). At the same time, the shale gas revolution in

North America provides very good opportunities to Estonia to diversify its gas supplies (Estonian Ministry of Economic Affairs and Communications, 2017).

The Estonian natural gas market was opened in 2007 but it is just a formal opening as existing legal and functional separation rules have failed to provide the necessary incentives to encourage competition or further developments in the gas market (International Energy Agency, 2013; Estonian Ministry of Economic Affairs and Communications, 2017). The vertically integrated operator Eesti Gaas is a dominant player for both wholesale and retail markets. Eesti Gaas established the independent system operator EG Võrguteenus, which leases Eesti Gaas's assets for the provision of transmission services. Eesti Gaas imports gas from a single supplier, Gazprom, under a long-term contract.[17] Furthermore, "in addition to the potential risk arising from reliance on a single supply source, the Estonian gas network has technical limitations related to the challenge of maintaining the required pressure in the transmission system during the peak load in cold winters and in spring, which can drop below the agreed limit" (International Energy Agency, 2013).

In order to ensure a more efficient development of the gas market, in 2012 the Estonian Parliament amended its Natural Gas Act in force since 2003. This act "provides regulations for all economic activities related to natural gas import, transmission, distribution, sales and connection to networks. These regulations allow for free third-party access and limit the possibility of denying network services to any market participant. (...) The Competition Authority provides the methodology for calculating tariffs for transmission and distribution network services, which are uniformly applied to all network operators regardless of their size" (International Energy Agency, 2013). The Estonian Competition Authority, which regulates both electricity and gas markets, is in charge of implementing state control, supervision and monitoring of the natural gas market. Additionally, in October 2017, the Estonian Government endorsed the national development plan of the energy sector until 2030, according to which Estonia should have a functioning open and free fuel and electricity market and the country's power system should be in the European Union frequency range by 2030. The plan also includes the diversification of energy supplies, the increase of the efficiency of energy consumption and of the share of renewable energy in Estonia's energy supply (The Baltic Course, 2017).

In this context, the Baltic Connector gas pipeline project (see Figure 2), which

[17] "The long-term contract contains clauses regulating gas supply technical conditions (pressure, calorific value, etc.), volumes of supply and storage (annual and monthly), gas storage and transmission charges, gas price calculation issues, conditions of payment, conditions for revisions of contracts when required, other liabilities, etc. (European Commission, 2014a).

is part of the EU PCI, is of utmost importance for Estonia as it will strengthen its energy relations with the other states in the region and contribute to its independence from Russian gas. The main aims of the project are the following: "1) improve regional security of supply by diversifying gas sources; 2) create a framework for market opening and growth and enable the use of alternative sources, such as LNG and biogas; 3) enables the interconnection of the Finnish and Baltic gas markets and their integration with the EU's common energy market" (Baltic Connector, 2017). The total cost of the project is 250 million euro and will receive funds from the EU. The project will comprise the construction of pipelines systems, stations and facilities to connect the existing gas networks in Finland and Estonia. The transmission capacity of the pipeline will be 7.2 million cubic metre (72 GWh) per day. The length of the pipeline will be 21 km. The station is bi-directional, which means that it can deliver gas both ways between Finland and Estonia (Baltic Connector, 2017).

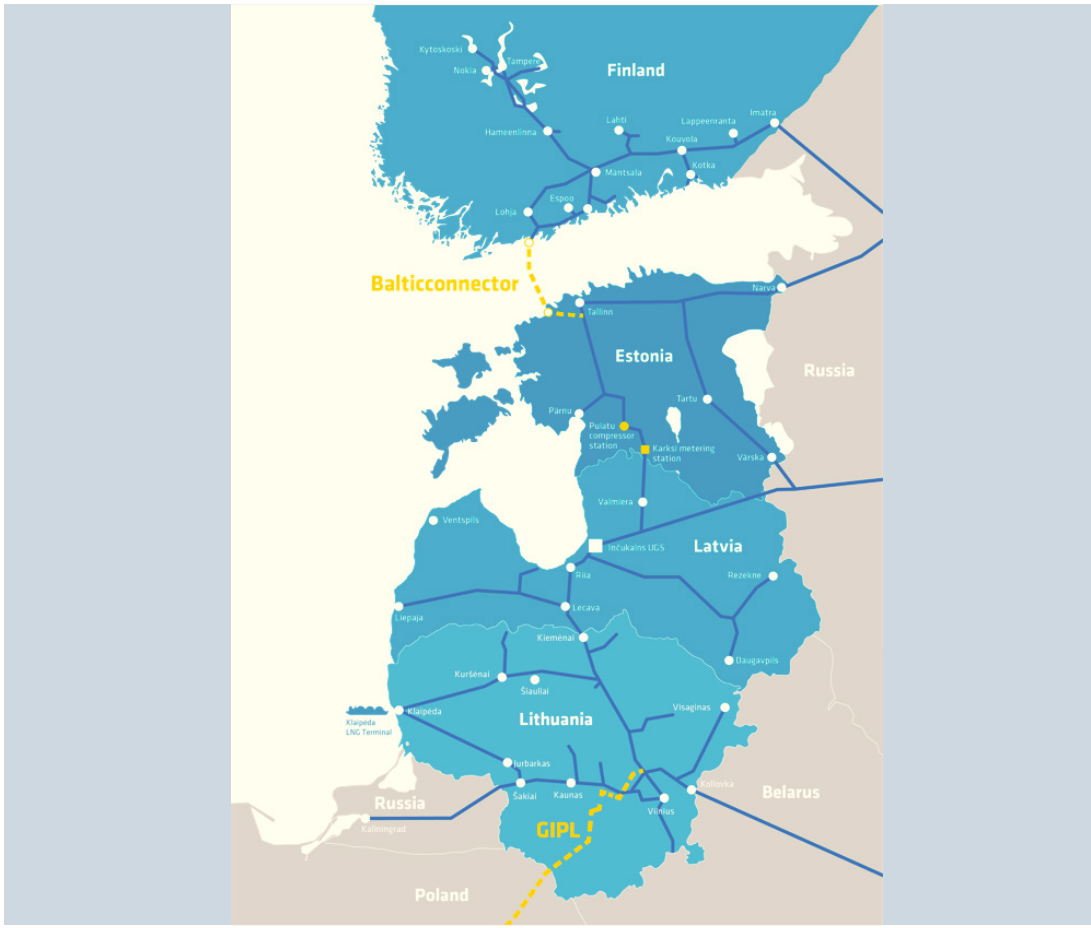

Figure 2. Balticconecctor project and the Estonia-Latvia Interconnection
Source: Elering
http://balticconnector.fi/en/the-project/

Furthermore, another relevant project is the enhancement of the Estonia-Latvia Interconnection that is part of the PCI. It is a bi-directional gas metering station in Karksi (GMS Karksi) and in the Border Valve (BV) near the Estonian-Latvian border and the bi-directional compressor station in Puiatu (CS Puiatu) in South –Estonia. It has daily capacity of 10 MCM/day and allows reverse gas flows. As the European Commission puts it, "the enhancement of Estonia-Latvia interconnection will ensure a more coherent and diverse natural gas transmission network in the Baltic Sea region and further enable the Baltic Connector project". Also, the enhancement will successfully connect the Finnish, Estonian, Latvian and Lithuanian gas markets, link the region to European energy markets via the GIPL interconnection between Lithuania and Poland (discussed below) and will bring an end to the energy island situation in the Eastern Baltic Sea Region (European Commission, 2017a).

As for the **protection of critical energy infrastructure**, Elering OÜ, which was unbundled from Eesti Energia in January 2010, has provided NATO ENSEC COE with answers to the questionnaire. Elering is responsible for planning and managing the system and ensuring the safe and reliable operation of the network. It is also responsible for balancing the electricity system. According to this company, the main threats from which Estonia needs to protect its critical energy infrastructure concern technical failures and difficult weather conditions (e.g. high winds and floods), cyber-attacks and physical attacks. Elering addresses threats in accordance with their nature. For example, the technical equipment of the grid is protected by special protection devices and protection systems. Against intrusions fences are established around Elering´s objects and monitoring devices, IT systems are protected by firewalls and with other IT means, and critical objects like control centres have their own protection design against physical intrusions or attacks. Also, Elering has contracts with security companies. Elering stressed that the main vulnerability of the Estonian critical energy infrastructures concern the possibility of the total collapse of the system. Several successive technological failures can lead to a black-out. This can happen if the control systems fail because of technical reasons or of cyberattacks or if the Supervisory Control and Data Acquisition (SCADA) system, which enables the real-time control over the entire electricity system, is taken over by outside forces.

Elering is one of the main providers and guarantors of the well-functioning of the energy system, which is defined as a vital service by the Estonian law. If the situation worsens, the state institutions intervene. For instance, the Estonian Information System Authority (CERT), that is an organisation responsible for the management of security incidents in computer networks, intervenes in case of serious cyber-attacks. In some other situations, the police or some other

bodies get involved. Furthermore, at the Ministries level and at the governmental level the crisis management teams can intervene. These teams, that consist of ministry officials and representatives of the providers of the vital services like Elering, shall coordinate the crisis management activities in accordance with their competence.

The well-functioning of the vital services is regulated by the State Emergency Law of 1996. According to this law, in case of an emergency "the Prime Minister or, in the event of his or her absence, the minister acting in the powers of Prime Minister shall be the head of state of emergency" (Estonian Parliament, 1996). Also, "the Minister of the Interior or, in the event of his or her absence, the minister acting in the powers of Minister of the Interior shall be the chief of internal defense. The chief of internal defense subordinates to the head of state of emergency and shall lead directly the elimination of a threat to the constitutional order of Estonia" (Estonian Parliament, 1996). Elering stressed that from this law derives the obligation for providers of vital services to conduct a risk assessment and prepare the action plan for assuring the functioning of vital services and for guaranteeing that the obligations contained in the action plan are properly fulfilled by the Ministry of the Interior. Indeed, in addition to conducting risk assessments and preparing action plans for assuring the functioning of vital services (both in the electricity and the gas sectors), Elering prepares restoration plans in case of a black out and defence plans in case of other events. Also, Elering conducts regular internal trainings, trainings with other Baltic Transmission System Operators and with service providers (for instance with companies who have contracts for grid maintenance). It takes part in trainings organised by state institutions.

Furthermore, Elering stressed that there are essentially two critical factors in its operations to protect critical energy infrastructure, namely the functioning of the transmission grids (cross-border connections included) and the success of real-time operations.

Italy

In 2013, the Italian Government drew up a **National Energy Strategy (NES)** in order to define the main goals to achieve in the field of energy by establishing the priorities of action and the most important decisions to be taken (Ministry of Economic Development, 2013). The main goals are essentially four: 1) significantly reduce the energy cost gap for consumers and businesses in order to bring prices and costs in line with European levels by 2020 and to ensure that the longer-term energy transition (2030-2050) will not negatively affect the Italian and the European industrial competitiveness; 2) achieve and exceed the

environmental and decarbonisation targets established by the European Union's 2020 Climate and Energy Package (known as the "20-20-20" package)[18]; 3) continue to improve Italy's security of supply, especially in the gas sector, and reduce its dependence on energy imports that costs 62 billion annually and exposes Italy to volatility and price risks; 4) foster sustainable economic growth by developing the energy sector (Ministry of Economic Development, 2013).

Among the seven priorities of actions[19] established by NES, two are relevant to the aims of this study. The first one is the creation of a competitive gas market and of a Hub Southern Europe. For Italy creating a competitive gas market that is fully integrated with the one of the other European states is a priority. For this reason, the alignment of the gas prices with those of the other EU members is essential. More competitive gas prices, indeed, would make Italy a state of exchange and/or transit to Northern Europe. This can happen by strengthening the energy infrastructure, which is an opportunity for Italy to become an important crossroads for the entry of gas to the EU from the South. Additionally, strengthening energy infrastructure also serves the aim of the Commission to ensure that all connection and storage infrastructures are completed by 2020 in order to create an integrated energy market and increase energy security. Indeed, "the European Council of 4 February 2011 underlined the need to modernise and expand Europe's energy infrastructure and to interconnect networks across borders, in order to make solidarity between Member States operational, to provide for alternative supply or transit routes and sources of energy and to develop renewable energy sources in competition with traditional sources" (Official Journal of the European Union, 2013). Additionally, Regulation No 347/2013 stresses that "energy storage facilities and reception, storage and regasification or decompression facilities for liquefied natural gas (LNG) and compressed natural gas (CNG) have an increasingly important role to play in the European energy infrastructure. The expansion of such energy infrastructure facilities forms an important component of a well-functioning network infrastructure" (Official Journal of the European Union, 2013).

In this context, the nine priority corridors and the three areas of interest identified in the Commission's *Guidelines for Trans-European Energy Infrastructure* of

[18] The 2020 package, whose targets were set by the EU leaders in 2007, "is a set of binding legislation to ensure the EU meets its climate and energy targets for the year 2020". It sets three key targets: 1) 20% cut in greenhouse gas emissions (from 1990 levels); 2) 20% of EU energy from renewables; 3) 20% improvement in energy efficiency. (European Commission, 2017g)

[19] The seven priorities of action identified by SEN are the following: 1) energy efficiency; 2) competitive gas market and Hub Southern Europe; 3) sustainable development of renewable energy; 4) development of electricity infrastructure and the electricity market; 5) restructuring the refining industry and the fuel redistribution sector; 6) sustainable production of domestic hydrocarbons; 7) modernization of the system governance. (Ministry of Economic Development, 2013)

2011 are of utmost importance to the EU in order to achieve its energy policy and climate objectives, namely affordable, secure and sustainable energy for all citizens, and the long-term decarbonisation of the economy in accordance with the Paris Agreement (European Commission, 2017c). The nine priority corridors and the three areas cover the electricity and gas transmission and storage networks, oil pipelines, smart grids and networks for CO2 transportation and re-injection. Italy is touched by five of the corridors and by three priority thematic areas. As for the electricity sector, Italy is touched by two corridors. The first one is the North-South Initiative West Electricity (NSI West Electricity) corridor, which interconnects the member states of the region (Belgium, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Malta, Portugal, Spain, the United Kingdom) with Mediterranean third countries in order to integrate electricity from renewable energy sources. The second corridor is the North-South Initiative East Electricity (NSI East Electricity) corridor, which is constituted of interconnections and internal lines in North-South and East-West directions to complete the internal market and integrate generation from renewable energy sources. As for the gas sector, Italy is touched by three corridors. The first one is the North-South gas interconnections in Western Europe (NSI West Gas) corridor, which are interconnection capacities for North-South gas flows in Western Europe (Belgium, France, Germany, Ireland, Italy, Luxembourg, Malta, the Netherlands, Portugal, Spain, the United Kingdom) to further diversify routes of supply and increase short-term gas deliverability. The second corridor is the North-South gas interconnections in Central Eastern and South Eastern Europe (NSI East Gas) that are regional gas connections between the Baltic Sea region, the Adriatic and Aegean Seas and the Black Sea (Austria, Bulgaria, Cyprus, Czech Republic, Germany, Greece, Hungary, Italy, Poland, Romania, Slovakia, Slovenia) whose aim is to enhance diversification and security of gas supply. The third corridor is the Southern Gas Corridor (SGC- see Figure 3), which is a transmission of gas from the Caspian Basin, Central Asia, the Middle East and the Eastern Mediterranean Basin to the European Union to enhance the diversification of gas supply (European Commission, 2011; International Network for Sustainable Energy, 2014). The SGC, which is one of the most complex gas value chains ever developed in the world, is particularly important not only because it contributes to the EU diversification policy but also because of its geopolitical implications. On the one hand, the SGC will contribute to satisfy the EU need of gas that is expected to grow in the future. Europe's dependence on gas import is expected to grow in the long run from the current 64% to above 80%. On the other hand, the SGC will erode the EU's dependence on Russian gas and will be essential to stabilize a volatile region (Koranyi, 2017). The SGC stretches over 3,500 kilometres and is comprised of several energy projects, namely:

1. the Shah Deniz 2 development, drilling wells and producing gas offshore in the Caspian Sea;
2. the expansion of the natural gas processing plant at the Sangachal Terminal on the Caspian Sea coast in Azerbaijan;
3. three pipeline projects: South Caucasus Pipeline (SCPX) – Azerbaijan, Georgia, Trans Anatolian Pipeline (TANAP) – Turkey, and Trans Adriatic Pipeline (TAP) – Greece, Albania, Italy;
4. the expansion of the Italian gas transmission network;
5. possibilities for further connection to gas networks in South Eastern, Central and Western Europe (Trans-Adriatic Pipeline, 2017).

Figure 3. Southern Gas Corridor
Source: Trans-Adriatic Pipeline
https://www.tap-ag.com/the-pipeline/the-big-picture/southern-gas-corridor

The SGC is "a major component of the EU energy policy" (Trans-Adriatic Pipeline, 2017). In this context, TAP, which is due for completion in 2019, plays a key role in realising the EU's main goals in the energy sector not only by providing economic benefits to the member states but also by ensuring that "one of the continent's vital energy routes remains viable for decades to come" (Trans-Adriatic Pipeline, 2017). TAP's initial capacity is 10 billion cubic metres of gas per year but the addition of two compressor stations could increase its capacity up to 20 billion cubic metres per year. Additionally, TAP will also have the 'physical reverse flow' feature that will allow divert gas from Italy to South East Europe if energy supplies are disrupted (Trans-Adriatic Pipeline, 2017). The first gas sales to the EU through TAP are scheduled for 2020 (International Energy Agency, 2016). Although Italy is largely dependent on Russian natural gas (indeed Italy imports 35% of its natural gas from Russia) (Rosato, 2016), it has the highest degree of diversification of gas supply routes and sources in the EU.

As for the **gas transmission network**, gas transmission activities are carried out by Snam Rete Gas S.p.A., Società Gasdotti Italia S.p.A., Edison Stoccaggio S.p.A. and a small number of companies operating at regional or local level. However, the main gas transmission company is Snam Rete Gas that owns and operates approximately 95% of the natural gas transmission network in Italy.[20] Italy has eight entry points of the National Network for natural gas coming from abroad: Tarvisio, Gorizia, Passo Gries, Mazara del Vallo, Gela, as well as the LNG terminals in Panigaglia, Rovigo (Cavarzere) and Livorno (OLT). Snam Rete Gas has adopted a network development plan for the 2015-2018 period for the Italian domestic market that amounts to investments of 5.1 billion euro. The aim of these investments is twofold. On the one hand, they are aimed at enhancing security of supply and the flexibility of the system. On the other hand, they are aimed at supporting gas flows towards the European markets in order to realise an effective interconnection with the continental networks (International Energy Agency, 2016). As for the transmission, the main elements of the 2015-2018 plan are the following: «a) development of infrastructure in the Po Valley, with the aim of increasing transport capacity in the north of the country, while at the same time making physical export to northern Europe possible; b) increasing liquidity in domestic and European markets, by making new integrated services, among other things, available to shippers; c) investing in the Italian domestic network to increase flexibility and interconnections with the regional network» (International Energy Agency, 2016). Additionally, the 2015-2018 plan envisages an extension of the 32 306 km gas network by about 1000 km. The autorisation of the Ministry of Economic Development is necessary in order to build new transmission pipelines for the National Transport Network (NTN) as well as by the regions for the Regional Transport Network (RTN). Also, the autorisation is granted by the Ministry of Economic Development only for infrastructure included in the NTN by a unified procedure, including the environmental impact assessment and a declaration of public interest (International Energy Agency, 2016).

As for the **electricity sector**, Italy, which is a net importer, has continued to make progress in terms of market liberalisation and infrastructure development. The national transmission system operator is Terna that was established as such in 2005 when it was fully unbundled from Enel. It manages the largest high-voltage network in Europe, with more than 63 500 km of transmission lines. As it is the only Italian transmission system operator, it owns the entire high-voltage network and is the single buyer for generation dispatching sevices. Therefore,

[20] **In January 2012, the company changed its name from Snam Rete Gas to Snam and conferred the transmission, dispatching, remote control and gas metering businesses to a new company Snam Rete Gas. (international Energy Agency, 2016)**

Terna has sole responsibility for the transmission system, while the distribution networks are controlled by Enel and various other market participants. Terna has upgraded its transmission system over the last five years in order to reduce congestion especially for two reasons, namely the significant transmission constraints between northern and southern Italy and the lack of connectivity to the two main islands, Sicily and Sardinia. Additionally, grid improvements have reversed the general flow of electricity from its historical north-south direction, to a south-north flow (International Energy Agency, 2016).

