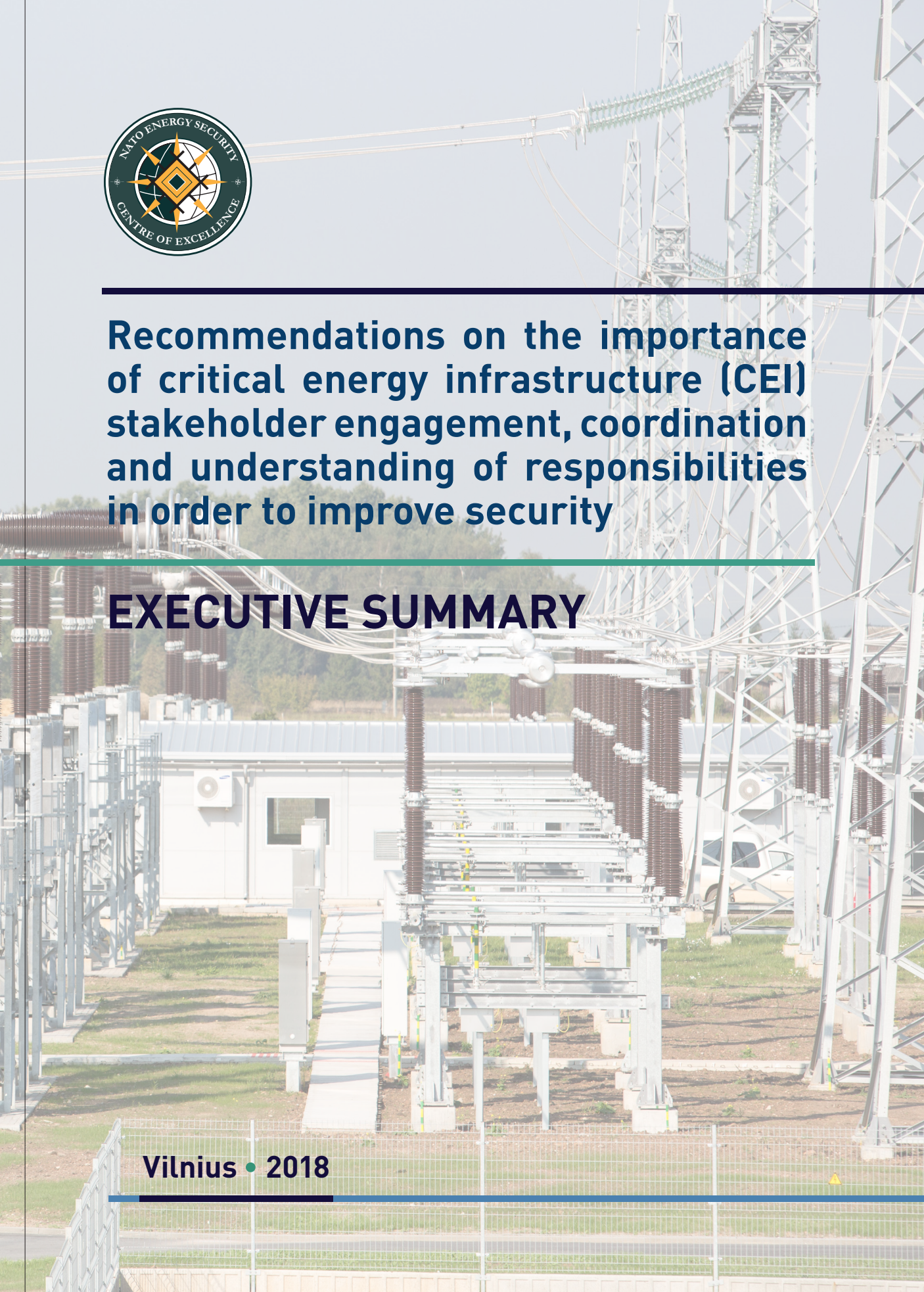

Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security

EXECUTIVE SUMMARY

Vilnius • 2018

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

EXECUTIVE SUMMARY

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

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

- The main objective of this study, which was requested from the Lithuanian Ministry of Foreign Affairs, is to give general recommendations to 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.

