Energy Security: Operational Highlights

No 11 • 2017

Contents

Editorial

Dr Arturas Petkus
Head of Strategic Analysis Division
NATO Energy Security Centre of Excellence

The protection of critical energy infrastructure (CEI) and its role in ensuring the energy security of a state are the core topics of this issue of 'Energy Security: Operational Highlights'. These topics are of utmost importance in the NATO context because a disruption of energy supplies can negatively affect both the well-functioning of its members' societies and its military operations. Therefore, protecting CEI from all possible threats and increasing its resilience is crucial in order to achieve the goals of energy sustainability, economic and social development. At the same time, it is necessary to ensure that NATO implements its military strategies and achieves its political objectives.

Furthermore, the recent Russia-Ukraine crisis of 2014 has clearly demonstrated the importance of CEI for states. It has shown that CEI has become a military target in conflicts and that energy can be an element of "hybrid warfare".

Consequently, the implementation of a risk management programme, incorporating analysis of the vulnerabilities, risk assessment and implementation of hazard mitigation procedures is essential in order to protect CEI. In this context, the establishment of a Public-Private Partnership (PPP) is important because coordinating the efforts of stakeholders, bodies and institutions is necessary to ensure an effective protection of CEI.

These factors are discussed in the four articles included in the current issue of this journal.

Mr Michael Rühle provides an overview of the major changes occurred in the international arena during the last years with a focus on energy and geopolitics. More specifically, he focuses his analysis on the main political and technological upheavals that have led to significant changes in the global energy landscape. In doing so, he illustrates eight main lessons that can be deduced from those changes and that must be taken into consideration when evaluating the current geopolitical situation with a focus on the energy sector.

Mr Antti-Pekka Manninen and Mr Heiki Jakson discuss the protection of CEI in the case of Finland, arguing that its security policy can serve as an example for the protection of CEI in other states at least in some respects. They link the Finnish case to the broader international context with an emphasis on the approaches of NATO and the European Union (EU) to CEI.

Mr Emanuele Nicola Cecchetti and Mr Heiki Jakson discuss the importance of energy in conflicts by focusing on the destruction of CEI in the Ukrainian crisis of 2014. After providing a short historical overview of the evolving role of energy in conflict throughout history, the authors analyse the main events of the Ukrainian crisis of 2014 showing that CEI was a major military target for Russia. Also, they briefly discuss the measures that NATO adopted in order to protect its member states and the essential role played by its Centres of Excellence to support its work.

Prof Dr Oleksandr Sukhodolia analyses the conflict between Russia and Ukraine in 2014 with a focus on the Russian attacks on CEI in Ukraine. The analysis shows that the Ukrainian crisis has contributed to incorporate energy in hybrid warfare and that threats to CEI are an essential part of it. Additionally, the author suggests that the protection of CEI should be included into the national defence policy of states. At the same time, he stresses that the establishment of Public-Private Partnerships (PPPs) and civil-military cooperation are essential in order to ensure an efficient protection of CEI.

Finally, Ms Moniek de Jong and Prof Larry Hughes discuss the identification and the protection of CEI. After defining CEI, the authors analyse the types of threats that can affect its functioning and the necessary countermeasures that can help protect CEI. Additionally, they outline the various levels of CEI protection at which private companies are willing and capable of protecting it by showing that states also contribute to provide security in the form of police or military presence.

Energy Security: **Eight Relevant Lessons**

Michael Rühle, NATO Headquarters, Belgium

The global energy landscape is transforming. New energy suppliers are entering the market, new pipelines are connecting producers and consumers. Renewables, such as wind and solar energy, are becoming economically viable. Deep offshore drilling, the "fracking" of gas from rock formations, and the liquefaction of natural gas are changing the global market. LNG (Liquefied Natural Gas) tankers enable the transport of gas by ship, just like oil, thus becoming more independent from pipelines. New interconnectors and the "reverse flow" of pipelines provide more flexibility for transporting energy across Europe way beyond its entry point, and encourage energy trade via dynamic "spot markets".

For European consumers, this could be good news. A flexible energy market means lower prices and greater security of supply. However, turning such an optimistic scenario into reality requires considerable effort. Achieving true energy security requires drawing the right lessons from the political and technological upheavals of recent years.

Eight concrete lessons stand out:

First, the Russia-Ukraine crisis has demonstrated that energy can be an element of "hybrid warfare". By annexing Crimea, Russia did not only illegally acquire Ukrainian territory, but also seized Ukrainian energy infrastructure on the peninsula as well as offshore installations in the Black Sea. The annexation of Crimea also allowed Moscow to renege on previous agreements with Kiev on renting the Sevastopol naval base, such as granting Ukraine a lower gas price. Although Ukraine is not a NATO member, Russia's skilful application of military and non-military means to destabilise its neighbour has sparked a lively debate in the West about how best to meet the challenge of "hybrid warfare". As the Russia-Ukraine crisis shows, an effective answer can only be found if the energy dimension is included in the analysis.

Michael Rühle, NATO Headquarters, Brussels

Michael Rühle is currently Head of the Energy Security Section, in the Emerging Security Challenges Division of NATO's International Staff. Previously he was Head, Speechwriting, and a Senior Political Advisor in the NATO Secretary General's Policy Planning Unit. Before joining NATO's International Staff in 1991, Mr. Rühle was a Volkswagen-Fellow at the Konrad-Adenauer-Stiftung think-tank in Sankt Augustin, Germany, and a Visiting Fellow at the Center for Strategic and International Studies (CSIS), Washington, D.C. He holds an M.A. degree in Political Science from the University of Bonn, Germany. Mr. Rühle has published widely on international security issues in American Foreign Policy Interests, Asia Times, Comparative Strategy, International Affairs (Chatham House), NATO Review, Parameters, Politico, and The World Today, as well as other titles.