Furthermore, here it is worth mentioning the biennial ten-year network development plan (TYNDP) that was delivered by the European Network of Transmission System Operators for Electricity (ENTSO-E). The «purpose of the TYNDP is to identify gaps in infrastructure from a broader European perspective and to inform decision makers in EU member states and other stakeholders about projects with a network-wide impact». The TYNDP builds on national and regional investment plans. ENTSO-E has formed six regional groups to identify and address network investment and development challenges reflecting regional particularities and needs. Italy is part of two groups, namely the Continental Central South (CCS) Regional Group and the Continental South East (CSE) Regional Group.[21] Additionally, TYNDP identifies about 100 locations on the European grid where bottlenecks exist or can develop if reinforcement solutions are not implemented. ENTSO-E has identified the northern borders of Italy and the boundary between Italy and Greece and the Balkans area as transmission bottlenecks. Internal bottlenecks are also observed in Italy with regard to market integration. The CCS-TYNDP identifies Italy-France interconnection, three Italy-Austria interconnections, the interconnection between Italy and the Balkans area, two Italy-Switzerland interconnections, Austria-Germany interconnection and two Italy-Slovenia interconnections as PCIs. The CSE-TYNDP identifies investments at France-Italy (one project), Austria-Italy (three projects), Italy-Montenegro (one project), Italy- Switzerland (two projects), and Italy-Slovenia (two projects) as PCIs (International Energy Agency, 2016).

Also, Italy has installed smart grids extensively in homes and businesses throughout the country. These smart meters include a wide variety of technologies and can be put to many uses, including remote metering, outage monitoring, fraud detection, retail-provider switching, electric vehicle charging, and variable renewables integration. The smart grids were deployed by Enel distribuzione, the second largest distribution company in Europe, but also by

[21] The Continental Central South (CCS) Regional Group also includes Austria, France, Germany, Slovenia and Switzerland. The Continental South East (CSE) Regional Group also includes Greece, Hungary, Romania, Slovenia and the Balkans (Albania, Bosnia-Herzegovina, Bulgaria, the Former Yugoslav Republic of Macedonia, Montenegro and Serbia. (International Energy Agency, 2016)

Terna at transmission level to help manage energy flows, help with real-time system optimization, perform real-time system monitoring, and predict variable renewable generation.

In case of an emergency, the Italian Grid Code is applied. This document "was drawn up in compliance with the provisions stated Prime Minister decree dated May 11, 2004 regarding unification between ownership and management of the grid and on the basis of the directives of the Authority for the Electricity and Gas as stated in resolution n.250/04" (Terna, 2017). The Grid Code was positively verified by the Authority for the Electricity and Gas with resolutions n. 79/05 and 49/06 and by the Ministry of Productive Activities. It is submitted to a continuous updating process according to the procedures that it establishes (Terna, 2017). In particular, when an emergency occurs, chapter 10 of the code, known as the Defense Plan, is designed to deal with multiple contingencies which can lead to a system cascading effect or emergency/interruption conditions in order to avoid the partial or total collapse of the system (International Energy Agency, 2016).

In the electricity sector, the main authorities responsible of the well-functioning of the system are the following : a) the Ministry of the Economic Development (MSE) that is responsible for the policy development in a number of sectors such as energy and mineral resources, economic development and cohesion, telecommunications and internationalisation and business incentives ; b) the Regulatory Authority for Electricity Gas and Water (AEEGSI) that is an independent regulatory body regulating and overseeing the electricity and natural gas sectors. It has been attributed new regulatory duties in the water and in the district heating sectors with the liberalisation. AEEGSI has a high degree of autonomy from the government and is funded by means of annual contributions paid by the service providers ; c) the Competition Authority (AGCM) that is an independent competition body that enforces rules against anticompetitive agreements among undertakings, abuses of dominant position as well as mergers and acquisitions, joint ventures) which may create or strengthen dominant positions detrimental to competition; d) Gestore dei Sistemi Energetici (GSE) that is the state-owned company which promotes and supports renewable energy sources in Italy; e) Gestore dei Mercati Energetici (GME) is a company established by GSE to organise and economically manage the electricity market in a neutral, transparent, objective manner; f) Acquirente Unico (AU) that is a subisidiary of GSE and it has the mission of procuring continuous, secure, efficient and reasonably priced electricity supply for households and small businesses. It "buys electricity in the market on the most favourable terms available and resells it, in accordance with directions given by AEEGSI, to distributors or retailers active in the standard offer market *(mercato di maggior tutela)* for supply to small

consumers who choose not to switch to the competitive market" (International Energy Agency, 2016).

Regarding the **oil sector**, oil share has been falling over the last decade although it still is one of the largest energy component in primary energy supply. In Italy there are 12 major refineries (as of 1 January 2014) of which nine are located along the coast and are supplied by sea, and three in the Po Valley in northern Italy and are supplied by pipelines from Genoa and Vado Ligure. Also, Italy has two major international crude oil pipelines. The first one is the Central European Line (CEL) from Genoa, with a 1 million barrels/day (mb/d) capacity, which supplies inland refineries in northern Italy and the Collombey refinery in Switzerland. The second pipeline is the Trans-Alpine Pipeline (TAL) from Trieste (850 kb/d capacity) that supplies Germany, Austria and the Czech Republic. Most refineries are located on the Mediterranean coasts. Italy has 16 crude oil tanker ports, four of which (Taranto, Milazzo, Falconara (Ancona) and Augusta (Santa Panagia)) can receive cargo ships up to 300 000 dead weight tonnes (International Energy Agency, 2016).

It is important to note that the government has stressed that the oil sector needs to be modernised in order to become more competitive and more efficient. In particular, the fuel distribution system suffers from major structural problems. In fact, the distribution network is extremely fragmented with high numbers of filling stations, which makes the protection of the infrastructure more difficult.

Regarding the **protection of critical energy infrastructure**, Terna, Ente Nazionale Idrocarburi (ENI) and Snam have provided NATO ENSEC COE with answers to the questionnaire. Terna, an electricity transmission system operator, has stressed that the Information and Communication Technology (ICT) systems can be considered as the main vulnerabilities of critical energy infrastructure and that cyber-attacks are the most serious threats. Terna has its own policies to face this kind of threats, which define the main security objectives and the miminum requirements for the protection of the Information and Communication Technology (ICT) assets. This is linked to the Information Security that defines the policies and the models for the Information Risk Management, while the implementation of these models is assigned to the owners of the assets (e.g. information systems). The Security Operation Centre is in charge of the coordination and of the real time/near real time of threats and of the security measures. It also deals with the management of negative events.

Regarding the management of emergency and crises security situations (e.g. sabotages, attacks, political instabilities), ENI, an Italian multinational oil and gas company, implements its Security Plans that are decided by ENI's higher

hierarchies. Among the main aims of the Security Plan there are: 1) definition of roles, responsibilities and necessary measures for the management of risks; 2) control of the events jeopardizing the security in order to minimise their effects; 3) definition of the measures to the reactivation of the activities after overcoming an emergency. The way emergencies are managed varies case by case. ENI categorizes the seriousness of an event according to four levels: a) first level-when an emergency can be managed locally by ENI; b) second level-when an emergency can be managed locally by ENI with the assistance of personal and means of the local public administration; c) when an emergency that concerns several companies management requires the involvement of the public administration at the state level; 4) crisis. Furthermore, ENI's Security Plans define how the activities of the company should be coordinated with the ones of the public authorities according to the kind of emergency. In the case of local emergencies, ENI's highest hierarchies coordinate the operations with the local authorities that are supported by the security managers (that have the necessary powers to properly interact with the public authorities). If the emergency concerns higher levels, ENI's central security coordinates their operations with the state authorities. The central security defines the general criteria and the methodologies to identify threats and to evaluate security risks. It defines the guidelines, the coordination of and the control on the implementation of the activities aiming at managing the security risks. Cooperation between ENI and the public authorities are essentially: 1) cooperation defined by formal agreements aimed at sharing information, analyses, and early warnings. These agreements are also aimed at integrating monitoring and security devices, people protection devices, infrastructure and the company's interests in a broad sense, both physical and cyber related; 2) cooperation that is not defined by formal agreements: this kind of cooperation, which is developed according to the respective institutional/private competencies, can be continuous or can concern particular cases. This kind of cooperation is usually concerned with the implementation of security measures, prevention of - or response to - security emergencies problems, information sharing on security phenomena. Among the main kinds of PPPs involving ministries, police forces and security forces in Italy there are the following: a) the Convention with the National Centre to Protect Critical infrastructure from IT crimes-CNAIPIC (depending on the Police Service for Post and Communication, which was agreed upon in 2014 with the aim to fight against terrorist and criminal IT attacks that could damage ENI's critical infrastructure (in particular those networks related to the distribution of energy resources). This mainly happens through coordinated intervention procedures and information sharing. The Convention was agreed upon according to the decree of the Ministry of the Interior of 9th January 2008 that identifies the digitalized critical infrastructure of national interest, which are those digitalized systems that are managed by private or public bodies and that

control the critical sectors for the functioning of the state; b) the coordination with the Intelligence System for the Security of the Republic of the Ministry of the Interior of: 1) relations of cooperation in the field of cyber intelligence in order to prevent cyber threats; 2) information sharing, bilateral meetings for specific needs and periodical operational meetings in the context of the Enterprises Technical Table. This latter has been established in the context of the so called DIS, the department that coordinates the intelligence activities and deals with cyber security. The importance of DIS is also stressed by Snam; c) agreement for the cooperation with the military navy; according to this agreement, ENI can benefit of the enhancement of the monitoring in the Libian area and in other areas where the military navy is present; d) consolidated cooperation with the Ministry of the Interior and with the local authorities such as prefectures and police headquarters. These relations concern the defense from several kinds of crimes and the prevention against terrorism in order to protect people and the management of infrastreucture security. In this context, the following kinds of cooperation are included: 1) cooperation aimed at the security of oil pipelines including the protection of people and economic and environmental protection. Over the last few years, ENI has enhanced its relations with the Ministry of the Interior in order to identify the best strategies to protect oil pipelines. ENI has participated in many Provincial Committees for the Order and the Security, that is indicated also by Snam, a natural gas infrastructure company, as the main local body dealing with critical infrastructure protection, and has provided the map of oil pipelines to the Police, and in the Criminalpol context, ENI has requested a criminal law for energy infrastructure which includes more sever norms in the case of environmental disaster; 2) information sharing in the case of public protests or anarchical insurrections threats that might jeopardize the security and the operational continuity of infrastructures. Furthermore, in relation to the activities with strategic relevance, Law 11th May 2012 has modified the Italian law conerning the special powers of the state in agreement with the European law. This has determined the transition from the golden share (a parcel of shares of the government that gives the state special powers with the aim of protecting the interests of people in the strategic enterprises) to the golden powers. This means that the state has the necessary powers to intervene in the case of extraordinary operations involving enterprises operating in strategic sectors envisaged by the law mentioned above. These special powers can be applied to enterprises owing assets of strategic importance for the national interest. ENI is subject to the golden powers principle. This gives the state a veto power (or the power to impose certain conditions) in the case of the operations concerning strategic assets that can jeopardize the public interests concerning the security of energy networks. Also, according to the golden powers principle, the state has the power to oppose to the acquisition of a part of an enterprise owing strategic assets by an enterprise external to the EU if this acquisition

might jeopardize the interests of the state.

Furthermore, Snam stressed in the questionnaire that in case of natural catastrophes it is up to the Civil Protection body to intervene, but that a catalogue of countermeasures does not exist. These latter vary according to the infrastructure at stake, of its strategic relevance and on the consequences that this could have on the normal functioning of the infrastructure. Also, every prefecture (at the local level) has its own plan against terrorist threats.

Another element that is necessary to mention is that according to Terna the most critical operations concern cyber security. In this field, the Computer Emergency Response Team (CERT) Italy participates in Cyber Europe exercises that organized by ENISA, the European Union Agency for Network and Information Security.[22] CERT also organizes Cyber Italy exercises that are based on simulations concerning crisis scenarios at the national level in order to test the response capabilities of enterprises.

In short, Italy is a good example of a big country with a huge market. Its companies have established quite close links with the public authorities in order to deal with the protection of critical energy infrastructure. However, in spite of the fact that Italy has been conducting an overhaul in the field of public policy since 2008, there is still room for improvement, as it is stressed by a report issued by the Ministry of Economics and Finance in 2015. This concerns in particular the necessity of clear and sound rules that should be put in place to remove obstacles, particularly with regard to the greater involvement of private capital in funding PPP projects. Also, frequent changes in legislation as well as legislative bills issued but still not enforced should be avoided and the regulatory framework should be improved by simplifying PPP approval procedures. The report stresses that at present it takes too long to award contracts. In many cases, this is due to the complexity of procedures (Italian Ministry of the Economy and of Finance, 2015).

Latvia

In April 2017, Latvia opened its **gas market** to competition after that Saeima, Latvia's Parliament, passed amendments to the energy law in order to open up Latvian gas market to external suppliers, including the Lithuanian LNG terminal in Klaipeda (DELFI, 2018). The importance of this latter for the

[22] The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. The Agency is located in Greece with its seat in Heraklion Crete and an operational office in Athens. (ENISA, 2018)

liberalization of the Latvian gas market was also recognized by the European Commission in its *Assessment of country performance and opportunities from the Energy Union* of 2016 and by Mr Jerzy Buzek, Chair of the ITRE Committee (The Committee on Industry, Research and Energy of the European Parliament) and former Chair of EP. He said that "it is exactly one year ago that a predominance of Gazprom ended in the Baltic States – LNG terminal opened roads to all gas markets in the world. It is true that this type of project that every country can implement by oneself, thought general aim has to be – creating a common gas market by the Baltic States, which let consumers to win" (Latvian Ministry of Energy, 2015). Also, the liberalization of the Latvian gas market "is part of a wider effort to develop diversified and secure gas markets in the Baltic countries integrated with the gas infrastructure and markets of other EU countries, and with reduced dependence on energy sources from Russia" (European Commission, 2017c). Before the liberalization of its energy market, Latvia was the only EU state entirely dependent on Russian gas imports. However, in spite of the fact that Latvia is breaking free from Moscow, the private firm Latvijas Gāze, which controls the gas flow of the country, is owned by Gazprom for 34%. Gazprom has a contract with Latvijas Gāze to exclusively supply it until 2030 despite the liberalisation of the Latvian gas market. This contract will make enter the Latvian energy market more difficult to smaller companies (El Pais, 2017).

In Latvia, infrastructures and pipelines are managed by JSC Conexus Baltic Grid that is the only natural gas transmission and storage operator in the country. The company, which owns 1191 km of gas transmission pipelines, ensures the transmission and storage of natural gas for customers in Latvia, Estonia, Russia, and Lithuania. The entire transmission system has been entirely upgraded since 1991 and gas pipelines undergo regular internal diagnostics (JSC Conexus Baltic Grid, 2017). In this context, the Latvian-Lithuanian interconnection is particularly important not only for Latvia but for the whole Baltic Sea region because it will contribute to increase the security of supply in the region and will provide a well-functioning and competitive energy market in the Baltic States. The project is aimed at increasing the interconnection capacity between Latvia and Lithuania and on the Latvian side includes the construction of the Riga-Iecava pipeline and the replacement of the existing Iecava-Lithuanian pipeline. The project, whose completion depends on the GIPL project (that is discussed in the section on Lithuania) and on the LNG terminal in Klaipeda (that is now completed), is expected to be completed in 2020 and is included in the Latvian and European transmission system development plans (JSC Conexus Baltic Grid, 2017). Also, the gas pipeline going from the Lithuanian border to Iecava is the oldest Latvian gas pipeline, it is in poor conditions. As the construction of the new pipeline is of

utmost importance for the whole region, it is essential not only to upgrade it but also to increase its capacity.

Furthermore, the expansion of the Inčukalns Underground Gas Storage (UGS) (see Figure 4) Facility is also of utmost importance. It is the only underground gas-storage facility in the Baltic Sea region. For this reason, it is considered a 'national treasure' (El Pais, 2017). It ensures the stability of regional natural gas supply. During summer, when the consumption of natural gas is much lower than in winter, natural gas is injected into the storage facility so as to be available for supply during the heating season to customers in Latvia, Estonia, north-western Russia, and Lithuania (JSC Conexus Baltic Grid, 2017). The UGS Facility is included in the EU PCI.

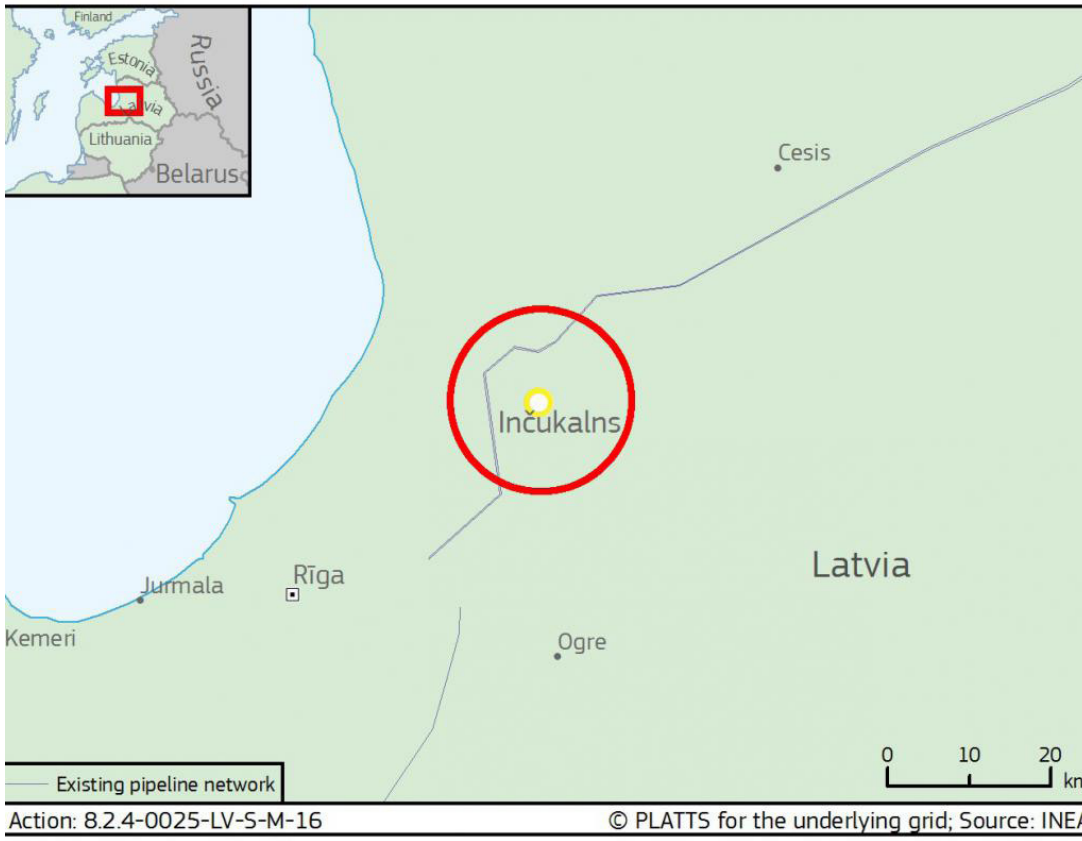

Figure 4. Inčukalns Underground Gas Storage (UGS) Facility
Source: European Commission
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-energy/projects-by-country/latvia/8.2.4-0025-lv-s-m-16-%C2%A0

The modernization of the facility will occur in three stages. The first one (2014-2018) includes the reconstruction of wells, collection points, compressors and installation of a new compressor. This will result in an improved safety of the

facility and in an increase of the parameters of natural gas extraction from 30 million m3 per day to 32 million m3 per day. During the second stage (2019-2020), the parameters of natural gas extraction will be increased to 35 million m3 per day. The third stage will include the further reconstruction of the infrastructure and the expansion of the facility from the present active natural gas volume of 2.3 billion m3 to 2.8 billion m3. The expansion will entirely depend on the development of regional infrastructure objects and the requests of companies from the neighbouring states. Such project requires the financial participation of the EU and of the neighbouring states because of the need to purchase cushion gas. The total estimated cost of the project is 376,5 million euro (Latvijas Gāze, 2017). Lithuania has considered building its own storage but it has decided to leave the Latvian one as the best option because of the too high estimated costs of around 361 million dollars (Reuters, 2014).