- As a consensual definition of 'critical infrastructure' does not exist, this study has deduced it from the ones provided by the US, NATO and the EU. Therefore, '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'. Critical energy infrastructure is a key factor of energy security that is defined by the International Energy Agency as 'the uninterrupted availability of energy sources at an affordable price'.

- Although most critical energy infrastructures are owned by the private sector, the government has the responsibility to regulate it and also to protect it to some extent especially where protection is too important to leave to the private sector. In order to protect critical energy infrastructure, the definition and the implementation of a risk management programme is essential. The risk management programme should incorporate the analysis of the possible threats, the risk assessment, the vulnerabilities,

and the implementation of hazard mitigation procedures. In this context, the risk analysis is particularly important because it is useful to determine the likelihood that an event occurs.

- Public-Private Partnerships (PPPs), which are long-term contracts between a public agency or public sector authority and a private sector entity, are a key factor in the protection of critical energy infrastructure. They are crucial to efficiently respond to the escalating worldwide threats that may jeopardize the good functioning of critical energy infrastructures. In spite of this, the establishment of PPPs is not an easy process for a number of reasons. One reason concerns the fact that the interests of the state and of companies do not coincide. Indeed, while the main interest of the state is national security, companies are very much business-oriented. This means that these latter accept to make critical energy infrastructure 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. Another reason concerns the problem of information sharing. The private and the public sectors are not always willing to 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.

- The sensitiveness of the problem concerning the protection of critical energy infrastructures has led the European Union (EU) to contribute to improve the protection of critical infrastructures in its member states. To this aim, it issues legislation and documents aiming at regulating it that the member states must transpose into their national legislation. At the same time, the European Union has also put in place several programs like the European Programme on Critical Infrastructure Protection (EPCIP) whose aim is to improve the protection of and to increase the resilience (against all threats and hazards) of critical infrastructures in the EU. The underlying rationale is that the 'disruption to infrastructures providing key services could harm the security and economy of the EU as well as the well-being of its citizens'. Another example of the EU's strong commitment to the protection of critical infrastructures in its member states is the European Network of Transmission System Operators (ENTSO-E) whose objective is

further liberalising the gas and electricity markets in the EU.

• Given the fact that the protection of critical infrastructure protection is a very important issue for the Allies, NATO has also committed to contribute to it mainly through documents and declarations aiming at forming a kind of acquis. A good example are the documents issued in 2017 by the Industrial Resources and Communication Services Group (IRCSG). Their aim is to 'support national policy makers and relevant authorities in their efforts to review their national sectoral arrangements'. Additionally, NATO Energy Security Centre of Excellence also plays a role in this context especially with the Table Top Exercises on critical energy infrastructure protection organised in Vilnius and in Kiev.

• Estonia, Italy, Latvia and Lithuania are the four case studies taken into consideration in this project. Italy is obviously very different from the other three states. The reason why it has been included in this project is that Italy adds value to the analysis not only because it is a good example of a big country with a huge energy market, but also because of its geopolitical, economic, and historical characteristics. Energy companies and ministries from the four states have provided answers to a questionnaire that was submitted to them in order to access information that are important to the aims of this project and that are not available on internet and on printed material.

• Elering, an Estonian transmission system operator for electricity and natural gas, has provided answers to the questionnaire for the Estonian case. It stressed that the main threats from which Estonia needs to protect its critical energy infrastructure concern technical failures, difficult weather conditions (e.g. high winds and floods), cyber-attacks and physical attacks. The energy system is protected with IT means, but Elering has agreements with security companies. In the worst scenarios also the state authorities intervene. Additionally, regular internal trainings, trainings with other Baltic Transmission System Operators and with service providers as well as trainings organised by state institutions are also important to get prepared in case of threats or disruptions. In this context, another element that has emerged from the analysis is that Estonia is trying to improve its energy

infrastructure with the aim to diversify its energy supply. In particular, the links with Finland through Estlink 1 and Estlink 2 and the Baltic Connector gas pipeline project aiming at strengthening Estonia's energy relations with the other states in the region and contribute to its independence from Russian gas are good examples.