Second, Europe's energy dependence on Russia remains a strategic liability. For the foreseeable future, Russia will remain a major gas supplier to Europe, since Moscow can, in principle, outbid almost any contender. But the ritually invoked "mutual interdependence" of producer and consumer has not tempered Russia's determination to dominate its immediate neighbourhood, including by using gas as a political and economic tool. Moreover, the falling oil price has brought home how much the Russian economy depends on the sale of fossil fuels, and how little has been done to diversify the country's economic foundations. This could spell bad news: Russia's economic decline could tempt its leadership to embark on foreign policy adventurism in order to solidify its power at home. The West would then have to deal with an even less predictable Eurasian great power.

Third, solidarity among European countries, as well as between Europe and North America, will no longer be measured exclusively in military terms, but also in the energy domain. The role of the EU as an intermediary in the gas dispute between Russia and Ukraine, the successful efforts to re-route Russian gas through Poland, Hungary and Slovakia to Ukraine, and the steps toward an Energy Union are important signals: within Europe, a new form of solidarity is emerging that benefits even non-EU countries such as Ukraine. Transatlantic solidarity, too, will acquire an energy dimension: with the technical and legal conditions now in place, US LNG can now be exported not only to Asia but also to Europe. The lower demand for US LNG in Asia has made the European market more interesting for the United States. In April 2016, the first American LNG tanker left its Louisiana port heading for Portugal.

Fourth, the changes in the global energy landscape will lead to a greater emphasis on maritime security. Today, two thirds of global oil shipments are transported by sea, and the increase in LNG shipments will further add to this percentage. Since these ships have to pass important straits like Hormuz or Malacca, they are vulnerable to piracy and military blockades. In the Gulf of Aden NATO and EU are already engaged in a counter piracy mission that has resulted in a considerable drop in the number of attacks on naval vessels. Although the energy security benefits of such operations are only indirect, they do bring home that the protection of maritime trade routes through the collective employment of naval power is bound to become an integral part of a comprehensive energy security strategy.

Fifth, the challenge of cyber attacks will increase further. More than a third of all known cyber attacks target energy infrastructure. The increasing computerization of this infrastructure, but also the increasing use of computerized control systems in private homes, open gateways for cyber attacks by private hackers as well as by state actors. Since most energy and cyber networks are in private hands, trustful cooperation both between private enterprises as well as between industry and government institutions will be essential. Building such "communities of trust", wherein one exchanges confidential information, will be one of the major challenges in the years ahead. Companies will also have to develop a better understanding of the need for investing in cyber defence, and not simply discard such financial investments as detrimental to one's competitiveness. Another challenge is the training of energy infrastructure operators: the damage inflicted by the reckless handling of computers and storage media could be much reduced by better training.

Sixth, more attention must be devoted to the role of energy in regional conflicts. While the spectre of outright "resource wars" is still distant, energy and natural resources are increasingly becoming a factor of international security policy. The territorial disputes between China and several neighbouring countries about islands in the South and

East China Sea clearly have an energy and resource dimension. Other examples where energy issues could lead to conflict might include an oil discovery in a region claimed by two states, or a dam project in an arid region, which compromises the water supply of a neighbouring country. The "Islamic State" has added another dimension to the link between energy and (in)security: before US air strikes put an end to its economic activities, the terrorist militia had succeeded in amassing assets worth billions of Dollars via illegal oil production in the areas it had occupied.

Seventh, the changes in the global energy landscape also mean geopolitical shifts. In the US, low energy prices have helped spark a "second industrial revolution". For the traditional energy producers in the Middle East, in turn, who used to "buy off" their populations through generous subsidies, the drop in oil prices could translate into political unrest. The same applies to the energy producers in Latin America and West Africa: in some states, the low oil price has resulted in domestic crises that push them to the brink of state failure. While Russia will not be hit quite as hard prices as, for example, Venezuela, Moscow will also have to change its business model. Through projects such as Nord Stream II Russia will continue to try to maintain its strong role as a gas supplier to Europe (and eliminate Ukraine as a transit country), while at the same time seeking to compensate for its declining European market by exporting to Asia. However, the fact that Russia failed to charge China European-level prices indicates who will be the winner and who will be the loser in this new "energy partnership".

Eighth, NATO's agenda needs to reflect the different links between energy and security. NATO is neither an energy institution, nor do allies want to militarize the issue of energy security. However, the relationship between energy and security is too obvious to be ignored. Concretely, this means that allies must enhance their intelligence sharing on energy developments, add energy security into the curricula of its education and training facilities, and incorporate energy scenarios into its exercises. It also means that NATO must develop closer relations with the EU and the International Energy Agency (IEA), in order to benefit from the unique expertise of both institutions. The fact that energy developments are now being discussed at the level of the North Atlantic Council demonstrates that NATO has started adjusting to a world where energy and security are inseparable. As former NATO Secretary General Manfred Wörner used to say, history does not hold back its surprises until we feel ready for them.

Critical Energy Infrastructure Protection through Comprehensive Security – **The Finnish example**

Antti-Pekka Manninen, KPMG, Finland
Heiki Jakson, Elektrilevi, Estonia

This article discusses the Finnish comprehensive security policy as an example of a good approach to protect the critical energy infrastructure of a state. After analysing the regional standardization efforts, the focus will be on the Finnish approach to the issue of critical energy infrastructure protection and to the possible best practices that could be drawn from it. Even though cyber security is widely emphasized in the Finnish security strategy, this field is knowingly left aside here, and the analysis focuses more generally on critical infrastructure protection.