As for the **electricity sector**, the electricity market in Latvia is led by transmission operator Augstsprieguma tīkls and the Scandinavian electricity exchange Nord Pool Spot AS. Augstsprieguma tīkls is an independent Transmission System Operator that ensures the security of the electric power supply in Latvia, provides power transmission services and free third-party access to the transmission network, and secure the interconnection with neighbouring power systems. In 2013, Latvia joined Nord Pool Spot AS that is an electricity bidding area in Latvia where it is possible to buy and sell electricity through offers and demands (Augstsprieguma tīkls, 2017). The largest electricity producer is the state-owned company Latvenergo whose overall strategic goal is "to provide in a sustainable, responsible and economically sound manner energy sector goods and services important for the competitiveness and growth of the national economy, and efficiently manage the resources and infrastructure of strategic importance for national development and security, contributed to increased reliability of energy supply" (Latvenergo, 2017). In 2013 Latvenergo launched the the second power generating unit of the gas-fired power plant TEC-2 near Riga. TEC-2 is a combined heat and power (CHP) plant with the largest power generation capacity in Latvia. The plant has now been fully reconstructed after the first unit was launched in 2009 (Nordic Investment Bank, 2013).

Latvia began the liberalisation of its electricity market in 2007 when, in accordance with Directive 2003/54/EC of the European Parliament and of Council of 26 June 2003 concerning common rules for the internal market in electricity, Latvia passed a law stipulating that all electricity final consumers, which have a connection to the power grid, have the right to change their electricity supplier without any limits. In addition, the Electricity Market Law of 2005 already stated the necessity of promoting energy independence by ensuring different suppliers of energy resources necessary for production of electricity

(Latvian Parliament, 2005). The electricity market opening in Latvia, which was completed in 2015, strengthens the single EU electricity market. In this way, it contributes to Latvia's power supply security and energy independence in the future (Bride and Zvaigzne, 2017). It is necessary to stress here that Latvia imports electricity basically from Estonia and Russia (Nordic Investment Bank, 2013).

As for the **oil sector**, Latvia officially does not produce it but does it only for research purposes.

In general, it is possible to state that the main aim of Latvian energy policy is to increase energy security by encouraging diversification of supplies of the primary energy resources, by creating the necessary conditions for increasing subsistence of electric energy generation, and by preventing isolation of the regional electric energy market through new interconnections.

In this context, the Baltic Energy Market Interconnection Plan (BEMIP- see Figu-re 5)[23], whose primary objective is to create an open and integrated regional energy market in electricity and gas between member states in the Baltic Sea region, is of utmost importance to Latvia. Indeed, the Informative Report Long-Term Energy Strategy of Latvia 2030 - Competitive Energy for the Society stresses that for Latvia it is essential "to continue close cooperation with regional partners within the framework of the Baltic Energy Market Interconnection Plan (BEMIP) and Connecting Europe Facility (CEF), based on solidarity and mutual financial support principles, and balancing national and regional interests for mutually beneficial solutions (e.g. the development of natural gas supply and storage infrastructure)" (Latvian Government, 2014). The Strategy also emphasizes that "increasing the security of energy supply is a sub-objective aimed at affordable and stable energy supplies to energy consumers, through reducing geopolitical risks, diversifying supply routes, developing energy infrastructure, setting aside reserves, and engaging in the improvement of the international regulatory framework" (Latvian Government, 2014).

[23] In 2009, the President of the European Commission and the political leaders of the eight participating EU countries (Denmark, Germany, Estonia, Latvia, Lithuania, Poland, Finland, and Sweden; Norway participates as an observer) signed a Memorandum of Understanding on BEMIP. The BEMIP initiative was later launched by the European Commission at the BEMIP High Level Group in 2014, while the Declaration on Energy Security of Supply was signed by the Energy Ministers of the Baltic States (Estonia, Latvia and Lithuania) in 2015. The current Action Plan defines the necessary actions to be implemented mainly in the areas of energy infrastructure, gas and electricity markets, power generation, security of energy supply, energy efficiency and renewable energy. During the last few years, the three Baltic States have achieved a good level of interconnection. In spite of this, their electricity grid still operates in a synchronous way with the Russian and Belarusian systems. For this reason, a BEMIP Working Group is working on this issue in order to synchronize the Baltic States' grid with the continental European continent by 2025. This project remains the main challenge in the region for the next few years. (European Commission, 2017f)

Figure 5. Baltic Energy Market Interconnection Plan
Source: Wind Power
https://www.windpowermonthly.com/article/1050607/uk-government-backs-supergrid

As for the **protection of critical energy infrastructure**, the Ministry of Economics has provided with some information on this topic. Like in other states, Latvia needs to protect its critical energy infrastructure from threats like natural disasters, sabotage, terrorism, cyber-attacks, military assaults. Natural disasters, which in the case of Latvia are strong storms, snowstorms, heavy cold weather and floods, and cyber-attacks are the main vulnerabilities of critical energy infrastructures. In order to protect them, the state has a regulatory framework containing a list of critical infrastructures divided into categories in order of strategic importance. Energy companies also have their own plans. The bodies involved in the protection process are the Ministry of the Interior (that is the responsible body for updating the list of critical infrastructure objects), Security Police, the Constitutional Protection Bureau, the Military Intelligence and Security Service, the Ministry of Defence, the Ministry of Economics, the Information Technology Security Incident Institution. The procedures to protect critical infrastructures are laid down in the Cabinet Regulation No. 496 Adopted on 1st June, 2010 - "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures". It contains legal norms arising from Directive 2008/114/EC. This Regulation "prescribes the procedures for the identification of critical

infrastructures, including European critical infrastructures, and planning and implementation of security measures" (Republic of Latvia, 2010). It stipulates that the Commission of Intermediary Institutions for State Security, which is an advisory collegial body, "evaluates and improves the critical infrastructures, including European critical infrastructures, the aggregate of systems and security measures" (Republic of Latvia, 2010). The Commission evaluates the proposals of the responsible sectoral ministries or members of the Commission regarding the determination of critical infrastructures. After that, it prepares its proposals to the Ministry of the Interior regarding the determination of an individual critical infrastructure as the European critical infrastructure and of the necessity of informing the European Commission and the other EU member states. Also, every two years, it prepares information for the European Commission regarding the types of risks, threats and vulnerabilities in each European critical infrastructure sector and submit it to the Cabinet for approval on the basis of the report by the Security Police, the Constitution Protection Bureau and the Military Intelligence and Security Service. The Commission has also the right to request and receive free of charge the information necessary to the work of the Commission regarding critical infrastructures, including European critical infrastructures, from State and local government institutions, as well as from private individuals. Additionally, as for the identification of critical infrastructures, the responsible sectoral ministries, the Security Police, the Constitution Protection Bureau and the Military Intelligence and Security Service are in charge of identifying the possible critical infrastructure, of submitting proposals to the Commission regarding inclusion thereof in the aggregate of critical infrastructures and of identifying the possible European critical infrastructure and submitting proposals to the Commission regarding the determination thereof as a European critical infrastructure (Republic of Latvia, 2010). The regulation also states that "a critical infrastructure may be recognised as a European critical infrastructure, if disruption to the activity of the relevant critical infrastructure or destruction thereof would significantly affect at least two Member States of the European Union and an agreement has been reached with the relevant Member States of the European Union. The significance of such effects shall be evaluated in terms of cross-cutting criteria, including the consequences resulting from the dependence of several sectors on other types of critical infrastructures". The cross-cutting criteria, whose threshold shall be based on the severity of the impact of the disruption or destruction of a particular critical infrastrure, are: "1) casualties criterion (assessed in terms of the potential number of fatalities or injuries); 2) economic effects criterion (assessed in terms of the significance of economic loss or degradation of products or services, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof); 3) public effects criterion (assessed in terms of the

impact on public confidence, physical suffering and disruption of daily life, including the loss of essential services, alternatives for the provision of services and disruption of services and length of restoration thereof)" (Republic of Latvia, 2010). On the basis of the proposals of the Commission, the Ministry of Interior shall inform the European Commission and those EU member states that may be significantly affected by the potential European critical infrastructure regarding such European critical infrastructure and reasons, why it was determined as the potential European critical infrastructure. Also, the Ministry of Interior shall coordinate bilateral or multilateral negotiations with other EU member states, which may be significantly affected by the potential European critical infrastructure. The Security Police, the Constitution Protection Bureau or the Military Intelligence and Security Service participate in the identification process of critical infrastructures. In particular, they shall inform the owner or legal operator of a critical infrastructure regarding the inclusion of the critical infrastructure in the aggregate of critical infrastructures or regarding the determination of the critical infrastructure as the European critical infrastructure. According to the Regulation, "the owner or legal operator of a critical infrastructure or a European critical infrastructure shall appoint an official responsible for the security of the infrastructure and determine the tasks thereof"[24]. Furthermore, as the Ministry of economics pointed out in the questionnaire, it is interesting to note that the Regulation stipulates that in case of an energy crisis (for instance in case of a high or very high terrorism threat level, of a state of emergency or of an exceptional state, the Cabinet may decree that the National Armed Forces of the State Police should take over complete or partial ensuring of measures for the physical security of objects vital for State security. Also, "in the case of the declaration of a high and especially high terrorism threat level, a state of emergency associated with terrorism and public disorder, an exceptional state or state of war, an owner or legal possessor

[24] **According to the Regulation "an official responsible for the security of a critical infrastructure or a European critical infrastructure may be a person: who is a citizen of Latvia; who has not been punished for an intentional criminal offence; who has not been convicted for an intentional criminal offence, releasing from a punishment; who has not been held criminally liable of committing an intentional criminal offence, except the case when a person has been held criminally liable but the criminal proceedings have been terminated on the grounds of exoneration; who has not been put under guardianship; who is not or has not been a staff employee or non-staff employee of the security service of the U.S.S.R., Latvian S.S.R. or a foreign state, or an agent, resident or safe-house keeper thereof; who is not or has not been a participant (member) of an organisation prohibited by the laws of the Republic of Latvia, decisions of the Supreme Council or court adjudications after prohibition of such organisations; who has received the opinion of a narcologist and a psychiatrist that he or she has not been diagnosed as having mental disorders or addiction to alcohol, narcotic, psychotropic or toxic substances; who in accordance with the information at the disposal of the Security Police, the Constitution Protection Bureau, the Military Intelligence and Security Service or the State Police, does not belong to groups of organised crime, unlawful militarised or armed formations, as well as to non-governmental organisations or associations of non-governmental organisations that have commenced activities (legal) prior to the registration thereof or continue to operate after suspension or termination of the activities thereof by a court adjudication". The Security Police, the Constitution Protection Bureau or the Military Intelligence and Security Service may screen employees of critical infrastructures or European critical infrastructures and approve the nomination of the official responsible for the security of a critical infrastructure or a European critical infrastructure. (Republic of Latvia, 2010)**

of critical infrastructures or European critical infrastructures shall co-ordinate their actions with the State Police, the National Armed Forces and the Security Police, the Constitution Protection Bureau or the Military Intelligence and Security Service according to the competence of the State security institution specified in laws and regulations, taking into account the location of the relevant critical infrastructure and other specific factors" (Republic of Latvia, 2010).

In conclusion, Latvia is trying to diversify its energy supplies both nationally and regionally in order to increase its energy security. The liberalisation of its energy market plays a key role in this context and the protection of critical energy infrastructures is essential in ensuring energy security.

Lithuania

In its *Assessment of country performance and opportunities from the Energy Union*[25] of 2016, the European Commission stated that "Lithuania has made recently visible progress in improving its **electricity and gas infrastructure**" (European Commission, 2016c). Already one year before, on the occasion of a meeting in Brussels to discuss the reform of the Economic and Monetary Union and further actions to strengthen the EU's single market and the Energy Union, the EU leaders agreed that Lithuania is a European leader in the field of energy security and that Lithuania's energy projects such as the Klaipeda liquefied natural gas (LNG) terminal and the power interconnections with Poland and Sweden are strategic achievements of the whole EU (President of the Republic of Lithuania, 2015). This was stressed also by Commission Vice-President Maroš Šefčovič. During his Energy Union tour in 2017, he stated that "security of energy supply and internal market functioning are significantly improving in Lithuania. This is a result of the LNG terminal already functioning in Klaipeda, and the development of electricity links with Poland and Sweden. The construction of the gas interconnector with Poland will further contribute to secure supplies. Now, along with the other Baltic States the country needs to move forward with connecting its electricity grids with European networks" (European Commission, 2017h).

The Klaipeda LNG terminal[26], which was put in operation in 2014, is located in the Southern part of the Port of Klaipeda near Kiaules Nugara (Pig's Back) Island. The project, which is operated by Klaipedos Nafta, has increased the number of gas suppliers in Lithuania, which previously imported gas solely from

[25] The Energy Union was launched in 2015 with the aim "to ensure that Europe has secure, affordable and climate-friendly energy". (European Commission, 2017d)

[26] The main gas supplier for the Klaipeda LNG terminal is Cheniere Energy (Texas). Statoil (Norway) also supplies the terminal since 2015. Additionally, in August 2017 Lithuania received the first LNG shipment from the United States, which has reduced the state's dependence on Russian energy. (Ministry of Energy of the Republic of Lithuania, 2017; Reuters, 2017)

Gazprom. Additionally, the country is expected to save approximately $ 931 million over a period of ten years by importing gas through the terminal (Ministry of Energy of the Republic of Lithuania, 2017; Reuters, 2017).

The Gas Interconnection Poland-Lithuania (GIPL - See Figure 6), which is part of the EU Projects of Common Interest (PCI), will connect the Polish and Lithuanian gas transmission systems by 2019. GIPL will establish an interconnection between the gas interconnection systems of Poland and of Lithuania.[27] The implementation of GIPL will contribute to the expansion of BEMIP.

Figure 6. Gas Interconnection Poland-Lithuania
Source: European Commission
https://ec.europa.eu/inea/en/connecting-europe-facility/cef-energy/projects-by-country/multi-country/8.5-0046-pllt-p-m-14

In the field of electricity more specifically, Nordbalt[28] (See Figure 7), which is a cooperation project between Swedish Svenska Kraftnät and Lithuanian Litgrid, connects Klaipeda in Lithuania to Nybro in Sweden with a cable 400 km long (of which almost 350 km are under water) with a capacity of 700 MW. The importance

[27] On the Polish side, GIPL consists of the gas pipeline between Hołowczyce and the compressor station in Gustorzyn on the Polish-Lithuanian border. On the Lithuanian side, it consists of the gas pipeline between the Polish-Lithuanian border and Jauniunai in Lithuania and the gas pressure reduction and metering station located near the Polish-Lithuanian border. Additionally, the supporting infrastructure of GIPL includes the construction of a new compressor station in Gustorzyn in Poland, the extension and modernization of the pipeline to the Hołowczyce compression station and the construction of one gas pressure reduction and metering station in Lithuania. (European Commission, 2016a)

[28] The project is co-financed by the EU. The total investment is estimated at 552 million euro. Sweden and Lithuania fund the reinforcements that need to be done on their territory. (Svenska Kraftnät, 2017)

of Nordbalt lies on the fact that the Baltic States (Estonia, Latvia and Lithuania) can become less dependent on fossil energy sources like gas and coal, as the new connection can transport renewable energy. Additionally, it strengthens the link between the Nordic and the Baltic electricity markets (Svenska Kraftnät, 2017).

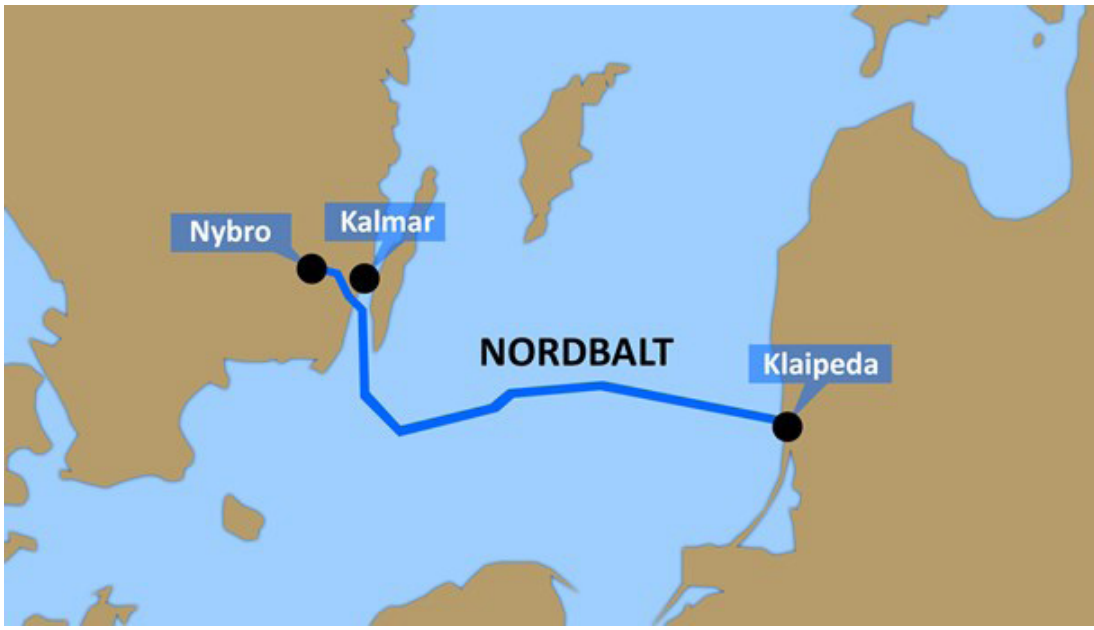

Figure 7. NordBalt
Source: Eye on the Arctic
http://www.rcinet.ca/eye-on-the-arctic/2015/05/05/security-expert-russia-seeks-to-block-baltic-energy-independence/

Moreover, another relevant project in the field of electricity is LitPol Link (see Figure 8), which connects Alytus in Lithuania with Elk in Poland and has a transmission capacity of 500 MW.[29] This power interconnection contributes to integrate the power system of the Baltic States into the synchronous grid of Continental Europe, to diversify the sources of electricity supplies, to the establishment of a single electricity market across the EU and to the energy security of Lithuania and of northern Poland (European Commission, 2015). For these reasons, LitPolLink has been recognised as one of the strategic priorities of the European Union (LitPolLink, 2014). Also, like GIPL, LitPolLink is part of the EU PCI and coincide with the Baltic Connector project (European Commission, 2015; Baltic Connector, 2017).

[29] **The total length of the overhead power transmission line is 163 km. The fact that LitPolLink is part of the EU PCI has given it access to a €27 376 500 Connecting Europe Facility grant for works carried out in Lithuania. The project has also benefitted from the EU's structural funds for construction works carried out in Poland, a loan from the European Investment Bank of €55 million and a Nordic Investment Bank loan of €50 million. (LitPolLink, 2014; European Commission, 2015)**

Figure 8. LitPol Link
Source: LitPol Link
http://www.litpol-link.com/

The importance of these projects in the electricity and in the gas fields will allow the modernisation of Lithuania's infrastructure and the optimisation of costs. However, although the Lithuanian energy system is improving, the state still has to face several challenges. In particular, not only Lithuania is not on track in meeting its national energy efficiency target, but its electricity grid is still connected with and operates in a synchronous way with the Russian and Bielorussian systems (European Commission, 2016c). The desynchronization from the Russian electricity system and the synchronization with the networks of continental Europe is a goal set by the National Energy Independence Strategy (NEIS). The overall objective of the Strategy is to ensure Lithuania's energy independence before the year 2020 by strengthening Lithuania's energy security and competitiveness (President of the Republic of Lithuania, 2015; International Energy Agency, 2017). As Minister of Energy Žygimantas Vaičiūnas puts it, "the long term-vision of the Lithuanian energy sector is to achieve complete independence from fossil fuels in both electricity generation and heating. This ambitious goal not only reflects European and global tendencies, but also coincides with the end of service time of our main energy infrastructure" (Ministry of Energy of the Republic of Lithuania, 2017a).