- As for the Italian case, Terna, an electricity transmission system operator, Ente Nazionale Idrocarburi (ENI), an Italian multinational oil and gas company, and Snam, a natural gas infrastructure company, have provided NATO ENSEC COE with answers to the questionnaire. According to the analysis of the questionnaires, the Communication and Information and Technology (ICT) systems can be considered as the main vulnerabilities of critical energy infrastructure while cyber-attacks are the most serious threats. The protection of critical energy infrastructures involves the cooperation between energy companies and state authorities (PPPs), which are fundamental for coordinated intervention in emergency situations, in case of threats as well as for information sharing. Furthermore, Italy is diversifying its energy supplies. In this context, among Italy's main aims there are creating a competitive gas market and becoming a Hub Southern Europe. In order to do this, Italy is strengthening its energy infrastructures. A good example is the Southern Gas Corridor (SGC) that concerns Italy in relation to one of the several energy projects of which it is constituted, namely the Trans-Atlantic Pipeline (TAP).

- The Ministry of Economics of Latvia has provided NATO ENSEC COE with answers to the questionnaire. The analysis has highlighted that the main threats to critical energy infrastructures are natural disasters, sabotage, terrorism, military assaults and cyber-attacks. While energy companies have their own plans to face these threats, the public authorities are involved in the protection of critical energy infrastructures according to specific procedures. Also, the Ministry of Economics provided interesting information on the complex procedure to identify critical energy infrastructures. The Latvian transmission system was upgraded in 1991. This has allowed Latvia to increase its interconnections with the other states in the region. In this context, the Baltic Energy Market Interconnection Plan (BEMIP) is of utmost importance as its aim is to create an open and integrated regional energy

market in electricity and gas between member states in the Baltic Sea region. The expansion of the Inčukalns Underground Gas Storage (UGS) Facility, which is the only underground gas-storage facility in the Baltic Sea region, is another example.

- Amber Grid AB, a Lithuania's natural gas transmission system, has provided NATO ENSEC COE with answers to the questionnaire. According to Amber Grid AB, cyber security is the most critical field for the protection of critical energy infrastructure both because competent people are lacking and because the budget for the acquisition of the necessary equipment is insufficient. Amber Grid AB also stressed that in Lithuania an important element of the protection of critical energy infrastructure is that all energy companies plan the necessary investments and implement the necessary measures to ensure it. These requirements are regulated by the Lithuanian laws that also define in detail which bodies are involved in the protection of critical energy infrastructure. Amber Grid AB has set out a Physical Security Plan to physically protect its critical infrastructures. Furthermore, Lithuania is improving its electricity and gas infrastructure both by modernising it and by implementing new projects like the Klaipeda Liquefied Natural Gas (LNG) terminal that has increased the number of suppliers in the country and Nordbalt connecting the electricity infrastructures of Lithuania and Sweden. These two projects also serve Lithuania's aim of diversifying its energy supplies in order to become less dependent on Russian energy.

- On 24th October 2017, NATO ENSEC COE held the Expert Level Workshop "Critical Energy Infrastructure Protection: the importance of the Public-Private Partnership". 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 highlighted the civilian and the military aspects of critical energy infrastructure protection and discussed the involvement of the public authorities and of energy companies in the process.

- **CONCLUSIONS:**

1. the four cases included in this study, namely Estonia, Italy, Latvia and Lithuania, clearly show that critical energy infrastructure protection is a top priority for every state;

2. PPPs are a key element for the protection of critical energy infrastructures. In spite of this, it is difficult to establish real PPPs mainly because of two elements. The first one is that the interests of the state and of companies do not coincide. The second element is the lack of information sharing;

3. it is essential that stakeholders/owners of critical energy infrastructure of all sectors (oil, gas, and electricity) cooperate among themselves because a disruption in the critical infrastructure of one sector may have negative consequences in the other sectors as they are interdependent. For this reason, they should share best practices, knowledge and information;

4. stakeholders/owners of critical energy infrastructure should cooperate with neighbouring states because energy infrastructures of neighbouring states are interdependent. This would increase the effectiveness of a resilient infrastructure;

5. energy companies are ready to cooperate but they expect more cooperation from the state authorities;

6. cyber security is the most sensitive vulnerability of critical energy infrastructures because they are mainly controlled through technology. Therefore, the continuous updating and training of the staff is essential. Also, the reliability of the personnel is very important;

7. the commitment of international organisations such as NATO and the OSCE in protecting critical energy infrastructure is of utmost importance because they concretely contribute to information and knowledge sharing among their members. However, NATO should adopt a clear strategy to better contribute to the protection of the critical energy infrastructure protection of the Allies.

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.