INTRODUCTION

The conflict in Ukraine in 2014 clearly showed that energy security is – and should be – a major issue in the geopolitical strategies of states. It not only unveiled the risks of energy geopolitics, but also demonstrated the threats that attacks on energy infrastructure can pose to civilian populations. During the conflict several incidents involving artillery fire on electricity transmitters occurred. An example is the case of the Kievsky district power station that was damaged by artillery fire leaving hundreds of people stranded underground in the Zasyadko mine (Luhn, 2015). Although being reprehensible from the international humanitarian law perspective, the possibility that these kinds of attacks against civilian electricity distribution networks can occur should not be neglected when planning the necessary measures for the protection of the society.

Antti-Pekka Manninen, KPMG, Helsinki

Antti-Pekka Manninen is a cyber security specialist at KPMG Finland, advising public and private sector clients in wide range of data protection and cyber security issues. He has an academic background in law and international relations, focusing mainly on regulatory issues relating to security in the information society. Before starting in his current position, Antti-Pekka gained professional experience in the public sector, including the Ministry of Foreign Affairs and Ministry of Defense in Finland. He did his internship at the NATO ENSEC COE in the Strategic Analysis and Research Division in 2014.

Nowadays, the most imminent threats to energy systems in most countries are natural catastrophes such as storms and floods. Still, as the energy transmission and distribution networks form a fundamental part of the critical infrastructure of a state, they are some of the most serious vulnerabilities in modern societies. Therefore, they can become targets of terrorist attacks or strategic strikes during hostilities. The existence and the seriousness of this risk means that disruptions caused by intentional acts should be a key element in threat scenarios concerning the protection of energy infrastructure. The most probable *intentional* attacks towards energy infrastructure would most likely be the physical destruction of transmission substations or cyber attacks targeting the supervisory control and data acquisition (SCADA) systems controlling the infrastructure. Sabotage, cyber attacks and other clandestine operations, whether organized by a nation state or by non-state actors, are the most viable threats especially during armed conflicts, and the possible consequences of these threats must be included in the main priorities during the planning phase of any strategy addressing energy infrastructure security (Jakson et al., 2017). As these threats are often unforeseeable and can have serious consequences, it is not possible to prevent them by hardening the targets only, but resiliency measures are also required. Nevertheless, resiliency cannot be achieved only through technical solutions, but political and legal considerations are also fundamental to ascertain the necessary societal context for a sufficient level of protection. As the situation in Ukraine shows, critical energy infrastructure protection (CEIP) should be prioritized in planning against threats in any modern state that is reliant on energy.

One approach to the threats described above is the Finnish comprehensive security approach, which aims to empower the whole society to participate in the common security agenda through the framework of *functions that are vital to the society*. Before describing the national approach, a brief review of some regional approaches to critical energy infrastructure protection will be provided.

This article is divided into five sections. The first one discusses the notion of Critical Energy Infrastructure as defined by different international actors. The second section focuses on the approaches taken by the North Atlantic Treaty Organisation (NATO) and the European Union (EU) to address the issues related to CEIP. The third section analyses the Finnish case example, where the comprehensive security approach is used to encompass CEIP into the strategic planning. The fourth section will continue developing this topic by focusing on the actors which are tasked to implement these notions into practice. The fifth section will discuss the possible lessons learned from this kind of approach.

THE NOTION OF CRITICAL ENERGY INFRASTRUCTURE

The use of the expression 'critical energy infrastructure' in this article is mainly based on the NATO and EU approaches to critical infrastructure protection in general. As there is

Heiki Jakson, Estonian Electrical Distribution System Operator, Tallinn

Heiki Jakson is currently working as electrical engineer for Elektrilevi (Estonian Electrical Distribution System Operator - DSO). Previously, he was a Subject Matter Expert at NATO ENSEC COE working on Critical Energy Infrastructure Protection topics. He has also worked as an electrical engineer in the electrical infrastructure construction sector and has a MSc degree in power engineering from the Tallinn University of Technology. Additionally, he has also been an infantry officer in the Estonian Defence League (which is a voluntary military national defence organisation) since 2003.

[1] SCADA systems are a type of industrial control system used to monitor and control large systems remotely.

no single definition available for the criticality of the infrastructure, the different definitions will be briefly presented here.

NATO's approach to critical energy infrastructure is strongly connected to civil preparedness and Civil Emergency Planning (CEP). The approach towards critical infrastructure protection adopted by NATO is not a regulatory one, but it is rather based on supporting the allied and partner countries in their national planning and identification programs. Much of this is based on the work of the Senior Civil Emergency Planning Committee (SCEPC). In addition, the NATO Parliamentary Assembly has drafted a Committee Report on the Protection of Critical Infrastructures in 2007, but the document refrains from suggesting a common definition.

The EU defines critical infrastructure as "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" (Commission Directive 2008/114/EC).

According to the Organization for Security and Cooperation in Europe (OSCE), Non-Nuclear Critical Energy Infrastructure includes "the exploration, production, storage, refining, processing and distribution of fossil fuels and supporting infrastructure systems such as electricity, as well as the extraction and processing of new energy sources" (OSCE 2013).

Finally, it is also interesting to mention that the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013), drafted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), defines Critical Infrastructure as "Physical or virtual systems and assets under the jurisdiction of a State that are so vital that their incapacitation or destruction may debilitate a State's security, economy, public health or safety, or the environment".

These definitions show that the criticality of the physical infrastructure is instrumental, as the definitions mainly focus on the harm caused by the inoperativeness of these systems. In this study, Critical Energy Infrastructure means any function of the energy infrastructure or a part thereof, which is critical in a way that its incapacity would seriously harm vital societal functions.