In this context, another element that should be taken into consideration is the closure of Ignalina Nuclear Power Plant (Ignalina NPP), the state's main supplier of electricity, which was a condition included in the EU Accession Treaty.[30] Ignalina NPP, which was decommissioned in 2010, supplied more than 70 percent Lithuania's electricity demand and about 2.7-2.8 billion kWh per year were exported to Estonia, Latvia, Belarus and the Kaliningrad region of the Russian Federation. After its closure, the state's power generation dropped by 63% (European Commission, 2014). Consequently, the closure of Ignalina NPP introduced huge structural changes into the Lithuanian energy mix because Lithuania compensated the loss of available electricity with an increase in the use of other fuels and by enlarging energy imports.[31] For instance, the share of natural gas in the energy mix has increased visibly. Lithuania imports gas from Russia through Belarus, but in the first half of 2016 it cut its dependence on Russian natural gas by 63,2% because new supply contracts with Norway's company Statoil came into effect (DELFI, 2016). Indeed, at the beginning of 2016, state-owned Litgas, a LNG importer, distributor and exporter, and the fertilizer company Achema, the biggest commercial gas user in the Baltic States, began receiving Statoil gas through a LNG terminal in the seaport of Klaipeda (Reuters, 2016). Therefore, the new infrastructures are essential to diversify Lithuania's energy supplies in order to become more independent from Russia. Indeed, energy reliance on Russia is to drop from 80% in 2012 to 55% in 2020 and to 35% in 2030.

Furthermore, the construction of the Visaginas Nuclear Power Plant (VNPP) would be important because it could ensure Lithuania's energy independence and integration into the international energy community, as former International Energy Agency General Director stated during his visit to the Ignalina Nuclear Power Plant in 2010 (The Baltic Course, 2010). However, the Lithuanians expressed their negative opinion on the construction of the VNPP in the referendum that was held on 14th October 2012. 52.52% of the voters participated in the referendum, 34.07% participants voted in favor of nuclear power plant construction while 62.70% of them voted against it (Ministry of Energy of the Republic of Lithuania, 2015). In spite of this, the significance of the project is recognised by the new National Energy Strategy of 2016 (still under examination in the Seimas, the Lithuanian Parliament). Nevertheless, the Strategy suggests

[30] Lithuania signed the EU Accession Treaty in 2003 and entered the EU in 2004. The Accession Treaty is signed by the EU member states and by the acceding state once the negotiations come to a close and ratified by all the parties. The Treaty enters into force on a date that was previously determined and sets out the conditions and arrangements regarding accession, including the rights and obligations of the new Member State as well as adaptations to the EU institutions. (European Commission, 2016b)

[31] "In 2016, two thirds of electricity consumed in Lithuania was imported. The majority (37%) was imported from Latvia, Estonia and Finland, 27% from Sweden via NordBalt link, 5% from Poland via LitPolLink and the remaining part from third countries". (Ministry of Energy of the Republic of Lithuania, 2017b)

"to bring the project to a halt until it becomes economically beneficial in terms of market conditions or becomes needed to ensure safe power supplies" (The Baltic Course, 2016).

Furthermore, the Lithuanian diversification of energy supplies is being implemented also through other strategies. For instance, in August 2017 Lithuania made its first spot shipment of LNG from the US. The LNG cargo arrived in Lithuania's Klaipėda port from the Sabine Pass terminal in Texas, following an agreement between the Lithuanian natural gas and trading company Lietuvos Dujų Tiekimas (LDT) and Cheniere Energy, the leading US LNG exporter (Grigas, 2017; Sytas, 2017). The gas trade of Lithuania with Norway and the US is important not only for Lithuania but also for Estonia and Latvia because it means the end of Gazprom's monopoly in its traditional market (Grigas, 2017).

Given this background, the **protection of critical energy infrastructure** in Lithuania mainly serves two purposes. On the one hand, it is necessary to ensure the well-being of its society, which implies the security of supply, as discussed in the first chapter. On the other hand, the protection of the new infrastructures as well as of the existing ones is geopolitically relevant in order to make Lithuania less dependent on Russia. In particular, the National Energy Independence Strategy, which was approved by the Government in 2012, states that the main goal of the state is to "ensure Lithuania's energy independence before the year 2020 by strengthening Lithuanian's energy security and competitiveness". In doing so, Lithuania will be able to freely chose the type of energy resources and the sources of its supply (including local production) in order to meet the state's energy security needs and Lithuanian consumers interests coinciding with obtaining energy resources at the most favourable prices (Republic of Lithuania, 2012). The Strategy defines "the main objectives of the Lithuanian state in the energy sector and to set national targets for the implementation of strategic initiatives until 2020, as well as to lay down guidelines for the development of Lithuania's energy sector until 2030 and until 2050" (Republic of Lithuania, 2012; International Energy Agency, 2012). In particular, the Strategy defines the main goals of Lithuania in each energy sector. In the electricity sector, the focus is on those projects that are necessary to ensure Lithuanian energy independence, such as LitPolLink, NordBalt, the development of the Regional Baltic States' electricity market and integration into the Nordic and European Electricity Markets, and the synchronous interconnection of the Lithuanian, Latvian and Estonian electricity transmission systems with the European Continental Network of ENTSO-E. In the gas sector, Lithuania will decrease its gas consumption in the long run by replacing it with renewable sources, while ensuring gas supply alternatives in the short run. The LNG terminal in Klaipeda and LitPolLink serve this purpose. Like in the gas sector, Lithuanian goal in the oil one is to replace

oil with renewable sources as well as to increase competition in the Lithuanian market. These initiatives reflect the three key principles of Lithuania's energy policy. The first one is security of energy supply not only in Lithuania but also in Estonia and Latvia. Lithuania is pursuing the security of energy supply through energy independence. This can be achieved by connecting the Lithuanian energy system to the Continental Western Europe and by diversifying the energy supplies (the projects discussed above are good examples of this). The second principle is competitiveness, which means that Lithuania is making its energy system more competitive by adopting the EU Third Energy Package.[32] This particularly implies the implementation of the ownership unbundling in the electricity and gas sectors in order to boost competition and bring more transparency. In the electricity sector, ownership of electricity generation is being unbundled from transmission. In the gas sector, ownership of gas transmission and supply is being separated. The third principle is sustainable development, which concerns the fact that the increased dependence of Lithuania on fossil fuels especially after the closure of the Ignalina NPP has caused a significant increase of CO2 emissions (Republic of Lithuania, 2012. Therefore, Lithuania must reduce them especially since it signed the Paris Agreement (COP21) in 2015.[33]

The protection of critical energy infrastructure is an essential element of the Lithuanian energy security strategy. In order to ensure it, Lithuania requires that all energy companies plan the necessary investments in and implement the following measures: a) organisational measures (regulations, procedures and plans for alarm signals, crisis and emergency management); b) technical measures (security, video surveillance, entry and access control equipment and other preventive equipment); c) physical security measures (guarded security); d) information and cyber security measures; e) human resources' compliance, control and checking measures; f) measures to maintain safe communication; g) awareness raising and training programmes for employees; h) annual hazard/risk assessment; i) audits and other checks of compliance with the legal requirements. These requirements are regulated by the Lithuanian laws and in particular by the following ones:

1. the Law of the Republic of Lithuania on Civil Protection that establishes "the legal and organisational framework for the organisation and functioning of

[32] The Third Energy Package was adopted in order to improve the functioning of the internal energy market and resolve structural problems. It covers five main areas: 1) unbundling energy suppliers from network operators; 2) strengthening the independence of regulators; 3) establishment of the Agency for the Cooperation of Energy Regulators (ACER); 4) cross-border cooperation between transmission system operators and the creation of European Networks for Transmission System Operators; 5) increased transparency in retail markets to benefit consumers. (European Commission, 2017e)

[33] In 2015, 195 signed an agreement in order to take the necessary actions aiming at avoiding dangerous climate change by limiting global warming to well below 2 degrees. (European Commission, 2017)

the civil protection system, the competence of state and municipal institutions and agencies, the rights and duties of other agencies, economic entities and residents in the sphere of civil protection". In particular, it regulates the intervention of the public bodies in case of emergencies. Article 27 indeed defines the municipal level as the lowest one at which decisions shall be taken and the governmental one as the highest level (Republic of Lithuania, 2009);

2. the Republic of Lithuania Law on Energy, which establishes "the main aims of energy activities in the Republic of Lithuania as well as the legal basis of state management, regulation, supervision and control of the energy sector, the general criteria, conditions of and requirements for public relations, and the main areas of state energy policy". This law defines the 'energy facilities of national importance' as "power plants and boiler houses of the capacity of at least 50 MW; transmission networks for electricity with a voltage of at least 110 kV and appurtenances thereof; main gas pipelines; natural gas import terminals and storage facilities with a capacity of at least 25,000,000 cubic metres; liquefied natural gas import terminals and storage facilities with a liquefied gas re-gasification capacity of at least 0.5 billion cubic metres per annum; main oil pipelines (petroleum product pipelines); oil refineries processing at least 50,000 tonnes of crude oil per annum; crude oil and/or petroleum products terminals and storage facilities with a capacity of at least 10,000 cubic metres; nuclear energy facilities; energy facilities whose importance to the State is recognised according to a procedure laid down by the Government of the Republic of Lithuania". This law also defines a 'project on the development of an energy facility of national importance' as "a document justifying the technical, financial and economic feasibility of the construction of a facility, prepared prior to the start of preparation of territorial planning documents in order to verify that the planned facility is in line with the strategic areas of the state policy and the measures of implementation of the National Energy Independence Strategy, and is compatible with the existing energy sector infrastructure of the Republic of Lithuania and its development" (Republic of Lithuania, 2002);

3. the Republic of Lithuania Law on Cyber Security that details how to set up, manage and control the national cyber security system and defines cyber security terms. According to this law, the Ministry of Defence is the body in charge of shaping, controlling and implementing the national cyber security policy. Additionally, in respect of Law on Cyber Security, the Ministry of Defence established a National Cyber Security Centre within its Cyber Security and Telecommunications Service. The Centre analyses the cyber security environment in Lithuania, protects national databases, manages internet

operations of national organizations, prepares cyber security plans and investigates internet attacks (DELFI, 2015; National Audit Office, 2015);

4. the Republic of Lithuania Law on Natural Gas that lays down "the rules relating to the organisation and functioning of the natural gas sector, access to the market, the criteria and procedures applicable to the issue of licences for transmission, distribution, storage, liquefaction and supply of natural gas and licences to undertake market operator activities". In particular, Article 26 on 'Tasks transmission, storage and/or LNG system operators' stipulates that each transmission, storage and/or LNG system operator shall "provide any other transmission system operator, storage system operator, LNG system operator and/or distribution system operator with sufficient information to ensure the compliance of the transportation and storage of natural gas with the requirements for the secure and efficient operation of the interconnected system" and "build sufficient cross-border capacity to integrate European transmission infrastructure accommodating all economically reasonable and technically feasible demands for capacity and taking into account security of gas supply" (Republic of Lithuania, 2000);

5. the Information Security Requirements for Enterprises and Facilities of Strategic or Paramount Importance for National Security that fall within the Area of Control of the Minister of Energy, approved by the order of the Minister of Energy n. 1-89 of the 2nd of May 2013.

The bodies that are involved in the protection of critical energy infrastructures are the following:

1. the Ministry of Energy that decides the necessary security requirements to protect critical energy infrastructure and that coordinates emergency exercises on interinstitutional, interdepartmental and national levels;

2. the State Security Department that collect information on various threats companies' in ensuring the reliability and compliance of human resources and holds trainings and presentations for the companies' management of conventional and hybrid espionage and terrorist threats;

3. the Special Investigations Service that deals with the implementation of anti-corruption measures and with ensuring the reliability and compliance of human resources;

4. the Ministry of Interior that makes the list of the managers of vitally important information infrastructures, deals with the reliability and compliance of human resources; also, its internal security units work on the protection of certain facilities (such as LNG terminals) under individual contracts;

5. the Fire Safety and Rescue Department under the Ministry of the Interior that intervenes in case of emergencies, natural disasters, technological failures and so on;
6. the Police that intervenes in cases of criminal acts;
7. the Ministry of Foreign Affairs that applies diplomatic measures in the area of mitigation of geopolitical and economic threats;
8. the Army that collects information on energy companies' protected facilities and draws up classified defense plans on conventional and hybrid threats[34] (NATO, 2017);
9. the National Centre for Cyber Security, which started its activities in 2015 and whose "mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation" (National Centre for Cyber Security, 2015);
10. the Risk Management and Crisis Prevention Bureau of the Office of the Government, which is a public institution established by the Government to support in discharging Government and Prime Minister's functions. The Office of the Government is headed by the Chancellor of the Government (Lithuanian Government, 2015).

However, the participation of these bodies in the protection of critical infrastructure is not regulated and coordinated by ad hoc regulations or procedures. By contrast, they act according to the existing laws.

Furthermore, energy companies refer to the governmental Emergency Management Plan in case an unexpected event occurs. The Emergency Management Plan, which regulates the mobilization of material and human resources and the necessary measures to manage them in the event of an imminent or actual state level emergency, is drawn up in accordance with the following laws:

1. the Republic of Lithuania Law on Civil Protection;
2. the Republic of Lithuania Law on Energy;
3. the Republic of Lithuania Law on Natural Gas;
4. the National Preventive Action Plan to ensure the Security of Natural Gas Supply;

[34] According to NATO "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non conventional means adaptively in pursuit of their objectives". (NATO, 2017)

5. the National Emergency Management Plan for Natural Gas Supply;
6. the Order of the Director of the Fire Safety and Rescue Department under the Ministry of the Interior n. 1-134 of 19th April 2010 'on the approval of the criteria for business enterprises and other organisations whose management body is obliged to organise the drafting, the agreement and the approval of emergency management plans, and the criteria for business enterprises whose management body is obliged to establish a centre for emergencies';
7. the Order of the Director of the Fire Safety and Rescue Department under the Ministry of the Interior n. 1-170 of 23rd February 2011 'on the approval of the methodological Guidance on the Drawing up of Emergency Management Plans'.

Additionally, the Ministry of Energy organises emergency exercises on a national scale. A good example is the national level comprehensive civil safety exercise 'Actions by subjects of the civil safety system in case of an emergency in the Liquefied Natural Gas Terminal of Klaipedos Nafta AB due to wilful acts, resulting in the disruption of the gas supply to the Lithuanian gas transmission system in the cold season of the year', which was held on 20th October 2016. The participants in the exercise were: the Ministry of Energy and its Centre for Emergency Operations, the Ministry of Agriculture, the Ministry of Environment, the Ministry of the Economy, the Police Department of the Ministry of the Interior, the Centre for Health Emergencies under the Ministry of Health, the Vilnius City Municipal Administration, the Kaunas City Municipal Administration, the Anykščiai District Municipal Administration, the Visaginas Municipal Administration, Amber Grid AB, Energijos Skirstymo Operatorius AB, Kauno Energija AB, the National Centre for Operations.[35]

As for the main threats to critical energy infrastructure, Amber Grid AB, a Lithuania's natural gas transmission system, has provided NATO ENSEC COE with very interesting and useful answers to a questionnaire submitted to various companies and national bodies for the purposes of this study. It is a very good example of the main threats that energy companies encounter. According to Amber Grid AB, in 2017 the main threats that it encountered are the following (in order of identification and risk level):

1. internal technological threats (breakdowns or failures resulting from employees' or contractor employees actions in gas transportation operation or repairs of the system);
2. internal technological threats (breakdowns or failures due to the action of

[35] **Answers of Amber Grid AB to NATO ENSEC COE's questionnaire.**

third parties, such as carrying out economic activities in the gas pipeline safety zone);

3. geopolitical and economic threats (geopolitical agreements in the energy sector such as the implementation of Nord Stream 2);
4. natural disasters and other metheorological events (heavy storms, rain or snow storms, sever frost, heat wave, hurricane). In this case, the measures set out in the Emergency Management Plan are applied;
5. risk of losing confidential information (malevolent/criminal or naïve actions by employees, treatment of sensitive information entrusted to them);
6. cyber threats (cyber-attacks, espionage, hacking, employee's mistake);
7. criminal threats (terrorism, sabotage, damage to property). In case of a terrorist attack, the measures set out in the Physical Security Plan are applied. In particular, the Dispatch Centre immediately closes the affected gas pipeline section. If there are hostages, the Security Service, which is a quick-response armed team, intervenes. Additionally, the event is immediately reported to the Police, to the Rescue Department and to the Situations Centre of the State Security Department depending on the Ministry of Interior.

In order to physically protect its critical infrastructures, Amber Grid AB has set out a Physical Security Plan (PSP) in accordance with the Physical Security Requirements for Enterprises and Facilities of Strategic or Paramount Importance for National Security that Fall within the Area of Control of the Ministry of Energy, approved by the Order of the Ministry of Energy n. 1-25th January 2013. According to the PSP, five facilities of Amber Grid AB are protected by the armed security guards, namely the dispatch Centre, two gas compressor stations and two gas metering stations. Additionally, over 70 facilities located in remote places are protected through electronic security systems and quick-response armed teams. All the facilities are fenced and have burglary and fire alarm systems. Also, they are protected with microwave, infrared and underground pressure perimeter detectors. The electronic systems of these facilities are connected to the central dispatch system of a private security company hired by Amber Grid AB operating 24 hours per day. Upon activation of the alarm system, the dispatch centre immediately sends the quick-response armed team to the facility. This latter is obliged to reach it within 5-15 minutes (however, the response time varies according to the facility). As soon as it arrives at the facility, the team acts following the procedures. For instance, it protects the property, detains the offender or other suspicious people, calls the police or other services, informs the company's authorised staff, and so on. Furthermore, a telemetric system protects the main gas pipeline. For instance, the dispatch centre monitors the

gas pipeline 24 hours per day and responds to all the situations where the pressure conditions are lower than the set values. In certain cases, the dispatch centre closes the affected pipeline section and sends a team composed of the company's technicians in order to identify the causes of the problem.

In the field of cyber security, Amber Grid AB protects its critical infrastructures on the basis of its Information Security Policy, which is based on the rules detailing the Policy including: a) Rules for Information Management and Security; b) Rules for Issuance of Permits; c) Rules for Management of Information Technologies; d) Rules for Using Information Technologies; e) Rules for Management of Enquiries and Incidents; f) Rules under the Plan on the Recovery of Information Technologies. These rules have been set up on the basis of the following national legislation: 1) Information Security requirements for Enterprises and Facilities of Strategic or Paramount Importance for National Security that Fall within the Area of Control of the Ministry of Energy, approved by the Order of the Ministry of Energy n. 1-89 of 2nd May 2013; 2) LST ISO/IEC 27001:2013. Information Technology-Security Techniques-Information Security Management Systems-Requirements; 3) LST ISO/IEC 27002-2014. Information Technology-Security Techniques-Code of Practice for Information Security Management. Furthermore, according to Amber Grid AB, cyber security is the most critical field for the protection of critical energy infrastructure. The reason is twofold. On the one hand, competent people are lacking. This is due to the fact that the current remuneration system of Lithuania does not allow hiring competent cyber security specialists and outsourcing is very expensive. Therefore, Amber Grid AB trains specialists at its own expenses. These specialists are often hired by other companies at a higher salary. The problem is that a national approach to the issue and decisions on training/education at the state level do not exist. On the other hand, the budget for the acquisition of the necessary equipment (both software and the hardware) is insufficient. Companies are responsible for buying the equipment necessary to protect their infrastructures.

Finally, Amber Grid AB has signed contracts with natural gas operators of other countries containing clauses on cooperation for the protection of the other party's critical infrastructure and provisions for assistance in case of emergency response actions.

CONCLUSION

The four cases analysed in this chapter need to protect their critical energy infrastructures from the same threats. In particular, cyber-security seems to be of utmost importance as nowadays informatics is essential to control the functioning of the energy system of states.

Each state has its own laws and regulations, but all of them have specific and detailed rules to protect critical energy infrastructures and to outline the necessary measures and procedures to follow in case of threats, of disruption of energy supply and of destruction of the infrastructure. Also, all states envisage the involvement of bodies at various levels according to the situation to face.

Furthermore, another similarity among the four cases is that all of them depend on Russian gas. This is the main reason why their energy strategy aims, inter alia, to become independent from Russia. To this aim, all of them are trying to diversify their energy supplies essentially by building new infrastructure allowing them to import energy from other states. The liberalisation of their energy markets is another element in common to the four cases.

What really distinguishes the four cases taken into consideration in this study is their energy system. This means that each state has its own energy mix and its own geographical characteristics that make it a unique case. This, together with national strategies, has an impact on the choices concerning the expansion of their energy infrastructures and connections with neighbouring states.

Moreover, in the case of Estonia, Latvia and Lithuania regional infrastructure connections involving other states like Finland and Sweden are essential in order to achieve diversification of energy supplies and to ensure energy security. Regional approaches to infrastructure connections and to a common energy policy are also essential not only to increase the level of energy diversification but also to achieve a unified EU energy policy.

The case of Italy is different not only because it has a huge energy market differently from the three Baltic States but also because of its geographical location. Indeed, its diversification of energy supply strategies is directed towards the Caspian region and the Mediterranean Sea.

BIBLIOGRAPHY

ABB. (2018). *ABB delivers European power link in record time.* Retrieved from http://www.abb.com/cawp/seitp202/3ff49f4e6df9656fc1257237005d24d7.aspx

Alstom. (2017). *The Auvere power plant in Narva is connected to the transmission network in Estonia.* Retrieved from http://www.alstom.com/press-centre/2015/5/the-auvere-power-plant-in-narva-is-connected-to-the-transmission-network-in-estonia/

Augstsprieguma tīkls. (2017). *About Augstsprieguma tīkls AS*. Retrieved from

http://www.ast.lv/eng/par_ast/

Baltic Connector. (2017). *Project purposes and objectives.* Retrieved from http://balticconnector.fi/en/the-project/

Bride, D., Zvaigzne, A. (2017). *Electricity Market Development in Latvia.* Journal of Social Sciences. Vol.1(8)

DELFI. (2015). *Lithuania launches National Cyber Security Centre.* Retrieved from https://en.delfi.lt/lithuania/defence/lithuania-launches-national-cyber-security-centre.d?id=66804362

DELFI. (2016). *Lithuania cuts Russian gas imports by 63%.* Retrieved from https://en.delfi.lt/lithuania/energy/lithuania-cuts-russian-gas-imports-by-63.d?id=71303026

DELFI. (2018). *Opportunity for Lithuania's LNG terminal as Latvia opens up gas market.* Retrieved from https://en.delfi.lt/nordic-baltic/opportunity-for-lithuanias-lng-terminal-as-latvia-opens-up-gas-market.d?id=70384182

Dudzińska, K. (2012). *Energy policy in the Baltic States-United or separate?* Policy Paper. The Polish Institute of International Affairs. No 37

ENISA. (2018). *About ENISA*. Retrieved from https://www.enisa.europa.eu/about-enisa

Eesti Energia. (2017). *Electricity and heat production.* Retrieved from https://www.energia.ee/en/tehnoloogia/elektri-ja-sooja-tootmine

Elering. (2017). *Estlink 2*. Retrieved form estlink2.elering.ee/public/Dokumendid/EL2_teabeleht_A4_eng.pdf

El Pais. (2017). *Latvia can't live with Russia, can't live without her.* Retrieved from https://elpais.com/elpais/2017/03/24/inenglish/1490368154_789831.html

Estonian Ministry of Economic Affairs and Communications. (2017). *Gas market.* Retrieved from https://www.mkm.ee/en/objectives-activities/energy-sector/gas-market

European Commission. (2011). *Action Plan for North-South Energy Interconnections in Central-Eastern Europe.* Brussels

European Commission. (2014). *Lithuania.* Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/2014_countryreports_lithuania.pdf

European Commission. (2015). *New electricity connections between Lithuania, Poland and Sweden create "Baltic Ring"*. Retrieved from https://ec.europa.eu/energy/en/news/new-electricity-connections-between-lithuania-poland-and-sweden-create-baltic-ring

European Commission. (2014a). *Estonia.* Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/2014_countryreports_estonia.pdf

European Commission. (2016). *Assessment of country performance and opportunities from the Energy Union.* Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/italy-benefits_of_the_energy_union_en.pdf

European Commission. (2016a). *Construction of the Gas Interconnection Poland-Lithuania (GIPL) including supporting infrastructure.* Retrieved from https://ec.europa.eu/inea/sites/inea/files/fiche_8_5-0046-pllt-p-m-2014_final_1.pdf

European Commission. (2016b). *European Neighbourhood Policy and Enlargement Negotiations.* Retrieved form https://ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/treaty-accession_en

European Commission. (2016c). *Assessment of country performance and opportunities from the Energy Union.* Retrieved from https://ec.europa.eu/commission/publications/benefits-energy-union-lithuania_en

European Commission. (2017). *Paris Agreement.* Retrieved from https://ec.europa.eu/clima/policies/international/negotiations/paris_en

European Commission. (2017a). *Enhancement of Estonia-Latvia Interconnection (PCI Project 8.2.2.* Retrieved from https://ec.europa.eu/eipp/desktop/en/projects/project-24.html

European Commission. (2017b). *Latvia's gas market now liberalised.* Retrieved from https://ec.europa.eu/energy/en/news/latvias-gas-market-now-liberalised

European Commission. (2017c). *Projects of Common Interest.* Retrieved from https://ec.europa.eu/energy/en/topics/infrastructure/projects-common-interest

European Commission. (2017d). *Energy Union and Climate.* Retrieved from https://ec.europa.eu/commission/priorities/energy-union-and-climate_en

European Commission. (2017e). *Market Legislation.* Retrieved from https://

ec.europa.eu/energy/en/topics/markets-and-consumers/market-legislation

European Commission. (2017f). *Baltic Energy Market Interconnection Plan*. Retrieved from https://ec.europa.eu/energy/en/topics/infrastructure/baltic-energy-market-interconnection-plan

European Commission. (2017g). *2020 climate & energy package.* Retrieved from https://ec.europa.eu/clima/policies/strategies/2020_en

European Commission. (2017h). *Focus on Lithuania: the Energy Union Tour.* Retrieved from https://ec.europa.eu/energy/en/news/focus-lithuania-energy-union-tour

Global Energy Observation. (2011). *Power Plants.* Retrieved from http://global-energyobservatory.org/geoid/42092

Grigas, A. (2017). *US Natural Gas Arrives in Lithuania. What it means for Russia and the Baltic Region.* Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/baltics/2017-09-12/us-natural-gas-arrives-lithuania

International Energy Agency. (2012). *National Energy Independence Strategy.* Retrieved from https://www.iea.org/policiesandmeasures/pams/lithuania/name-44281-en.php

International Energy Agency. (2013). *Estonia 2013.* Paris

International Energy Agency. (2016). *Energy Policies of IEA Countries. Italy. 2016 Review.* Paris

International Energy Agency. (2017). *Energy Efficiency.* Retrieved from https://www.iea.org/policiesandmeasures/pams/lithuania/name-44281-en.php?s=-dHlwZT1lZSZzdGF0dXM9T2s,&return=PG5hdiBpZD0iYnJlYWRjcnVtYiI-PGEgaHJlZj0iLyI-SG9tZTwvYT4gJnJhcXVvOyA8YSBocmVmPSIvcG9saWNpZXNhbmRtZWFzdXJlcy8iPlBvbGljaWVzIGFuZCBNZWFzdXJlczwvYT4gJnJhcXVvOyA8YSBocmVmPSIvcG9saWNpZXNhbmRtZWFzdXJlcy9lbmVyZ3llZmZpY2llbmN5LyI-RW5lcmd5IEVmZmljaWVuY3k8L2E-PC9uYXY-

International Network for Sustainable Energy. (2014). *Trans-European Energy Networks (TEN-E's) Connecting Europe.* Retrieved from http://www.inforse.org/europe/eu_ten-e.htm

JSC Conexus Baltic Grid. (2017). *JSC Baltic Grid.* Retrieved from https://capacity.conexus.lv/?id=101&lang=eng

Koranyi, D. (2017). *Southern Gas Corridor: Godot Finally Comes?.* Re-

trieved from https://www.huffingtonpost.com/david-koranyi/southern-gas-corridor_b_3383805.html

Latvenergo. (2017). *Mission. Vision. Strategy.* Retrieved from https://www.latvenergo.lv/eng/about_us/briefly_about/mission_vision_strategy/

Latvian Government. (2014). *Informative Report Long-Term Energy Strategy of Latvia 2030 - Competitive Energy for the Society.* Riga

Latvian Ministry of Energy. (2015). *Lithuania LNG terminal-energy security for the Baltic States.* Retrieved from https://enmin.lrv.lt/en/news/lithuanian-lng-terminal-energy-security-for-the-baltic-states

Latvian Parliament. (2005). *Electricity Market Law.* Vilnius

Latvijas Gāze. (2017). *Development of Inčukalns UGS.* Retrieved from http://www.lg.lv/index.php?id=3376&lang=eng

Lithuanian Government. (2015). *Mission.* Retrieved from https://lrv.lt/en/office-of-the-government-1/mission

LitPolLink. (2014). *About the project.* Retrieved from http://www.litpol-link.com/about-the-project/summary/

Merko. (2017). *300 MW Eesti Power Plant of Eesti Energia*. Retrieved from http://group.merko.ee/en/projekt/300-mw-narva-power-plant-of-eesti-energia/

Ministry of Economic Development of Italy. (2013). I*taly's National Energy Strategy: for a more Competitive and Sustainable Energy.* Rome

Ministry of the Economy and of Finance of Italy. (2015). *A focus on PPPs in Italy. 8th Annual Meeting of Senior PPP Officials.* OECD Conference Centre. 23-24 March 2015. Paris

Ministry of Energy of the Republic of Lithuania. (2015). *Visaginas Nuclear Power Plant.* Retrieved from https://enmin.lrv.lt/en/strategic-projects/electricity-sector/visaginas-nuclear-power-plant

Ministry of Energy of the Republic of Lithuania. (2017). *For the first time natural gas from Lithuanian LNG terminal will be stored in the Latvian Inčukalns storage facility.* Retrieved from https://enmin.lrv.lt/en/news/for-the-first-time-natural-gas-from-lithuanian-lng-terminal-will-be-stored-in-the-latvian-incukalns-storage-facility

Ministry of Energy of the Republic of Lithuania. (2017a). *The vision of the Lithua-*

nian energy sector: complete independence from fossil fuels by 2050. Retrieved from https://enmin.lrv.lt/en/news/the-vision-of-the-lithuanian-energy-sector-complete-independence-from-fossil-fuels-by-2050

Ministry of Energy of the Republic of Lithuania. (2017b). *Electricity consumption in Lithuania: highest in a quarter of a century.* Retrieved from https://enmin.lrv.lt/en/news/electricity-consumption-in-lithuania-highest-in-a-quarter-of-a-century

National Audit Office. (2015). *The Cyber Security Environment in Lithuania.* Vilnius

National Centre for Cyber Security. (2015). *Our Mission and Vision.* Retrieved from https://ccdcoe.org/history.html

NATO. (2017). *Hybrid Threats.* Retrieved from http://www.natolibguides.info/hybridwarfare

Official Journal of the European Union. (2013). *Regulation (UE) No 347/2013 of the European Parliament and of the Council of 17 April 2013 on guidelines for trans-European energy infrastructure and repealing Decision No 1364/2006/EC and amending Regulations (EC) No 713/2009, (EC) No 714/2009 and (EC) No 715/2009.* Brussels

President of the Republic of Lithuania. (2015). *Lithuania-EU's energy security leader.* Retrieved from https://www.lrp.lt/en/press-centre/press-releases/lithuania-eus-energy-security-leader/24424

Republic of Latvia. (2010). *Cabinet Regulation No. 496 Adopted on 1st June, 2010 - "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures.* Vilnius

Republic of Lithuania. (2000). *Law on Natural Gas.* 10 October 2000 No VIII-1973 (As last amended on 13 March 2014 – No XII-772). Vilnius

Republic of Lithuania. (2002). *Republic of Lithuania Law on Energy.* 16 May 2002 No IX-884. Vilnius

Republic of Lithuania. (2009). *LAW on Civil Protection*. 15 December 1998 No VIII-971 (As last amended on 22 December 2009 No XI-635). Vilnius

Republic of Lithuania. (2012). *National Energy Independence Strategy.* Vilnius

Reuters. (2014). *Latvian gas storage site could hold back Baltic mar-*

ket for years. Retrieved from https://uk.reuters.com/article/latvia-gas-idukl6n0th4v320141202

Reuters. (2017). *Lithuania receives first LNG from the United States.* Retrieved from https://www.reuters.com/article/us-lithuania-lng/lithuania-receives-first-lng-from-the-united-states-idUSKCN1B11BW

Estonian Parliament. (1996). *State Emergency Law.* Tallinn

Rosato, A. (2016). *A marriage of convenience? The future of Italy-Russia relations. European Council on Foreign Relations.* Retrieved from http://www.ecfr.eu/article/commentary_a_marriage_of_convenience_the_future_of_italyrussia_relations

Statistics Estonia. (2017). *Electricity production increased last year.* Retrieved from http://www.stat.ee/news-release-2017-094

Svenska Kraftnät. (2017). *Nordbalt*. Retrieved from https://www.svk.se/en/grid-development/grid-projects/nordbalt1/

Sytas, A. (2017). *Lithuania receives first LNG from the United States.* Reuters. Retrieved from https://www.reuters.com/article/us-lithuania-lng-idUSKCN-1B11BW

Terna. (2017). *Grid Code.* Retrieved from http://www.terna.it/en-gb/sistemaelettrico/codicedirete.aspx

The Baltic Course. (2010). *Yukiya Amano: New Visaginas Nuclear Power Plant-important project for the region.* Retrieved from http://www.baltic-course.com/eng/energy/?doc=28179

The Baltic Course. (2016). *Energy, Energy Market, Gas, Lithuania, Markets and Companies, Nuclear Power, Nuclear power Plant.* Retrieved from http://www.baltic-course.com/eng/energy/?doc=125521

The Baltic Course. (2017). *Estonian government approves energy sector development plan until 2030.* Retrieved from http://www.baltic-course.com/eng/energy/?doc=134273

Trans-Adriatic Pipeline. (2017). *Southern Gas Corridor.* Retrieved from https://www.tap-ag.com/the-pipeline/the-big-picture/southern-gas-corridor

Chapter 3
Expert Level Workshop "Critical Energy Infrastructure Protection: the Importance of the Public-Private Partnership"-a Report

On 24th October 2017, NATO ENSEC COE held the Expert Level Workshop "Critical Energy Infrastructure Protection: the importance of the Public-Private Partnership", that is the third step of this study, as stated in the Introduction. Its aim was to provide an expert level platform to discuss critical energy infrastructure protection as an important part of energy security and with a focus on the coordination of the efforts of stakeholders/owners of energy infrastructure (electricity, oil, gas) and of public bodies in order to ensure the protection of critical energy infrastructure. The event gathered experts from the public and private sectors from Italy, France, Latvia, Lithuania, Poland, and the United Kingdom.

The workshop began with the introduction of Director of NATO ENSEC COE Col. Gintaras Bagdonas that welcomed the speakers and the guests and explained the reasons of the organisation of the workshop. The project was briefly presented by Dr Tiziana Melchiorre, leader of the project and Fellow at NATO ENSEC COE. She outlined the main aims of the study and explained how it would be developed.

The workshop was then divided into three sessions:

First Session: 'Energy supply and critical energy infrastructure: the involvement of supranational entities and of international organisations'. It was constituted of three speakers.

Co-Chair of NATO Industrial Resources and Communications Services Group (IRCSG-Industry) **Ms Aušra Semaškienė** spoke about "Critical Infrastructure

Protection in NATO Resilience enhancement agenda". The necessity of enhancing resilience was stressed in the Alliance's Warsaw Summit held in July 2016 when NATO Heads of States agreed on the importance of their "Commitment to Enhance Resilience". As Ms Semaškienė noticed, Former NATO Head of Civil Preparedness Lorenz Meyer-Minnermann said that "The Warsaw Summit Commitment to Enhance Resilience was a historic reaffirmation that resilience, ensured through systematic civil preparedness and effective civil-military planning, is a central pillar of NATO's collective defence. Requirements have been agreed and criteria for success are being defined. The basic process is thus in place, but delivering on the Warsaw Commitment remains a complex undertaking. It will require a holistic view on resilience, both within national governments, across governments and the private sector, between NATO and the European Union, and with partner countries beyond NATO".

After defining the 'resilience' of infrastructure as "the ability to quickly adapt to disruptions in the face of adversity, recover from setbacks, while maintaining continuous business operations and safeguarding people", she explained that enhancing resilience through the civil preparedness of the Allies is essential for the following reasons. Firstly, resilience is an essential basis for deterrence and effective fulfilment of the Alliance's core tasks. Second, resilience is first and foremost a national responsibility of the Allies, and NATO is as resilient as the weakest of its members. Third, in order to be able to deter and defend themselves from the full range of modern threats, the Allies need to maintain and protect critical civilian capabilities alongside and in support of military capabilities. Ms Semaškienė also explained that resilience can be enhanced in three ways. First, through a political commitment at the highest level by each allied nation to strive to achieve the agreed requirements for national resilience. Second, by setting relevant legal basis, devoting needed capabilities and resources, with the involvement of the whole of government and the private sector. Third, by ensuring working arrangements with relevant organizations and partner countries. She referred to the 7 baseline requirements for civil preparedness: a) continuity of government; b) resilient energy supplies; c) resilient civil communication services; d) ability to deal with large scale population movements; e) ability to deal with mass casualties; f) resilient civilian transportation systems; g) resilient food and water supply. The 7 baseline requirements were agreed by Defense Ministers in February 2016 and the Heads of State and of Government committed to achieve them in July the same year. Additionally, the Defense Ministers agreed on the resilience guidelines in June 2016. However, they are not binding. Instead, they just detail the basic requirements leaving the nations to decide on how to achieve the requirements. In December the same year, the Defense Ministers agreed on the (self) evaluation criteria, which were worked out by NATO planning groups and experts to provide tools for national

self-assessment and further action. The Allies must evaluate the state of the resilience of their critical energy infrastructure against the NATO criteria by the end of 2017. A report on NATO State of Civil Preparedness will be released in Spring 2018. Also, the Allies will have to fill the resilience and civil preparedness gaps through national programs and send their progress report to NATO every two years.

Given this background, Ms Semaškienė identified the two main pillars of a resilient energy system. The first one is security of supply that implies diversification of sources, routes suppliers and generations forms as well as redundancy and reserves. The second pillar is the protection of critical energy infrastructure, which means: 1) creation of an efficient public/private platform; 2) adequate continuous investments; 3) standardised requirements; 4) dealing with transnational and trans-sectoral dependencies. Therefore, the concept of critical infrastructure protection is based on information security, cyber security, physical security, and personnel security.

Finally, Ms Semaškienė emphasised that the NATO requirements for critical energy infrastructure protection are an added value for the improvement of the national system. They focus on two aspects, namely vital aspects (that are civil preparedness integrated into the defense planning and a trans-sectoral relationship) and on the possibilities for an efficient use of the resources (that include sharing expertise/taking into account the relevant capabilities within the Alliance and looking for arrangements with strategic partners).