CEIP STANDARDIZATION EFFORTS IN NATO AND EU

Energy infrastructure is primarily a responsibility of national governments. However, it is worth discussing what a supranational (EU) or international (NATO) approach can bring to the sphere of CEIP. Indeed, CEIP has been very much debated not only at the national level but also at the international one. The reason for this is the fact that energy infrastructure has various cross-border dimensions from acquiring the raw material to distributing the generated electricity through the high voltage lines. Due to the systemic nature of energy and electricity business, the network effects and the efficiency benefits gained through cross-border harmonization would be significant not only from an economic perspective but also from a security point of view. In this context, the approaches taken by the EU and NATO are quite relevant. The EU introduced CEIP in its legislation in 2008 with the Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection. The energy sector is one of the two infrastructure sectors considered in the implementation of the Directive so far, the other being the transportation sector. CEIP was inserted in the NATO agenda of the Bucharest Summit in 2008 as part of the broader topic of energy security. Later, at the Wales Summit of 2014, NATO welcomed the *"efforts both by NATO Allies and EU members to enhance their defense capabilities"* and supported the *"continuing close cooperation and complementarity between the two organizations."* (NATO, 2014) This is a sound recommendation, and wherever synergies between the organizations

can be found, duplication of efforts should be avoided as far as possible.

As the standardization efforts at the NATO and EU level have been progressing slowly, NATO and EU member states have developed their own definitions and approaches regarding CEIP. Critical infrastructure can be seen as the blood veins of the nation, and thus they are under national sovereignty. This means that it would be worth finding a common way to cooperate to increase the resilience of CEIP that would be acceptable for all. This is why both the EU and NATO initiatives in the field aim at sharing best practices and lessons learned. However, in the case of the EU, member states mostly regarded the practical effects of the aforementioned EU initiative on security as ineffective. In the Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection it is stated that "Implementation of the Directive has not resulted in sufficiently clear and tangible improvements to ECI security levels" (European Commission, 2012).

THE FINNISH EXAMPLE: CEIP AS PART OF THE COMPREHENSIVE SECURITY

Finland is a EU member state and an active NATO partner, being part of the Enhanced Opportunities Partner programme since 2014. In the NATO framework more specifically, Finland has been active in the context of the civil emergency planning, including security of supply related issues. The approach that Finland has promoted in this field, and towards critical infrastructure protection in general, is based on the concept of comprehensive security as contained in the Security Strategy for Society, which was enacted as a government resolution in 2010 and is to be updated in 2017. This document emphasizes the cooperation among the authorities at all levels and within the civil society, including the business community. The implementation of the governmental strategy is monitored by the Security Committee – a permanent and broad-based body in charge of assisting the government and the ministries in the field of comprehensive security.

According to the Security Strategy for Society, the comprehensive concept of security comprises the preparedness for dealing with security issues, which may turn into threats that can jeopardize or seriously harm Finland, its citizens or the functions vital to the society. This approach takes into account the potential of the whole society by offering the possibility to use the resources of the different sectors of the society to ensure its security. The idea is to coordinate the activities of the public and private sectors as well as the voluntary activities of the citizens in order to ensure that the society is functional under all circumstances. The main focus of this approach are the seven vital functions of the society outlined in the Security Strategy for Society, which must be secured in all situations. These are specified and divided into strategic tasks assigned to the respective ministries.[2]

Graph 1: Vital functions of the society as specified in the Security Strategy for the Society 2010

[2] The seven vital functions are the following: 1) Management of Government affairs, 2) International activity, 3) Finland's defense capability, 4) Internal security, 5) Functioning of the economy and infrastructure, 6) The population's income security and capability to function, and 7) Psychological resilience to crisis. (Ministry of Defense of Finland, 2010)

[3] From a slideshow presentation, available from http://www.turvallisuuskomitea.fi/index.php/files/26/Downloadable%20Materials/39/Security%20Strategy%20for%20Society%202010%20english.ppt

It is interesting to note that although the "functioning of the economy and infrastructure" does not directly translate into CEIP, the energy aspect is strongly emphasized in the document:

"Energy availability is safeguarded with domestic solutions and international cooperation. Availability and use of domestic, renewable, agriculture-based energy as well as bio fuels will be increased. The share of energy from renewable sources will have to be raised to 38% by 2020; in practice this means to a large extent that the use of bio fuels will be increased. The production of electricity and heating, the capacity of the electric grid, resilience of functions as well as the functioning of technical systems are safeguarded. Electric power supply relies on a functioning electricity market, an adequate electric grid, dispersed production facilities and multiple sources of energy as well as the proper balance between peak demand and capacity" (Ministry of Defense of Finland, 2010).

Even though energy infrastructure is not specifically mentioned as one of these seven vital functions, it is possible to state that it is given much relevance in the document. In fact, according to the Security Strategy for Society, in order to face the threat scenario defined as *"Serious disturbances in the power supply"*, *"undisturbed production and distribution of power is the precondition for the functioning of society and, in fact, for all vital functions"* (Ministry of Defense of Finland, 2010). The document also stresses that *"extensive and long-term failures in production and distribution of power can seriously undermine society's capability to function"* (Ministry of Defense of Finland, 2010). Thus, the strategy makes it clear that disturbances in the power supply can possibly endanger the whole society and that these risks must therefore be addressed effectively.

Additionally, the Security Strategy for Society states that Critical Infrastructure (CI) includes *"the structures and functions which are critical for the continuous functioning of society"* (Ministry of Defense of Finland, 2010). According to the Strategy, these involve both the physical facilities and structures and the electronic functions and services necessary to ensure the security of energy supply. The document also highlights the relevance of specific critical points or nodes in the infrastructure networks, which must be "found and secured while at the same time paying close attention to the functioning of the infrastructural entity" (Ministry of Defense of Finland, 2010). Thus, although lacking the precise definition of CEIP, the Finnish Security Strategy for Society provides sufficient strategic framework for addressing the issues connected to it.