Mr Rémi Mayet, Deputy Head of Security of Supply Unit at the European Commission spoke about the "Security of energy supply in the European Union". After stressing that energy supply is a shared competence of the EU and its members, Mr Mayet outlined five main points. First, he outlined the main components of the EU Energy Strategy of 2014 stressing that the EU imports half of its energy needs and that it must face persistent risks of geopolitical disruptions as well as technological, terrorism and climate risks. Additionally, the EU aims at increasing energy efficiency and endogenous renewable energy supply by 27% in 2030, which is a target that is being discussed at present and which is likely to be increased. The EU Energy Strategy also aims at creating a well interconnected energy market and at increasing the diversification of suppliers and routes. At present, 39% of gas is imported from Russia. Therefore, increasing the EU independence from Russia is important. Mr Mayet also stressed three other important issues related to the EU Energy Strategy, namely the necessity of the EU members to prepare to risks, the importance of the principles of solidarity and trust among the EU members as well as of the energy and climate diplomacy. Second, Mr Mayet spoke about the security of gas supply that

is characterised by three trends: 1) a slow but continued downward trend in the EU gas domestic production; 2) a small decrease in gas consumption until 2040 when a more significant decrease is expected; 3) stable gas imports until 2040 is expected. Diversification of supply sources is crucial for the EU. To this aim, the EU is developing the Southern Gas Corridor, trying to access new fields in the Eastern Mediterranean area, having a facilitated access to the global LNG market, and optimizing the utilization of its storage capacity. Additionally, a hot topic is the Nord Stream 2 pipeline, which transports gas from Vyborg in Russia to Greisfald in Germany and to which several EU states oppose for different reasons. Among these, the main one is that the pipeline is incompatible with the objectives of the EU as it will make it even more dependent on Russian gas. However, the European Commission, to which some states have tried to give the mandate to negotiate on the project, has no veto power on its construction.

Mr Mayet has stressed the importance of the new regulation on gas supply, Regulation (EU) 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. This Regulation goes further than Regulation (EU) No 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC. The main reason is that the new regulation shifts from a national to a regional approach requiring that the EU members work together in 'risk-based groups' to assess the potential for disruption to their gas supplies and agree on joint actions to prevent or mitigate the consequences. On the basis of the solidarity principle, cross-border measures are necessary in order to help neighbouring states guarantee the provision of gas to protected consumers in the event of an extreme shortage. The European Commission has a facilitator role in this process and organises the sharing of best practices for arranging regional cooperation. Also, the Regulation ensures that new preventive non-market-based measures, if needed in last resort, do not endanger the security of gas supply of other Member States or in the Union. The Gas Coordination Group (GCG) plays an important role in the information sharing, report and advice in the sector. Member States are required to establish preventive action plans and emergency plans to better prepare to face a supply crisis. Provisions to ensure reverse flow are also included in the regulation for all pipelines with few justified exceptions. Furthermore, according to the regulation, the member states must ensure that all necessary measures are taken so that in the event of a disruption of the single largest gas infrastructure, the technical capacity of the remaining infrastructure, determined in accordance with the N – 1 formula is able to satisfy total gas demand of the calculated area during a day of exceptionally high gas demand occurring with a statistical probability of once in 20 years. This shall be done taking into account gas consumption trends,

the long-term impact of energy efficiency measures and the utilisation rates of existing infrastructures. In particular, the national competent authorities must take all the necessary measures to supply protected customers in the following cases: (a) extreme temperatures during a 7-day peak period occurring with a statistical probability of once in 20 years; (b) any period of 30 days of exceptionally high gas demand, occurring with a statistical probability of once in 20 years; (c) for a period of 30 days in the case of disruption of the single largest gas infrastructure under average winter conditions. Mr Mayet also explained that the regulation identifies risk groups because assessing correlated risks jointly in risk groups will ensure that Member States are better prepared for any crises. The risk groups are the following: 1) Eastern risk group, 2) North Sea risk group; 3) North African risk group.

Additionally, in agreement with Article 7.1 of the Regulation, in November 2017, ENTSOG carried out a Union-wide simulation of gas supply and infrastructure disruption scenarios. The simulation included the identification and assessment of emergency gas supply corridors and shall also identify which Member States can address identified risks, including in relation to LNG. The gas supply and infrastructure disruption scenarios and the methodology for the simulation were defined by ENTSOG in cooperation with the GCG. According to Article 7.2, by October 2018 the competent authorities shall prepare a common risk assessment at group risk level of all relevant risk factors such as natural disasters, technological, commercial, social, political, and other risks. Also, the competent authorities of each member state shall make a 'national risk assessment' of all relevant risks affecting the security of gas supply by October 2018. Stakeholders should cooperate with the competent authorities and provide the requested information. The result of the simulation should be an integrated perspective on gas and electricity systems. According to Article 8.3, the preventive action plan and the emergency plan shall contain a regional chapter by March 2019.

Third, Mr Mayet also stressed that in the electricity sector, the Commission has proposed the European Parliament and the Council a regulation on risk-preparedness. It is part of the 'Clean Energy Package' which was proposed in 2016 and includes a new market design for electricity. The proposal gives a key role to Transmission System Operators and to cross-border regional security coordinators. Mr Mayet underlined that the necessity of the regulation stems from the fact that uncoordinated actions between member States can undermine the market functioning and threaten the security of supply of other countries, as already seen in the past. Indeed, when preparing or managing crisis situations, the member states follow different approaches and tend to disregard the situation across their borders. Their crisis plans and actions tend to remain national in focus (therefore regional cooperation remains very limited), there

is lack of information sharing and transparency and of a common approach to identify assess risks. Consequently, a common methodology is necessary for: 1) identifying electricity crisis scenarios; 2) assessing short-term adequacy issues; 3) regional and national risk preparedness. In this context, national plans based on common rules are necessary as well as some measures coordinated at regional level and prior consultation of other member states and the Energy Cooperation Group (ECG). Member states should handle crises on the basis of common principles, namely 'market comes first' and cross-border cooperation and assistance. Other important elements are the systematic monitoring of security of supply and an ex post evaluation of electricity crisis events. The EU will monitor security of supply through its European Agency of Regulators and the Electricity Coordination Group. Also, information sharing and transparency are essential. The regulation is now being discussed and its final adoption by the European Parliament and the Council can be expected in 2018.

Fourth, Mr Mayet's speech also covered the oil sector. He stressed the relevance of Directive 2009/119/EC on minimum emergency oil stocks. According to this Directive, member states shall adopt the necessary measures to ensure that the total oil stocks correspond to 90 days of average daily net import or 61 days of average daily inland consumption, whichever of the two quantities is greater. Mr Mayet stressed that stocks remain permanently available and physically accessible and that member states must take the necessary measures to enable their competent authorities to quickly, effectively and transparently release their emergency stocks in the event of a major supply disruption. He also stressed the key role played by the European Oil Coordination Group (which is made of representatives of the member states and chaired by the Commission) in the exchanging of information and in coordinating the measures on restrictions on consumption. Another important point is the coordination of the Commission with the International Energy Agency in case of absence of an effective international decision to release stocks and when difficulties arise in the supply of crude oil or petroleum products to the member states.

Fifth, Mr Mayet illustrated Directive 2008/114/EC to identify and designate the European critical infrastructures and assess the need to protect them. This directive covers the energy and the transport sectors. It includes measures concerning infrastructures and facilities aiming to produce, transport and store oil, gas and electricity. According to this directive, operator security plans should be put in place for every designated critical asset as well as a security liaison officer in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. Additionally, European rules exist to ensure that the ownership by entities of third countries does not endanger security. In the third package rules the member states must check with the

Commission before delivering a certification to a transmission operator controlled by a third country. Also, the risks related to the control of security of supply concerning the infrastructure owned by third countries must be taken into account in the gas and electricity rules on security of supply. In this context, in September 2017, the Commission proposed horizontal rules to coordinate national screening of foreign investments in strategic sectors and screen investments in Union projects.

Mr Koen De Smedt, Coordinator in the Action Against Terrorism Unit of the Transnational Threats Department of the Organisation for Security and Cooperation in Europe (OSCE) gave a speech on the "OSCE efforts in the field of protecting critical energy infrastructure from terrorist attack". He began presenting OSCE's aim in the field that is working for stability, prosperity and democracy in 57 States through political dialogue about shared values and through practical work that makes a lasting difference. The OSCE area covers one billion people from the Euro-Atlantic to the Eurasian regions and it has 11 partners for cooperation. Mr De Smedt also described the work of OSCE in the counter-terrorism area. In particular, OSCE focuses on the following sectors:1) international legal framework, co-operation in criminal matters related to terrorism; 2) preventing and countering violent extremism and radicalization that leads to terrorism; 3) preventing and suppressing the financing of terrorism; 4) countering the use of the Internet for terrorist purposes; 5) promoting Public-Private Partnerships (PPP); 6) UNSCR 1540 ; 7) travel document security; 8) promoting and protecting human rights.

Mr Koen De Smedt outlined OSCE's actions to protect critical energy infrastructure that concern the field of cyber/ICT security as well as the physical protection of non-nuclear critical energy infrastructure from terrorist attacks. In this sector in particular, OSCE has produced the

"Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace" whose aim is to "raise awareness of the risk of cyber-related terrorist threat to NNCEIP, particularly to industrial control systems and cyber-related infrastructure, among all stakeholders and to promote the implementation of good practices for protecting this infrastructure" (OSCE, 2013). Also, the Guide "identifies key policy issues and challenges and collects selected good practices as possible solutions. The Guide is to serve as a reference document containing key information for government policy makers, state authorities in charge of critical (energy) infrastructure protection, owners and operators of non-nuclear energy infrastructure, and other stakeholders in OSCE participating States and Partners for Co-operation" (OSCE, 2013). OSCE has produced also other works

that are the following: 1) Cyber-related Terrorist Attacks on Non-Nuclear Critical Energy Infrastructure; 2) Good Practices in ICT Risk Management Frameworks to Address Cyber-related Terrorist Risks; 3) Good practices in ICT-related Terrorist Risks; 4) Good Practices in Critical Infrastructure Protection within the OSCE; 5) Suggestions for Future OSCE Roles to Advance Cyber Security in Non-Nuclear Critical Energy Infrastructure.

OSCE's efforts to protect critical energy infrastructure include:

1. OSCE Ministerial Council Decision on the protection of critical energy infrastructure from terrorist attacks -2007
2. OSCE Expert Meeting on Protecting Critical Energy Infrastructure from Terrorist Attacks, in Vienna –2008
3. CTN Newsletter Special Bulletin on Protecting Critical Energy Infrastructure from Terrorist Attacks –January 2010 available at www.osce.org/atu/41367
4. OSCE Public-Private Expert Workshop on Protecting Critical Energy Infrastructure from Terrorist Attacks, in Vienna –2010

Furthermore, OSCE organizes national crisis management and risk assessment exercises involving state authorities and the private sector in order to increase the ability of the participating states to respond to cyber related terrorist incidents by improving public-private and private-private cooperation based on the recommendations of the Guide. Indeed, in order to increase resilience of national critical energy infrastructure and to advance the capabilities to respond to a terrorist cyber-attack against the industrial control systems, OSCE's exercises aim at: a) raising awareness about the (current) vulnerabilities of ICT-dependent critical energy infrastructure; b) disseminating knowledge and good practices offered in the Good Practices Guide; c) allowing states to test the effectiveness of existing legal and regulatory framework in the field of cyber security and CEIP; d) advancing private-private and private-public co-operation. Since 2016, OSCE has organized six national exercises in the OSCE area, namely one in central Europe, three in South-Eastern Europe, one in Western Europe and one in Central Asia. The results of these exercises were the following: 1) a hands-on experience on the possible consequences and vulnerabilities of terrorist attacks; 2) better awareness of the risk, better understanding of cyber security vulnerabilities; 3) ability to test the effectiveness of existing protection and crisis management systems; 4) better working partnership between the public and private sectors 4) analysis of the readiness to mitigate a cyber-attack on NNCEIP with tangible recommendations and ideas of way forward. Mr Koen De Smedt provided two examples. The first one was a framework for improving critical infrastructure cyber-security that includes the following phases:

a) identification (access management, business environment, governance, risk assessment, risk management strategy); b) protection (access control, awareness and training, data security, information protection processes and procedures, maintenance, protective technology); c) detection (anomalies and events, security continuous monitoring, detection processes); d) response (response planning, communications, analysis, mitigation, improvements); e) recovering (recovery planning, improvements, communications). The second example is the assessment of the readiness to mitigate cyber attacks. In this exercise, five phases were identified. The first phase concerned the identification of the crisis that meant an early detection and escalation of cross-organizational/sectoral issues. The other four ones were related to the coordination during the crisis and included the information flow (interfaces) between public bodies and between private bodies, the cross-sectoral information flow (e.g. CERTs or other branches), information flow between the private and the public bodies, and the interconnected communication and solution finding.

OSCE is also committed to building confidence between states in cyber-space. To this aim, the OSCE States adopted two sets of confidence-building measures in 2012 and 2016 essentially for achieving two objectives. First, to increase co-operation, transparency, predictability and stability between States. Second, to reduce the risk of misperception, escalation, and conflict that may stem from the use of ICTs. Mr Koen De Smedt stressed that the second set focuses on further enhancing co-operation between States–including for example to effectively mitigate cyber-attacks on critical infrastructure that could affect more than one country. Also, Participating States, on a voluntary basis, will encourage, facilitate and/or participate in regional and subregional collaboration between legally-authorized authorities responsible for securing critical infrastructures. In this context, Mr Koen De Smedt gave two examples: 1) on 22 October 2017, the U.S government issued a rare public warning that sophisticated hackers are targeting energy and industrial firms, the latest sign that cyber attacks present an increasing threat to the power industry and other public infrastructure; 2) on May 2017, hackers gain entry into U.S., European energy sector, Symantec warns.

Second Session: 'The role of the state security forces in critical energy infrastructure protection'. It was constituted of three speakers.

Major General Francesco Maurizio Noto, Director of the Italian Ministry of Defence Energy Task Force, gave a speech on "Energy Critical Infrastructure and Building a Management System". He firstly addressed the activities of the Italian Ministry of Defence Energy Task Force by illustrating its three main pillars: 1) consumption and energy support to military capacities and cost reduction; 2)

implementation of energy efficiency; 3) environmental protection. Major General Noto then stressed the importance of the White Paper for International Security and Defense of 2015 that was prepared by the Ministry of Defense. This document emphasises the strategic interest of Italy in the Euro-Atlantic and in the Mediterranean areas and the necessity of a reform aiming at a better internal integration of the Defense system. In addition, Major General Noto pointed out that the White Paper stresses that the competition among states for natural resources (energy and raw materials) could produce a higher level of international tension leading to possible conflicts. Therefore, Italy must increase its capacity levels of national defense and contribute to international security. In this perspective, Italy should increase its defense technological level and identify which model of governance can best guarantee the Ministry of Defense its compliance with modern criteria of effectiveness, efficiency and economy. Furthermore, according to the White Paper, Italy should promote the culture of participation in public institutions and in the academic/industrial sector.

Major General Noto also illustrated the main energy objective of the Italian defense that are based on the national guidelines and on the EU directives. In particular, he mentioned the Constitutional Decree 26 January 2015 and the Enhancement Decree 13 January 2013 that are the only legal documents referring to the involvement of the Ministry of Defense in the energy sector. These two documents also discuss the national strategies in the energy sector, the evaluation of energy security, energy efficiency and the importance of the renewables. They also stress the importance of trainings and of information sharing in the sector.

Major General Noto then illustrated the composition of the Energy Task Force of the Ministry of Defense. It is linked to the Armed Forces and is constituted of the Support Secretariat and of the following units dealing with: 1) legal affairs; 2) energy efficiency; 3) renewable energy production; 4) energy consumption; 5) technical standards; 6) ICT systems; 7) environmental aspects. The Energy Task Force has to deal with many issues among which there are new technological solutions, new EU and Italian regulations and directives, new lines of financing, relationships with other Ministries and with universities and research institutes, new energy performance contracts.

After having mentioned the EU definition of critical infrastructure that has been discussed in the first chapter of this study, Major General Noto emphasised that energy, which refers to production, transmission, distribution, dispatching of electricity and all forms of energy, such as natural gas, is strictly linked to security, military defense and civil defense. Also, the concept of energy is strictly linked to: 1) transport-aviation, naval, railway, road transport and distribution of

fuels and products of primary necessity; 2) ICT-Telecommunications and telematics; 3) water- water resources and wastewater management; 4) agriculture, production of foodstuffs and their distribution; 5) health-hospitals and networks of services and interconnection; 6) finance-banks and financial services; 7) chemical industry; 8) networks supporting the government, central and territorial entities, and emergencies. Therefore, energy infrastructures are complex systems that affect other critical areas. In fact, a disruption of critical energy infrastructure can have a negative cascading effect on other infrastructures. Consequently, there are physical, geographical, cyber and logical interdependency.

Critical energy infrastructure has been defined by each state within the EU, but the dependency of the defense sector on it has poorly been addressed. Instead, this dependency is crucial as the defense sector depends almost entirely on national infrastructures. The armed forces are a large consumer of energy that is a significant vulnerability in military capabilities. Therefore, it is necessary to critical energy issues in the defense sector, to identify the several levels of energy independence of the armed forces, to promote the civil-military synergy, to support energy security, and increase energy resilience. Major General Noto stated that a correct approach to critical energy infrastructure protection includes: 1) requirements, which means security of energy infrastructures, security of supply routes, and capability to manage crises and conflicts; 2) threats, which can reduce or inhibit the operational capabilities (this concern both the physical and cyber domains); 3) solutions, such as the one proposed in the 'concept development and experimentation' (CD & E), which is an integral part of capability development, providing potential solutions to conceptual gaps identified within NATO's capability shortfalls, and the DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability) methodology.

Major General Noto stressed that the diversification of sources and the security of critical energy infrastructure is essential for the well-being of the society. In order to achieve these goals, an integrated approach within the Diplomatic Component, Information, Military and Economic (DIME), which are the four sources of national power, is necessary. A partnership with the academic, private and industrial sectors is also important. In this context, the analysis of energy issues applying NATO's DOTMLPFI methodology is useful. If this methodology is applied to defense, the following results are obtained: 1) doctrine: implementation of critical infrastructure protection national doctrine (energy-security and cyber security); 2) organization: cross-cutting approach at military summit level; 3) training: education and training oriented to the energy security sector; 4) material: research and development concerning low energy consumption materials and equipment; 5) leadership: define a clear chain of command in energy secu-

rity sector harmonized at central government level; 6) personnel: awareness, knowledge-employing specialized personnel; 7) facilities: implementation of micro-smart grid combined with energy storage solutions and energy management; 8) interoperability: promoting synergy (national and international context) through the development of common platforms.

Furthermore, Major General Noto identified some of the main elements of energy management system, namely a comprehensive and holistic (multidimensional) approach, efficiency as energy capability of defense and interaction and cooperation with public institutions/universities/industries/private sector. The main goal should be the 'smart military district' by using BATs and ICT systems. Also, he pointed out that the energy and the environmental sectors are strictly intertwined. For this reason, an integrated management system is necessary when analysing the link between them. It should include energy, water, waste and cyber security. In this context, the smart military districts are very important. They are characterized by smart/eco building that are built with the Nearly Zero-Energy Buildings technologies and where a building management system (BMS) is installed. BMS is a computer-based control system used to control and monitor the building's mechanical and electrical equipment. Also, a smart grid ensures that the buildings in the district are connected and that the various military districts are connected. Therefore, Smart Military Districts support national security defense capacities and civil protection activities and contribute to the resilience of the national energy system. Additionally, they have a small impact on the environment, ensure an energy-waste-water integrated management, and integrate with the territory. Major General Noto also said that the following elements are important in a building management system: 1) human factor, which is fundamental within an entire organization's security system; 2) vulnerability of the SCADA systems; 3) cyber security. The first phase of the critical energy infrastructure protection is being implemented. It will lead to the implementation of 'resilient' BMS. Major General Noto ended his speech with a quotation by George Grant Mac Curdy: "the degree of civilization of any epoch, people or group of peoples is measured by the ability to utilize energy for human advancement or needs".