THE PUBLIC AUTHORITIES IN THE FIELD OF CEIP

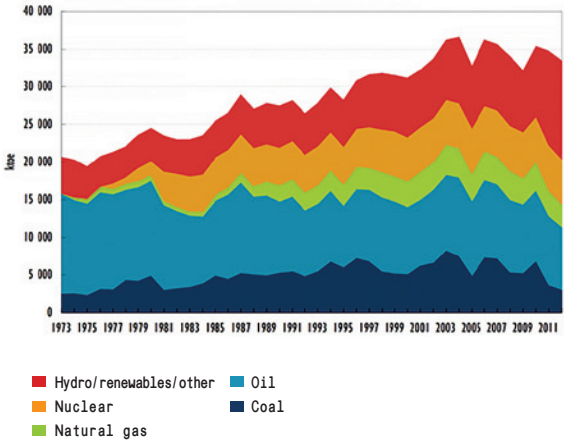
Although the Security Strategy for Society is the main strategic document concerning comprehensive security, it does not contain an exact definition of CEIP, as stated above. Therefore, it is necessary to take some other actors into consideration in order to get the full grasp of the institutional framework concerning CEIP.

One of the main elements of national preparedness traditionally is the national emergency resource reserves, which in Finland are managed by the National Emergency Supply Agency (NESA), whose history can be traced back to the 1920s. Nowadays, NESA is in charge of various CEIP related tasks. For example, according to the Act on Electricity Markets (588/2013), the network operators are responsible of issuing a preparedness plan, which has to be accepted by NESA. As this example shows, the tasks assigned to the agency go well beyond the traditional task of managing emergency storages.

In this context, it is interesting to note that the 2013 Government Decision on Security of Supply (857/2013) states that the main objective of the state in regards to Security of Supply is to ensure the continuity of production and infrastructure vital to the society

under all circumstances in such a way that the living conditions of the population and the critical functions of the society are secured also in the event of disruptions and crises, including a state of emergency. The objectives of the state are divided into two categories: securing critical infrastructure and securing critical production and services.

According to a study conducted by the University of Cologne titled "An Embargo of Russian Gas and Security of Supply in Europe" (Hecking, H. et al 2014), Finland would be the most vulnerable European country if gas imports from Russia were cut off. Although it provides food for thought, this study overestimates the dependency on short term gas imports as the portion of natural gas in the Finnish energy production has been quite small over the last few years, as shown in the graph below (Graph 2). Furthermore, natural gas is mostly used for central heating and for industrial purposes, not for residential use, as it is the case in many countries. The amount of the natural gas used for these purposes can be replaced by other energy sources, if necessary. This also demonstrates the current importance of traditional storage. According to the Government Decision, the objective is to have five months reserves available at any given time. Therefore, it is possible to state that the risk is not as high as the study implies.



Graph 2: Total primary energy source trend, 1973-2012 (IEA 2014)

Besides NESA, another important actor in the field of CEIP is Fingrid – the national transmission grid operator, of which the state owns a significant portion. Fingrid is mainly responsible for the functioning of the national electricity transmission grid, which is a high-voltage network covering entire Finland. The risks are managed on the base of the N-1 criterion, according to which the power system withstands the normal individual faults and the disconnection of a faulty component in the network without an interruption in electricity production or consumption and without secondary failures (Fingrid, 2017). The cooperation between the public authorities is frequent, and constantly upheld through regular and nation-wide preparedness exercises.

THE STRENGTHS OF THE COMPREHENSIVE CONCEPT OF SECURITY

The implementation of the comprehensive security approach involves the coordination of the measures of the government, the state authorities, the municipalities, the private sector and non-governmental organizations (NGOs) to maintain the functions vital to the society under all situations. The aforementioned Security Committee is in charge of coordinating the strategic level of security policy implementation, based on close cooperation among the public authorities. In the Committee, all the Chiefs of Staff from each ministry and the chiefs of public security bodies such as the police and the border guard meet regularly. Additionally, comprehensive security is not limited to cooperation between the public officials only, but it also concerns the cooperation between the public and the private sector. The Public-Private Partnerships (PPPs), which are nowadays the spearhead of critical infrastructure protection actions internationally, have a long tradition in the Finnish security policy. They imply the cooperation among the municipalities, companies and NGOs as well as active contingency planning and preparedness. Another good example of PPPs are the National Defense Courses, which train and prepare both civilians and military personnel work-

ing in the key positions of the society. The aim is to make them able to act in emergency situations under the rules and principles of the comprehensive security approach. Functioning PPPs are achieved through wide and well-structured cooperation not just legally, but most importantly by building a culture of trust between the various actors involved.

As for the critical energy infrastructure protection more specifically, it is important to define what is actually being protected. The criticality of the infrastructure comes from the societal functions, which the PPPs enable, and this is where the Finnish example of vital functions to the society can be used to build a coherent framework of critical energy infrastructure protection, while promoting PPPs and a whole-of-society approach.

CONCLUSIONS

Critical energy infrastructure protection boils down to a basic problem: not everything can be protected, although in some regards the hardening of the systems can bring good results (like in cyber security) while in some other cases it is necessary to concentrate on resilience and on the capability to recover. This is done through a combination of technical and administrative/regulatory aspects. On the more technical side, it is necessary to develop new energy storage and smart grid applications while encouraging controlled and sustainable shift into renewables and distributed generation. In addition to this, a functioning legal framework for these issues should be created taking into account the questions regarding preparedness and operator responsibilities. In addition, security of supply must be understood in a modern sense. It can no longer mean just having stocks of strategic resources, as it's equally important to also have technical capabilities and know-how available during possible crises.

Comprehensive security strategy is one of the possible approaches to achieve these goals. Finland, which is a country with a long tradition in adopting measures aiming at protecting critical functions and infrastructure, can be used as a good example at least in some regards. Of course, as countries differ in many respects, good results cannot be directly transferred from a country to another. Therefore, it is necessary to take into account the specificities of each country when applying the measures that have been successful in other countries. Finland is a relatively small country, with a long tradition of cooperation (not of competition) among its authorities. Nevertheless, cooperation between the different agencies and bodies should be something to strive for regardless of the country, as should the wide participation of civil society and the private sector. In this context, much still needs to be done in order to make societies ready to deal with the risks connected to the protection of critical energy infrastructure.

As a general rule, consultations between the public and the private sector are of a growing importance today as most of the critical infrastructure is increasingly privately owned and operated. Also, owners often have very little or no connection at all with the actual country where the physical operations are run. Overregulation must be avoided, but state interference is needed when markets and self-regulation do not provide the owners with incentives that are strong enough to prepare for eventual problems.

As for the inter-organizational cooperation, it is important to define roles and responsibilities as well as to find effective ways for collaborating and sharing information. The EU provides its member states for a political framework for discussion, for the establishment of a decision-making platform as well as for the possibility of adopting a cross-sectoral approach especially in the context of new regulations and policies. Additionally, NATO is complementary to the EU as it uses its resources for civil protection and for dealing with the military aspects of CEIP.

BIBLIOGRAPHY

European Commission. (2012). Commission staff working document on the Review of the European Programme for Critical Infrastructure Protection SWD(2012) 190 Final. Brussels

Fingrid. (2017). Maintaining of security system. Retrieved from http://www.fingrid.fi/en/powersystem/Power%20system%20management/Maintaining%20of%20system%20security/Pages/default.aspx

Hecking, H. et al. (2014). An Embargo of Russian Gas and Security of Supply in Europe. Retrieved from: http://www.ewi.uni-koeln.de/fileadmin/user_upload/Publikationen/Studien/Politik_und_ Gesellschaft/2014/2014-09__An_Embargo_of_Russian_Gas_and_Security_of_Supply_in_Europe_0610.pdf

International Energy Agency. (2014). Energy Supply Security 2014, Chapter 4: Emergency response systems of individual IEA countries. Retrieved from: https://www.iea.org/media/freepublications/security/EnergySupplySecurity2014_finland.pdf

Jakson, H. et al. (2017). Hybrid Warfare against Critical Energy Infrastructures Study. Retrieved from: https://enseccoe.org/data/public/uploads/2017/05/irregular_warfare_176x250mm_20170411.pdf

Luhn, A. (2015). Ukraine miners rescued after shelling left them trapped. The Guardian, 26 January. Retrieved from: http://www.theguardian.com/world/2015/jan/26/ukraine-miners-trapped-freed-shelling-donetsk

Ministry of Defense of Finland. (2010). Security Strategy for Society. Retrieved from http://www.defmin.fi/en/publications/strategy_documents/the_security_strategy_for_society

NATO CCDCOE. (2013). The Tallinn Manual on the International Law Applicable to Cyber Warfare. Retrieved from: https://ccdcoe.org/tallinn-manual.html

NATO. (2014). The Wales Declaration on the Transatlantic Bond. Retrieved from: http://www.nato.int/cps/on/natohq/official_texts_112985.htm

Organization for Security and Co-operation in Europe. (2013). Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Retrieved from: http://www.osce.org/atu/103500

The Role, Risks and the Strategic Importance of Energy in Conflicts. The case of Ukraine

Emanuele Nicola Cecchetti, SHAPE, Belgium
Heiki Jakson, Estonian Electrical Distribution System Operator, Estonia

The aim of the article is to discuss the key role that energy plays in conflicts by focusing on the war between Ukraine and Russia in 2014. After discussing the evolving role of energy in conflicts throughout history, this study analyses the main events of the conflict between Russia and Ukraine showing that destroying critical energy infrastructure (CEI) was a major military target for Russia. In this context, the strategies adopted by NATO in order to protect the national security of its members and the support it receives from its Centres of Excellence and in particular by NATO Energy Security Centre of Excellence are also discussed.

INTRODUCTION

The Ukrainian crisis in 2014 has clearly shown that war can be effectively fought with both conventional and unconventional means. Conventional warfare is "a form of warfare between states that employs direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory in order to force a change in an adversary's government or policies. The focus of conventional military operations is normally an adversary's armed forces with the objective of influencing the adversary's government" (US Department of Defense, 2007). Unconventional warfare "means activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary, or guerrilla force in a denied area" (US Government, 2015). This article mainly focuses on conventional warfare.

Emanuele Nicola Cecchetti, NATO Supreme Headquarter Allied Powers Europe, Mons

Emanuele Nicola Cecchetti is currently undertaking an internship as a Junior Analyst at the NATO Supreme Headquarter Allied Powers Europe (SHAPE) in Mons (Belgium). He holds an MA degree in Interdisciplinary Research and Studies in Eastern Europe (MIREES) from the University of Bologna, and he has other two internship experiences as an analyst/researcher in the NATO Energy Security Centre of Excellence in Vilnius and in the Istituto Affari Internazionali (IAI) in Rome respectively. Emanuele Nicola Cecchetti is a co-author of the 'Energy in Conventional Warfare' and 'Energy in Irregular Warfare' volumes published by the NATO Energy Security Centre of Excellence within the "Energy in Conflict" series.

The Ukrainian crisis has also shown that energy is an important dimension of warfare nowadays as it has become one of the major military targets. This is evident in the way Russia has conducted the war against Ukraine to annex Crimea. The destruction of critical energy infrastructure (CEI) was indeed one of the strategies used by Russia in the conflict with Ukraine. CEI is "the energy infrastructure that is so essential that its failure or destruction would have far reaching negative effects on economic and social security as well as on the defensive capabilities of the state". This definition of CEI refers to: (1) energy extraction facilities (oil and natural gas wells, mines); (2) energy transportation infrastructure (pipelines, train and road carriers, oil tankers, electric power lines); (3) energy conversion infrastructure (refineries, power plants) (NATO ENSEC COE, 2016).