CWO5 Stefano Bergonzini, of the Italian Carabinieri, working as Staff Assistant at the NATO Stability Policing Centre of Excellence (NATO SP COE) in Vicenza (Italy), illustrated the 'NATO Stability Policing' Concept. After having briefly presented the main aims of NATO Centres of Excellence, he discussed the main activities of the SP COE which are: 1) developing and validating concepts for the Alliance; 2) contributing to the development of Allied (Joint) Doctrine; 3) developing training curricula and delivering courses; 4) operating the lessons learned cycle in the field of Stability Policing.

To these aims, the SP COE interacts with national and international military and civilian bodies/institutions, industry and academia. As for the SP COE communication is very important, it manages a website with graduated access, a facebook page as well as linkedin and twitter profiles.

CWO5 Bergonzini discussed NATO Stability Policing (SP), which is "the evolution of the concept of the Multinational Specialized Unit (MSU), developed and led by the Italian Carabinieri and deployed in several TOOs, tasked mainly with patrolling, crowd and riot control and training of local police forces". CWO5 Bergonzini stressed the importance of the idea of MSU, which preceded by some years the UN Brahimi Report of 2000 addressing shortcomings, including in policing activities, in the then existing UN peace support operations.

Within NATO, Stability Policing "is a set of police related activities intended to reinforce or temporarily replace indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights". When, during a crisis, a vacuum in policing capabilities and capacity arises, SP can bridge this so-called "security gap" through its two missions, namely reinforcement and/or temporary replacement of the indigenous police forces. "When the indigenous police or a recognized government are non-existent, incapable or unwilling to perform their tasks, all police tasks must be assumed by Stability Policing assets, including law enforcement, area patrolling and control, forensics, control of borders and sensitive structures, criminal investigations and intelligence, and civil disturbance operations". A reinforcement mission is necessary "when the indigenous police is existing and reliable but its effectiveness is limited" and may require "monitoring, mentoring, advising, reforming, training and partnering with. The ultimate goal is to enhance the indigenous police self-sufficiency and effectiveness".

NATO Stability Policing activities are conducted with the aim of: 1) re-establishing a safe and secure environment (SASE); 2) establishing the conditions for meeting longer term governance and development needs, in particular through Security Sector Reform (SSR); 3) restoring Public Order and Security.

CWO5 Bergonzini explained that Stability Policing can be employed throughout the whole spectrum of conflict, from stable peace to high-intensity conflict, adapting to different campaign themes and to the specific mission mandate. This also implies that military or civilian authorities might be in the lead during specific phases, operations, activities or tasks.

SP requires different levels of policing skills, from basic to advanced and can be

conducted by a variety of actors namely gendarmerie-type forces, the military police, other combat/support military forces, non-military actors like international organizations, non-governmental organizations, and contractors; while all can contribute in some way, in relation to their training and equipment, not everything can be done by all.

Some SP tasks listed in the Allied Joint Doctrine for Stability Policing (AJP-3.22,) include: crowd and riot control, border control, restoration of public security and public order, election security, close protection, searches and seizures, criminal investigations, high risk arrests, critical site security, negotiation and mediation, protect people (especially vulnerable groups) and property, rapport building (population and authorities), support to judicial and correction institutions, support to military explosive ordinance disposal/improvised explosive devices EOD/IED and civilian unexploded ordnance UXO activities, conduct forensic activities, biometric, support weapon intelligence teams (WIT), police intelligence, contribution to situational awareness, counterterrorism, counter-organized crime, hostage rescue and the connection between most of them and the safeguarding of CEIs was explained.

As illustrated by CWO5 Bergonzini, SP plays a critical role in supporting the protection of critical energy infrastructure as an important player in the public-private partnership at all levels, from strategic to tactical. In fact, SP subject matter experts interacting with public and private entities such as the Ministry for Energy or Industry and private companies producing, distributing or storing energy, can advise policy makers and central authorities in the development and implementation of a strategic campaign aiming at securing CEI; they can support the elaboration and execution of a plan at the operational level linking the activities and tasks at the tactical level with the strategic goals, objectives and overall end-state.

In relation to the existence and performance of the indigenous police, they can temporarily replace or reinforce it also focusing on the specific CEI protection. If an effective and efficient indigenous police is lacking, SP can take over, amongst others, by providing police intelligence to increase the situational awareness and patrol CEI sites and surroundings. In case of unrest, SP can conduct crowd and riot control (CRC) operations in and around such structures; it can investigate crimes related to CEI including cyber, organized crime and terrorism. SP supports the development and improvement of lacking capabilities and capacities of the indigenous police or other entities of the security sector.

Dr Nicolas Mazzucchi, Chargé de Mission Perspective Technologique de Défense at the French Ministry of the Army, gave a speech on 'Armed Forces, Energy

Security and Natural Events: Irma Storm RETEX'. Dr Mazzucchi's presentation aimed at discussing the intervention of the Armed Forces in the case of natural disasters by taking the Irma storm on S. Martin island in Martinique as an example. He discussed the French military doctrine on natural disaster relief by stressing the importance of the 2013 White Paper whose first priority is "to protect national territory and French nationals". Out of military action, the armed forces could be used by the Ministry of the Interior, on which they depend, under requisition in order to face natural disaster events. Also, according to the '4 i rule', the armed forces are used when civilian means do not exist, are unavailable, maladjusted or insufficient. In case of natural disasters, the Military Fuel Service (SEA), which is an inter-service branch of the French Army subordinate to the head of the defense staff, had to provide petroleum support by coordinating the armed forces POL (petroleum oil and lubricant). It also has to provide advisors to the Ministry in charge of energy issues and to private operators. It has to deploy specific means to provide assistance on the national territory and act in cooperation with private operators. Regarding the electricity support that has to be provided in these cases, in addition to SEA there are also other organisations involved in the process such as the one of engineers.

Dr Mazzucchi said that in this case there was civilian-military cooperation where: 1) the armed forces operated under the civilian supervision (préfet) to secure the area; 2) the armed forces supported civilian initiatives (for instance, helicopters helped raising electric poles); 3) the utilities companies provided post-disaster support (e.g. EDF and ENEDIS provided 50 generators); 4) engineers supported the utility companies for emergency supply with power generators, potable water and food rations). Furthermore, on the French side of the island the installations that was meant to supply the population of energy, namely 1 jet-fuel tanker truck and 2 25cm mobile tanks at Grand Case airport, 1 desalination plant, was unavailable during the storm except of the truck and the tanks of the airport. After the storm, the National Command officer in Martinique coordinated the SEA actions. The transport aircraft (CASA) was defuelled at the airport and local equipment was used (e.g. the airport jet-fuel truck). Also, some equipment (barrels, pumps, flexible tanks) was sent to supply the forces and to provide an emergency support to the population. In the post-emergency phase, a SEA coordination officer was installed at the Theatre Joint Headquarters. SEA cooperated with the local oil companies to provide fuel for the forces (F-35/F-54/F-67) and the BPC ship arrived with helicopters and SEA tanker trucks. However, Dr Mazzucchi clarified that SEA equipment is not made for this kind of situation. Its exercises concern natural disaster relief but they do not concern the energy sector except in the case of POL. He also stressed that the intelligence is necessary to prepare the right quantity and nature of equipment. In fact, SEA had to work on the basis of hypotheses

because communication was not possible during the storm. Additionally, SEA had to work under the pressure of important media and politics. Dr Mazzucchi gave interesting numbers about the French Armed Forces action during the Irma storm: 1) 5200 people transported; 2) 350 military deployed on S. Martin island; 3) 1700 tons of freight carried to the island; 4) 330 air lines assuring connections by air; 5) 70 assistance missions by helicopter. From this case, it is possible to draw the following lessons learned: 1) France conducted important military operations with an impact on capabilities; 2) the ability to provide important means in the post-emergency phase was shown; 3) the joint military operation of the navy and of the air force transporting and supporting the land forces was important; 4) a combined military operation with the Allies (US, Netherlands, UK) was crucial; 5) it is necessary to update the emergency support doctrine to include energy issues as a top priority.

Third Session: 'Critical energy infrastructure protection: perspectives from different angles'. It was composed of six speakers.

Mr Vytautas Butrimas, Subject Matter Expert at NATO ENSEC COE, gave a speech on 'The cyber security dimension of critical energy infrastructure'. After having presented his huge experience in the field of cyber-security, Mr Butrimas showed that cyber security is a priority for protecting critical energy infrastructure because the success of a cyber-attack is very likely (even more than in the case of a physical attack if infrastructures are not adequately protected). He pointed out the following important points: 1) the Industrial Control Systems (ICS) and Operational Technology (OT) depend on people, machines, automation, and IT to monitor and control a physical process; 2) Basic Process Control Systems (BPCS) are necessary for normal operations; 3) Safety Instrumented Systems (SIS) are programmed emergency actions to protect the facility and its people and bring a critical process back to a safe state, avoid loss of live, damage. Also, the priorities of the industrial control systems (ICS/OT) space are: safety, availability, integrity, confidentiality (SAIC). If the view or the control is degraded or lost, physical harm is likely. Mr Butrimas emphasised the difference between IT where the operation is securing the data and ICS where the operation is securing the operation. At the same time, he pointed out that the situation is changing because IT is coming to ICS/OT. Indeed, before the equipment was manually controlled while nowadays it is digital and remotely controlled. Before IT provided wonderful features and efficiencies for the operator. It supports the modern world but has introduced complexity and vulnerabilities. Additionally, cyber defense was not included as a requirement in ICS design. Mr Butrimas stressed that not understanding the difference between IT/OT will lead to bad policy and that IT introduced new vulnerabilities in ICS/OT world, in particular intentional and unintentional cyber incidents. For instance, "a nuclear power

plant was recently forced into an emergency shutdown for forty-eight hours after a software update was installed on a single computer". According to his experience, we are addressing cyber threats very well but it is not enough to focus on cybercrime threats. A real issue occurs when a cybercrime is the work of a state. He provided the following examples: 1) Iranian nuclear and oil facilities (STUXNET2010); 2) Saudi Aramco DOC attack 2012/2013; 3) Belgacom compromised 2013; 4) 2013 Sandworm Team / B.E. (ICS Reconnaissance); 5) 2014 BSI reports cyber-attack on German steel mill; 6) 2015 TV5Monde; 7) 2015/2016 Cyber attack on control systems of Ukraine's powergrid; 8) 2017 "WannaCry" as latest "wake-up-call". He stressed the CrashOverride 2017 case study in particular. In this case, an Advanced Persistent Threat (ATP) Group used a cyber-attack platform designed for power grids. It was 'the first OT malware designed to specifically attack electric grids' and 'was developed by an organization with resources and interdisciplinary skills with the sole purpose of impacting ICS operations across multiple targets'. In the future, there will be more IT/OT convergence and more vulnerabilities. IT will be characterized by the so called 'caveat emptor', which is the contract law principle that controls the sale of goods after the date of closing. This will imply:

1. "Industry 4.0" integrating manufacturing plant w/ business functions;
2. IIoT and DA "improve efficiency, reduce downtime and save money";
3. autonomous control and self-configuration;
4. getting a lot of support from government and industry in economic terms;
5. There will be not much to talk about about new vulnerabilities and cybersecurity.

This means that policy makers have failed to establish cyberspace rules and that the "Multi-stakeholder" governance model is obsolete. Consequently, the rules of the "wild west" prevail. Also, states, those they sponsor, and less skilled adversaries will continue to see this behavior as effective, cheap and deniable. Therefore, things are getting worse, and many have yet to "wake up".

Mr Butrimas closed its speech with the following key points to remember:

1. the lesson of the "3 little pigs";
2. protecting IT is not enough, forgetting OT can hurt you;
3. fighting cybercrime is not enough, other dangerous actors involved;
4. when developing policies, don't forget to invite the engineers;

5. can't defend from an APT by yourself, need to partner cooperate;
6. there is no such thing as "not connected to the Internet".

Mr Massimo Rocca, Head of Security Processes, System and Planning at Enel, gave a speech on 'Critical Infrastructures and information sharing'. He illustrated the current approach of Enel to critical infrastructures security. He stressed that at present the main challenge to the corporate security is the prevention of threats. The reason is the fast evolution of threats that spread very easily. Therefore, the main objectives are increasing the system resilience and giving to the company the capabilities to respond promptly and resolutely to weak signals. In order to do so, it is necessary to evolve from a 'reactive' to a 'proactive' approach. This means to involve all the organization and external peers, define processes, responsibilities and planning carefully.

Enel is a global and diversified operator and a global leader in renewables. It is present in Italy, Spain, Chile, Argentina, Colombia, Peru', Romania and Russia with operational assets and in more of 40 countries with construction, engineering and trading activities. It has a 40 billion euro Regulated Asset Base, 62 million distribution end users, and 18,3 million free retail customers. It has 38 GW renewable capacity and 47 GW thermal capacity. At the global level, the security organization of Enel is essentially based on security processes, systems and planning on the one hand, and on global security coordination and performance management on the other one. Through these tools Enel addresses global and local security threats, enterprise risks and crisis management. In the context of cyber security in particular, Enel operates globally according to the following framework of operation: 1) cyber security strategy, assurance, reporting; 2) cyber security monitoring and response; 3) cyber security information system engineering; 4) cyber security OT engineering. Finally, at local security level, the security operational organization of Enel is based on the following framework of operation: 1) intelligence and security risks analysis; 2) emergency management and personal protection; 3) infrastructure security and local operations; 4) security affairs and compliance. Mr Rocca illustrated the four process steps of Enel's security management. The first step is planning that includes the intelligence and the risk assessment and evaluation. The second step is protection including risk mitigation, which means people protection, infrastructures protection, and intangible assets protection. The third step is monitoring that includes residual risk evaluation and event detection. The fourth step is response consisting in incident and critical events management. Mr Rocca also discussed the most relevant applications concerning the corporate intelligence of Enel that are the following ones: a) counterparties analysis: prevention of the impacts on the Group's reputation and security enhancement through supply chain

monitoring; b) threats analysis: search of new threats affecting the company's assets and monitoring of the trends; c) travel/country security: analysis of the social, political and economic context in the countries where the company business is developing; d) reputation and sentiment monitoring: monitoring of the brand and top management reputation on press, web and social networks. In this context, there are two kinds of sources to be considered. The first ones are internal sources, namely systems logs, anomaly detection, incident reporting tools, anti-fraud controls, access control systems. The second kind of sources are external sources, which can be distinguished in two types; a) open external sources like social network, press, blogs, forum, wikis; b) legacy/proprietary/certified external sources like chamber of commerce, international services, national archives. Additionally, Mr Rocca identified the external sources potential issues that are publicly accessible, numerous and heterogeneous, potentially infiltrated by hostile actors (i.e. fake news), redundant and unstructured. However, he stressed that the analysis is more complex and the results are less reliable compared to internal sources. The illustration of a wider view of a threat scenario with a hierarchical order of threats (from the higher level down there are warfare, advanced/hybrid threats, new vulnerabilities, known vulnerabilities) shows that the private critical infrastructures operator has a reduced degree of autonomy in mitigating risks and facing threats due to limited resources, nature of threats, legal implications, and influence on the supply chain.

Furthermore, Mr Rocca emphasised the importance of information sharing and of PPPs. He said that in order to cover the gaps in cyber security Enel must cooperate with other utilities, institutions, and authorities in terms of information sharing, simulations, joint programs and trainings. Enel is a member of the European Energy - Information Sharing & Analysis Centre (EE-ISAC) that plays a key role in helping utilities to improve the cyber security and the resilience of their grid through trust-based data and information sharing. It "is an industry-driven, information sharing network of trust. Both private utilities and solution providers and (semi)public institutions such as academia, governmental and non-profit organizations share valuable information on cyber security & cyber resilience" (EE-ISAC, 2018). EE-ISAC members share: a) real-time security data & analysis; b) reports on security incidents and cyber breaches; c) technical & operational experiences with applied security solutions; d) lessons learned from past security issues; e) future challenges, security outlooks and warnings.

Also, Enel CERT is very important for the cyber security of the company. It is evolving from incident response to readiness, fostering the preparation for incident response and designating multidisciplinary people to cope with extraordinary events. Enel CERT mission is to support and protect Enel, from intentional and malicious attacks that would hamper its Constituency.

Enel CERT's activities cover the Cyber Security Incident: prevention, detection, response, recovery. Enel's constituency includes: Enel employees, Information systems and data assets, industrial assets and critical infrastructure. Its business lines are: thermal generation (OT-IT) renewables (OT-IT), corporate and markets (IT), infrastructures and networks (OT-IT), trading (OT-IT). IT and OT systems allocation is different for every business line. The Enel CERT Implementation Project involves different internal stakeholders and manages the activities of Enel CERT worldwide with an inclusive approach. Also, Enel CERT provides three processes to the Constituency in order to Prevent and Respond to Cyber Incidents and Threats. The first process is the Cyber Incident Response, which is a key process to Prevent, Detect and Respond to Cyber Incidents. Its key aspects are: 14 services from Service Activation to Recovery & Lessons Learned, Inclusive of all multidisciplinary Enel roles and capabilities, Full integration with existing Enel policies (i.e. Emergency and Crisis Policy). The second process is Cyber Threat Surveillance, that is a process to harvest privileged information related to cyber threats and attacking actors from multiple open, closed and commercial sources. Its key aspects are: create actionable information, relevant for Enel context, and early detection of cyber threats with potential impact to Enel Constituency. The third process is CERT information sharing that is a trusted communication process among all involved Internal Stakeholders and related External Counterparts. Its key aspects are: CERT Communication Workflow and Information Dissemination and Confidentiality management (Traffic Light Protocol).

Dr Richard Piggin, Specialist Warrant Officer of the UK Specialist Group Military Intelligence, gave a speech on 'Integrating cyber security with government and industry: standards and good practice". After having introduced himself and his huge expertise in the field, Dr Piggin illustrated the main threats of control systems, which are: a) Control devices reprogrammed -false information sent to operators to disguise changes or to initiate inappropriate actions; b) Modification of software or configuration producing unpredictable behavior; c) Denial of control action -unauthorised changes made to automation control programs, alarms or unauthorised commands sent to control equipment. They could cause damage to equipment, shutdown of processes, causing an environmental incident, or even disabling control equipment; d) Malicious software (e.g., Virus, Worm, Trojan) introduced into the system; e) Safety systems modified and fail to operate or perform incorrect actions that damage the control system; f) False status information sent to control system operators either to disguise unauthorised changes or to initiate inappropriate actions by system operators. He said that the IT and the Engineering sector have two different perspectives on control systems. IT perspective is based on confidentiality, integrity and availability. The engineering perspective is based on safety, reliability, and availability.

He identified the so called security headwinds, which are: 1) awareness of operational systems and their security nuances; 2) articulating OT organisational risk to the Board ; 3) establishing appropriate OT security governance; 4) determining responsibility and accountability for OT security, and managing the risk; 5) establishing effective collaboration across IT/OT and safety domains; 6) ICS security competency is scarce; 7) procurement. He also proposed some recent cyber security guidance: NIST Guide to ICS security; CPNI SICS; DoE C2M2 –risk assessment; DHS ICS Procurement language; NIST Cyber security framework; IEC 62443 ICS Cyber Security; VDI 2182 IT-security for industrial; automation; IAEA Nuclear Security Series; ANSSI Cybersecurity for IndustrialControl System; PAS 555 Cyber security risk –Governance and management specification; NRC 5.71 -Cyber Security Programs for Nuclear Facilities; UK ONR SyAps; UK Cyber Essentials; Defence Cyber Protection Partnership.

Dr Piggin illustrated the UK Civil Nuclear Cyber Security Strategy. He identified three main actors. The first one is the Government that includes the Department for Business, Energy and Industrial Strategy providing a strategic direction and the legal framework, the National Cyber Security Centre dealing with threat ad vulnerability intelligence, and the Nuclear Decommissioning Authority whose task is to enhance cyber security across the decommissioning estate and its subsidiarity. The second actor is Industry including Duty Holders that manage and mitigate their cyber vulnerabilities and assure the supply chain, and the Supply Chain that manages and mitigates cyber vulnerabilities and informs the Duty Holders of any compromises or vulnerabilities. The third actor are the Regulators including the Office for Nuclear Regulation that regulate cyber security and information assurance and hold industry to account on behalf of the public, and the Information Commissioner that upholds information rights in the public interests.