This article analyses the role of energy in the conflict between Russia and Ukraine in 2014 by focusing on conventional warfare against CEI. It is divided into four sections. The first one briefly discusses the importance of energy in conflicts throughout history in order to show that energy has played a key role in all times but also that technological development has changed the military targets in the energy sector passing from food to CEI. The second section briefly discusses the main events of the conflict between Russia and Ukraine by explaining why Ukraine is important for Russia in its 'near abroad'. The third section focuses on the destruction of CEI in Ukraine showing the relevance that it has in conflicts nowadays both because it ensures energy supply and because it is a military target. Finally, the fourth section analyses NATO's strategies to react to the Ukrainian crisis in order to protect its member states of the eastern flank.

THE IMPORTANCE OF ENERGY IN CONFLICTS THROUGHOUT HISTORY

Energy has played a key role in man's life since the ancient times when it was essentially represented by food. Over time, technological development has allowed man to tap new forms of energy. Man passed from exploiting large, strong animals providing an excellent source of energy for a limited set of applications to extracting coal, which was necessary for industry and for the development of towns during the 18th and the 19th centuries. During the following two hundred years, man learned to extract and produce more sophisticated forms of energy such as natural gas, oil, nuclear power and sustainable energy resources like the wind and the sun (Khan Academy, 2015). The ability of man to exploit these energy resources due to technological development has changed the way wars are currently conducted not only because new kinds of weapons have been created, but also because the strategies that it is possible to adopt to defeat the enemy have become very sophisticated. Additionally, the energy targets have also changed over time. In the ancient times, for instance, commercial ships were sometimes a military target. The case of the Athenian ships ensuring the passage of grain carriers that were captured by the Spartans in the Battle of Aegosopotami at the end of the Peloponnesian War in 405 BC is a good example.[4] In the 20th century,

Heiki Jakson, Estonian Electrical Distribution System Operator, Tallinn

Heiki Jakson is currently working as electrical engineer for Elektrilevi (Estonian Electrical Distribution System Operator - DSO). Previously, he was a Subject Matter Expert at NATO ENSEC COE working on Critical Energy Infrastructure Protection topics. He has also worked as an electrical engineer in the electrical infrastructure construction sector and has a MSc degree in power engineering from the Tallinn University of Technology. Additionally, he has also been an infantry officer in the Estonian Defence League (which is a voluntary military national defence organisation) since 2003.

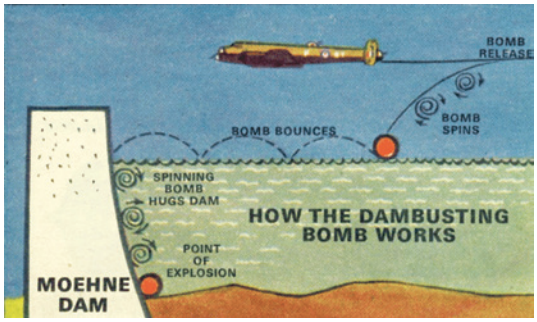


Figure 1 Operation Chastise 1943 (www.iwm.org.uk)

oil, gas and electricity products together with critical infrastructure necessary to transport and distribute them became one of the military targets. In fact, they are essential not only for the well-being of societies but also for military operations. During the First World War, for instance, Britain used oil-fired combustion engines for warships making them lighter, more powerful and able to transport a huge number of weapons. Consequently, Britain became very much dependent on external sources for iron ore and oil coming through the Atlantic. Therefore, German U-Boats began attacking British ships causing an oil shortage that was fatal for the British fleet. The UK was forced to recognise the fragility and the importance of oil supplies and look for alternative sources. During the Second World War, the importance of CEI increased, both from a defensive and an offensive point of view. A good example is Nazi Germany's seizure of the most important electricity systems, dams, oil fields, and refineries especially in Romania[5]. It secured CEI with air defense systems, thus ensuring a constant flow and supply of energy for its military actions. Some years later, CEI became the main targets of the Allies. More than six hundred attacks occurred from 1940 to 1945 against CEI. Among them, the most successful one was the Operation Chastise in May 1943 (Mason, 2017). The peculiarity of this attack was the weapon that was used, namely the "bouncing bomb"[6], which breached the German Möhne and Edersee Dams leading to a catastrophic flood of the Ruhr and the Eder valleys, and causing the destruction of roads, bridges and railways (School of Chemistry, 2001).

Over time, war tactics have continued developing, so that both conventional and unconventional war strategies were planned, leading energy infrastructure to become a major military target. For instance, during the Cold War the Soviet Union planned to attack oil and gas pipelines crossing Canada and Mexico, the North American dams, or the electricity system of New York City (Christopher, 1999). Of course, none of these plans was implemented. At the same time, the US planned attacks against the Urengoy–Surgut–Chelyabinsk gas pipeline as countermeasure and retaliation, by inserting a malicious code into the control system of the pipeline (Robertson, 2014). This sabotage allegedly resulted in the explosion of a portion of the pipeline (Rid, 2013).