Dr Piggin also illustrated the life cycle approach to security that describes the activities for the development of electronic systems and the relationships between these activities. Computer security needs to be considered in all phases in IAEA draft guidance. Computer security should be coherently planned at the earliest opportunity for the entire C&I life cycle. In addition to the phases the C&I system lifecycle also involves common activities: quality assurance; configuration management; verification and validation; security assessment; documentation.

Dr Piggin emphasized the following points: 1) cyber-attack has been deemed a Tier One risk to the UK; 2) organisations, regardless of size or sector, need to take appropriate steps to protect themselves, and their customers, from the harm caused by cyber-attacks; 3) the Defence Cyber Protection Partner-

ship (DCPP) is a collaboration between government and industry; 4) industry is working with the MOD to improve the cyber resilience of the UK's defence supply chain.

Dr Piggin also stressed that assuring the cyber-security of Defence's supply chain through the application of risk based controls must be a priority. The following activities are also necessary:

1) simplifying cyber-assurance within Defence's supply chain through the implementation of a set of coherent and widely recognised standards; 2) accelerating the implementation of the National Cyber Security Strategy by ensuring the Defence sector's actions and the National Cyber Security Centre's actions are coordinated and mutually reinforcing; 3) enabling the improvement of cyber-security within Defence and other sectors by facilitating best practice sharing and learning from experience.

Given this background, Dr Piggin outlined the following key points: 1) effective cyber security is paramount to achieving comprehensive protective security and resilience; 2) cyber security of OT, especially basic plant control & instrumentation is of prime importance to government, industry and regulators; 3) compromise of plant systems may, as a minimum, have operational, regulatory, financial and reputational consequences; 4) mature approaches to security risk are essential if the benefits of digitisation are to be fully achieved ; 5) appropriate Governance is essential for successful, sustained security programmes; 6) the application of cyber security frameworks with an ICS focus, not just Information Assurance.

Finally, he suggested some recent papers for further information: 1) Cyber security of operational technology: understanding differences and achieving balance between nuclear safety and nuclear security; 2) industrial systems: cyber security's new battlefront; 3) Risk in the Fourth Industrial Revolution; 4) What should keep CEOs awake at night; 5) IET Cyber security of Ports.

Mr Andrea Foschini, Head of Information Security Governance, Direzione Tutela Aziendale at Terna, gave a speech on 'Information Security Standards, Development of a corporate Model'. He presented Terna that is a large TSO and the sole operator and owner of the Italian High-Voltage National Transmission Grid. It has 72,800 km of high-and extra-high voltage power lines (123/150 kV, 220 kV, 380 kV), 708 transformers and 855transforming stations, 1 Security Operations Centre, 25 interconnection lines with neighbouring countries. Terna has interconnections with more than 40 TSO in the EU in the ENTSO framework. Mr Foschini illustrated the main corporate networks that are" 1) ICS/SCADA sys-

tems (there is a central SCADA system as well as peripheral SCADA systems); 2) energy exchange; 3) corporate applications; 4) websites. He stressed a major need for Cybersecurity Corporate Governance.

Mr Foschini also discussed the development of the corporate cybersecurity standard. It occurred in seven years: 1) 2009: the Information Security Policy designated the Chief Information Security Officer; 2) 2011: the NIST 800.53 for Corporate Security Controls Baselines was adopted; 3) 2012: ISO27001 certification for Electricity Market Monitoring; 4) 2013: the Presidency of the Council of Ministers adopted the Italian Cybersecurity Strategy and the Terna Enterprise Risk Management was designed and the Chief Risk Officer was appointed; 5) 2014: the GRC was applied for the Security Plans Management; 6) 2015: the Italian Cybersecurity Framework was established; 7) 2017: the Policy Framework 2.0 was established.

Mr Foschini identified three key components of the security architecture. The first one is security processes. The Information Security body of policy defines 30+ cybersecurity policies. They identify security roles and responsibility for each role. All policies are mandatory and must be complied with. More than 50 operational procedures translate what has to be done into how to do it. These are defined from both Information Security department or the ICT department. The Corporate Security department periodically trains its people to assure awareness and commitment on information security. Process audits are performed too from the Corporate Security department, and other departments as well. Third Parties are targeted by specific initiatives in order to mitigate the risk associated. The second component are security roles. Roles are fundamental components to assure clear commitment, engagement and smooth processes. Terna has decided to tailor major NIST roles while maintaining a cross organization approach to assign cybersecurity responsibilities. The major roles are: 1) CISO: Chief Information Security Officer, accountable for information security operation and infosec processes/projects (SOC, VA/PT, IAM); 2) ISO: Information System Owner, accountable for asset classification (CIA) and protection; 3) IRO: Information Risk Owner is only one who can accept the residual risk after mitigation has taken place. The third component are the security controls. Risk Based approach and a Control Based Approach are mixed together at different levels of organization. In one statement: ICT operates compliance based security processes, assuring compliance to control baselines, Corporate Security operates risk based operations, tailoring security baselines to threats, incidents and changes of environment.

Mr Foschini also discussed the Risk Management Framework constituted of six steps: 1) categorize the information system; 2) select security controls; 3)

implement security controls; 4) assess security controls; 5) authorize the information system; 6) monitor security controls.

Finally, he discussed the Security control library that is structured into three levels of impact (low, medium, high, according to the NIST standard). Also, 800 controls are classified into four layers of applicability (processes, infrastructures and logistic, systems and applications) to minimize effort of running the security framework.

Mr Dainis Dravnieks, Senior Officer of Electricity Market and Infrastructure Division of the Latvian Ministry of Economics, gave a speech on "State Policy towards critical infrastructure in Latvia". He illustrated the legal framework for critical infrastructure, which consists of the following laws: 1) National Security Law (in force from 12.01.2001): Section 22 deals with Critical Infrastructure. The related laws are: Civil Defense and Disaster Management Law, Law on Emergency Situation and State of Exception, Law on Official Secrets; 2) Cabinet of Ministers Regulations No 496 (adopted 1 June 2010) "Procedures for the Identification of Critical Infrastructures, Including European Critical Infrastructures and Planning and Implementation of Security Measures"; 2) Commission of Intermediary Institutions for State Security-advisory collegial institution, which evaluates and improves the critical infrastructures, including European critical infrastructures, the aggregate of systems and security measures. The Commission shall operate in accordance with Regulation No 496.

According to these laws: 1) the Ministry of the Interior is responsible for updating the list of critical infrastructure objects; 2) the Security Police, the Constitutional Protection Bureau, the Military Intelligence and Security Service, the Ministry of Defence, the Ministry of the Interior, the Ministry of Economics, the Information Technology Security Incident Institution (Cert.lv) are involved in the protection of critical energy infrastructure; 3) energy companies have specific action plans. In case of a high and extremely high level of threat of terrorism, in the event of a state of emergency, the Critical Infrastructure owner or legal possessor coordinates his actions with the State Police, the National Armed Forces and the Security Police, the Constitutional Protection Bureau or the Military Intelligence and Security Service in accordance with the competence of national security authorities specified in regulatory enactments, taking into account the location of the relevant critical infrastructure and other specific factors.

Mr Dravnieks also discussed the Physical Security Policy of energy companies. The aim of the Policy is to provide a high quality, economically sound and consistent solution to the issues of physical security and information security. The main threats that the Policy identifies are natural disasters, sabotage, terrorism,

cyber-attacks, military assault. Also, according to the Policy, the government should stipulate a 3-year contract with Security company (for instance G4S, Securitas). The Policy has established a 24 h Security Control Center (monitoring: video cameras, thermal cameras). Energy companies have agreements with the Security Police counter-terrorism center, Ministry of the Interior (in particular the National Fire and Rescue Service), National Armed Forces, the Information Technology Security Incident Institution. Furthermore, the action plans should be applied according to defined 4 levels of terrorist threats. Threats and exercises are also envisaged: personal training, exercises on company level, high level national and international exercises (NATO CMX, KRISTAPS, BALTIC HOST).

Ms Dorota Leduchowska, Head of Crisis Management Unit of the Security Department at Polskie Sieci Elektroenergetyczne, gave a speech on 'Partnership between CI operators and public authorities'. After having stressed that the protection of critical infrastructure is an operator's duty, she illustrated the Polish National Critical Infrastructure Programme. According to this latter, protection means ensuring functionality, continuity and integrity of critical infrastructure. Protection has the following dimensions: physical, technical, personnel, IT, Legal, Recovery Plan. Between the public and the private bodies there should be shared responsibility, cooperation and trust. The main partners are the Government Centre for Security, the Internal Security Agency, the Ministry responsible for a critical infrastructure system, the critical infrastructure operator, and local and regional authorities.

Ms Leduchowska stressed the importance of information exchange in the cooperation in the area of critical infrastructure protection, which has three levels: 1) strategic level: National Critical Infrastructure Forum supported by system and regional forums; 2) operational level: direct and ongoing information exchange; 3) management level: trainings, exercises, conferences, advisory services. She said that there are several critical infrastructure protection forums, namely the National forum, the Regional Forum, and the System Forum (related to the Ministry responsible for the critical infrastructure system). The information exchange is a continuous process involving the Minister's Plenipotentiary that every year provides four reports for Government Centre for Security and the Minister for Energy. Another important element of critical energy infrastructure protection are the exercises that are held at the national, regional and local levels. An example is 'Tertyl' that was done in cooperation with the Police and without information in advance so that the situation was as real as possible. The scenario involved a suicide bomber that threatened to contaminate the area with radioactivity. The exercise consisted in a rescue operation and in the evacuation of the building.

Mr Leduchowska identified the best practices: 1) planning and training; 2) CIP Forums; 3) informal forums(networks) –"3 Musketeers" (the main areas are: Risk Assessment, Business Continuity Planning); 4) Cyber Protection (CERT PSE –INTERPOL, FIRST, USA, Austria, Norway, ISA, Gas-System etc). She also identified the main areas of improvement: 1) information sharing that is a one-way street; 2) too many CI operators and too few experts in the government (regional/central level); 3) new threats (e.g. disinformation); 4) involvement of academia. All these gaps make the partnership between the public and the private sector inefficient.

BIBLIOGRAPHY

EE-ISAC. (2018). *EE-ISAC*. Retrieved from http://www.ee-isac.eu/

OSCE. (2013). *Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace.* Vienna

OSCE. (2017). *Partners for cooperation.* Retrieved from http://www.osce.org/who/84

UNODA. (2017). U*N Security Council Resolution 1540 (2004).* Retrieved from https://www.un.org/disarmament/wmd/sc1540/

Conclusion and Recommendations to NATO members

The aim of this chapter is twofold. On the one hand, it tries to draw the main conclusions from the analysis conducted in the previous chapters. On the other hand, it tries to identify some recommendations to NATO members that could be useful to improve the protection of critical energy infrastructure on the basis of the results obtained from the analysis conducted in this study and from the Expert Level Workshop held on the 24th of October.

This study has shown that every state considers the protection of its critical energy infrastructure as a priority because the well-being of its society depends on the functioning of infrastructures ensuring the uninterrupted supply of energy. The four case-studies taken into consideration here, namely Estonia, Italy, Latvia and Lithuania, are clear examples of this. Indeed, although each of them has its own national strategies with specific geopolitical and economic aims, all of them consider the protection of critical energy infrastructure as a state priority. These cases also have some other similarities such as the crucial role that energy security plays in their national strategy that means, inter alia, diversification of supplies, in particular from Russia. This is true not only for Estonia, Latvia and Lithuania but also for Italy that is very much dependent on Russian gas. These elements are also common to Italy that is a different case from the other three for political, economic, geographical and historical reasons. The four cases are updating and expanding their energy infrastructure in order to increase their energy security and to connect to other states. For instance, Estonia, Latvia and Lithuania are building new infrastructure connecting them to each other and to Northern Europe and Poland while Italy is building new pipelines to import gas from the Caspian region that serves its purpose to become a Southern Gas Hub. Furthermore, all of them are EU members. Therefore, they are subject to the same supranational legislation that must be transposed into their national one and are part of the EU Energy Strategy. All of them are also members of NATO that is very much committed to increase their protection of critical energy infrastructure not only by creating an acquis through concepts

and summit declarations but also practically through Table Top Exercises such as the ones that it has organised over the last few years. They have been a success as they have contributed to increase strategic awareness of the security implications of energy developments and to information sharing, which are essential not only to help states to improve the protection of their critical energy infrastructure but to achieve NATO's goals in the energy field more generally.

Furthermore, the analysis has shown that PPPs are of utmost importance in the protection of critical energy infrastructure because they are mostly owned by the private sector. As the protection of critical energy infrastructure is strictly linked to national security and as the private sector often needs the help of the state authorities to protect it, a partnership between the public and the private sector is of utmost importance. However, real partnerships are difficult to achieve because the interests of the public and of the private sectors do not often coincide and because there is lack of trust between them that translates into lack of information sharing. This is also the conclusion drawn from the Expert Level Workshop that has clearly raised the issue. Therefore, both the discussion conducted in this study and in the workshop have stressed that the human factor (lack of trust) and information sharing are paramount to establishing functioning PPPs.

In this context, the workshop has also highlighted that the involvement of the state authorities at different levels is essential to protect critical energy infrastructure in various kinds of emergencies and crises. Of course, this must occur according to the state procedures and to the specific situation at stake. Also, an element that emerged from the discussion was that energy companies are ready to cooperate but they expect more cooperation from the authorities, in particular the local ones. It is also important that all stakeholders/owners of critical energy infrastructure from all sectors (oil, gas and electricity) cooperate with each other because sectors are interdependent. Therefore, a disruption in the critical infrastructures of one sector may cause disruptions in the infrastructures some others.

Another conclusion drawn from the workshop is that cyber security is nowadays essential for the protection of critical energy infrastructure because they are mainly controlled through technology. In this context, the continuous updating and training of the company's staff dealing with IT is essential. Additionally, the reliability of the personnel is very important for cyber security. This is why strict controls on it are necessary.

Furthermore, as highlightened in the analysis conducted in this study, the commitment of international organisations such as NATO and the OSCE in protect-

ing critical energy infrastructure is also of utmost importance because they concretely contribute to information and knowledge sharing among their members. The Table Top Exercises organized by NATO and the national exercises organized by the OSCE are an excellent example of the work of international organisations in the field of critical energy infrastructure protection and in the energy sector more broadly. It is necessary to stress once again here that the EU is not considered as an international organisation but as a supranational entity whose legislation impacts the ones of the member states as it is evident both from the analysis of this study and from the discussion conducted in the workshop. This latter has indeed clearly shown that the EU legislation and strategies guide and support the national ones although the protection of critical energy infrastructure remains a national competence.

Additionally, another consideration pertains to the fact that the protection of critical energy infrastructure is not merely a national issue as the disruption of energy supply and the destruction of a part of energy infrastructure may affect not only the state where they occur but also other states. This is clear not only from the fact that states (like in the case of the four case studies analysed here) depend on infrastructure to import energy from abroad but also from the fact that they are building new infrastructures to increase their connections with other states.

This last consideration is the basis on which recommendations to NATO members and NATO partners in order to improve the protection of their critical energy infrastructure have been divided. In particular, recommendations are divided into two groups, namely recommendations concerning the national level and recommendations concerning the international level. This division is made for a mere reason of convenience as this would make the recommendation clearer and more understandable. However, the two levels are strictly intertwined as it has been argued above.

RECOMMENDATIONS CONCERNING THE NATIONAL LEVEL:

1. The state should elaborate a clear strategy for the protection of critical energy infrastructure, which should be disseminated among all stakeholders/owners of critical energy infrastructure together in order to spread the awareness of the need of a coherent policy in the field at the national level;
2. Best practices should be shared by all stakeholders/owners of critical energy infrastructure in order to increase information sharing among them. This should also include the state authorities as a mutual exchange of knowledge and information is essential for an effective protection of infrastructures. This implies that the stakeholders/owners of critical energy

infrastructure share updated knowledge and information about: a) their risk management programme including the analysis of the possible threats, the risk assessment, the vulnerabilities, and the implementation of hazard mitigation procedures; b) the main vulnerabilities of the infrastructure they manage; c) the threats they have faced and the solutions that they have adopted to face them;

3. The exchange of knowledge and information among all stakeholders/owners of critical energy infrastructure should lead to the development of common standards to achieve at the technical level. This is desirable in order to achieve common security arrangements ensuring minimum levels of protection;
4. stakeholders/owners of critical energy infrastructure should ensure that the public authorities at all levels involved in the protection of infrastructure are continuously informed and updated about eventual new vulnerabilities and threats stemming from new technology;
5. stakeholders/owners of critical energy infrastructure should closely cooperate with the public authorities to increase their preparedness to eventual threats. This implies a more efficient contingency planning as well as intensifying the number of exercises practiced in cooperation by the private and the public sectors;
6. as the human factor is of utmost importance in the cooperation between the public and the private sectors, these latter should work closely in order to strengthen the relationships between their respective staff. For instance, this can happen if the two sectors increase their contacts through information sharing;
7. as PPPs are just one form of cooperation between the private and the public sector, some other ways of interaction can be found. These can be special-purpose associations mandatory for companies or incentives to support networks through promotion or consultancy (Dunn-Cavelty and Suter, 2009);
8. the public authorities from the governmental to the local level should increase their coordination in order to define a more coherent national strategy for critical energy infrastructure protection. This can be done only if the cooperation with the private sector is efficient;
9. the private and the public sectors should practice regular exercises and tests because they ensure that the personnel becomes confident in handling and acting on material. Exercises and tests increase the ability of the staff to respond and its confidence in what it is doing. Additionally, exercises and tests help identify new vulnerabilities (OSCE, 2013);
10. the public and the private sectors should be ready to coordinate their efforts to allocate both human and financial resources to protect critical energy infrastructure.

RECOMMENDATIONS CONCERNING THE INTERNATIONAL LEVEL:

1. states should agree on a common definition of critical infrastructure in order to address the protection of critical energy infrastructure issue on the basis of a shared understanding of the problem. This would also make communication on the issue among them easier;
2. stakeholders/owners of critical energy infrastructure should cooperate with neighbouring states in order to increase the ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event that has a negative impact beyond the borders of a state. This would increase the effectiveness of a resilient infrastructure. This is essential especially because many businesses that make up critical energy infrastructure are multinational companies;
3. cooperation to protect critical energy infrastructure should involve not only the stakeholders/owners of critical energy infrastructure but also governments. They should agree on common measures and standards to ensure an adequate protection of infrastructures that involve more than one state;
4. EU members that are also NATO members should reinforce the coordination of their activities aiming at protecting critical energy infrastructure at the EU level. This would benefit also those NATO members that are not EU members (e.g. Norway) because an increased resilient critical energy infrastructure of a state also increases the security of the critical energy infrastructure of the neighbouring states;
5. It would be desirable that NATO members reinforce their cooperation in the field of cyber-security, which is a key area in the protection of critical energy infrastructure;
6. NATO members should increase their cooperation at the state level to protect their critical energy infrastructure at NATO level. This could happen if NATO increases its commitment to contribute to this aim, but member states should push the organization to be more active in the field. It is indeed of utmost importance that NATO strengthens its efforts to protect the critical energy infrastructure of its members by elaborating a clear strategy for all of them. In this context, it would be desirable that NATO coordinates its activities with the EU in order to avoid duplications.

All in all, although states have a high degree of critical energy infrastructure protection, there is still room for improvement especially in two areas, namely the coordination of the activities of the state authorities and of stakeholders/owners of critical energy infrastructure, and international cooperation.

NATO Energy Security Centre of Excellence

Šilo g. 5A, LT-10322 Vilnius,
Lithuania
Phone: +370 706 71000
Fax: +370 706 71010
Email: info@enseccoe.org
www.enseccoe.org.