Nowadays, serious threats to CEI come not only from physical destruction, but also from cyber-attacks because many parts of energy infrastructure are automatized. In this context, two examples of cyber-attacks well il-

Figure 2 Baku – Tbilisi – Cehyan pipeline explosion 2008 (http://www.enerji.gov.tr)

[4] The Athenian fleet was sent off to the Black Sea in order to protect the passage of grain carriers through the Dardanelles. The Spartans positioned their fleet of 170 Peloponnesian ships at Lampsacus at the southern shore of the Dardanelles. When the Athenians arrived, they had to anchor at Aegospotami opposite Lampsacus, which was the only safe port in the area. Some days later, Lysander's fleet made a sudden crash across the water, pounced on the anchored Athenians, captured 160 ships and killed the crew. The decisive victory over the Athenian fleet broke the Athenian naval superiority that had been unchallenged until then and ended the Peloponnesian war. (Marine Solutions, 2015)

[5] Romania (in particular the county seat Ploiesti) which was a major power in oil industry since the 19th century, was one of the biggest producers in Europe. The oil refineries of Ploiesti supplied about the 30% of oil to Nazis and to the whole Axis (ANEIR, date not available). The whole Romania was the target of a strong Allies' bombing campaign in 1943 aiming at cutting the oil supply to the Nazi regime. (Dugan, Stewart, 1998)

lustrate the case. The first example concerns the STUXNET operation against the Iranian nuclear power plants in 2010, which caused serious malfunctioning of the systems for several days (Melman, 2010). The second example concerns the Baku-Tbilisi-Cehyan pipeline in 2008, whose functioning was interrupted by an "anonymous" hacking of power plant system and by a suspicious hand-driven malfunctioning of the security system leading to the explosion of part of the system in Refahiye in the Eastern part of Turkey (Robertson, Riley, 2014).

A BRIEF OVERVIEW OF THE UKRAINIAN CONFLICT

Ukraine is part of Russia's 'near abroad', which is a term originally used to refer to the newly independent republics surrounding Russia after the dissolution of the Soviet Union. Ukraine has very strong historical, geopolitical, economic and geostrategic ties with Russia. As Polish-American and political scientist Zbigniew Brzezinski stated, Russia would never be a European empire without Ukraine, which is Russia's historical aspiration. Indeed, by losing its political influence on Ukraine, Russia would no longer control the trade route of its products and hydrocarbons to the EU that is Russia's largest economic partner. Additionally, Ukraine is important for Russia's national security for its peculiar geographical position as its southern border adjoins the Black Sea. This latter plays a key role in Russia's exports to Europe as well as in terms of defense as Russia has three naval bases on the coasts of the Black Sea, namely in Novorossiysk and two in Ukraine, in Sebastopol and in Odessa. Additionally, the Black Sea plays an important role for Russia in its relations with Turkey, its historical rival, as well as in its influence in the Middle East, Central Asia and the Caucasus. For these reasons, from Russia's perspective, Ukraine's approach to the EU represents a challenge to its national security. This means that Russia is willing to go as far as it is necessary to defend its national interests (Milosevich, 2014). It is in this perspective that Russia invaded Ukraine.

The crisis between Russia and Ukraine dates back to 2013 when mass protests against then-president Viktor Yanukovych and against his decision to abandon the Association Agreement with the European Union (EU) that would make the political and trade relations with Ukraine closer began (Curtin, Rahman, 2014).

Strong clashes occurred in many cities among which the harshest ones were in Kyiv, leading then president Viktor Yanukovych to

Figure 3 Urengoi-Pomary-Uzhgorod gas pipeline explosion, in May 2014

[6] The 'bouncing bomb' was a drum-shape that spun backwards at over 500 rpm and had to be dropped at a sufficiently low altitude at the correct speed. In this way, the mine skipped for a significant distance over the surface of the water in a series of bounces reaching the dam wall. Using a hydrostatic fuse, an accurate drop could bypass the dam's defenses and enable the bomb to explode against the dam. (Mason, 2017)

[7] An association agreement is a bilateral agreement between the EU and a third country. In the context of accession to the EU, it serves as the basis for implementation of the accession process. (European Commission, 2016)

[8] In 2014, then French President François Holland and German Chancellor Angela Merkel brokered a 'Package of Measures for the Implementation of the Minsk Agreements', known as Minsk II. The agreements included, inter alia, the Immediate and full ceasefire in particular districts of Donetsk and Luhansk Oblasts of Ukraine and Pull-out of all heavy weapons by both sides to equal distance with the aim of creation of a security zone (The Telegraph, 2015)

resign. The crisis between Russia and Ukraine reached its peak in March 2014 when the former militarily occupied Crimea, at a first stage unofficially through unconventional means such as protests and riots (Amos, 2014), information and psychological operations (Yuhas, 2014) and unidentified fighters known as "little green men" (Shevchenko, 2014). Later, Russia officially occupied Crimea with its Armed Forces. The same month a disputed referendum took place in order to decide whether Crimea should become part of Russia or not. 95,5% of voters supported joining Russia (BBC, 2014c).

Figure 4 Gas Compressor Station N1, Lugansk-Verbovka area

Today, the situation in Ukraine is still difficult. The country is divided and corruption corrodes the economy and the society. Additionally, in Donbass and Luhansk the Ukrainian separatists continue feeding the conflict with the Russian military support. It is thus clear that the Minsk II agreements of 2015[8] are not being fully implemented. While Ukraine and the West insist on a full ceasefire before moving on with the political elements of the deal, Russia accuses Ukraine of not respecting the agreement (The Economist, 2016).

A BRIEF DESCRIPTION OF THE ENERGY INFRASTRUCTURE DESTRUCTION DURING THE CONFLICT BETWEEN UKRAINE AND RUSSIA IN 2014

The conflict between Russia and Ukraine was characterized by the destruction of energy infrastructure, which is necessary for the well-being of the society as well as for military operations. The first attack against energy infrastructure in Ukraine occurred on March 15, 2014 when the Russian Armed Forces seized a gas distribution station on the north-eastern border of the peninsula, thus ensuring the supply for the area and avoiding sufferings to the population (Baker, 2014). Two months later, on May 14, 2014 an explosion occurred near the Urengoi-Pomary-Uzhgorod gas pipeline, which is also known as Brotherhood and which is the largest consumer gas pipeline in Europe. In addition to this, in the month of June, Russia cut off all gas supplies to Ukraine. Russia's state-owned gas giant Gazprom claimed that Ukraine had to pay upfront for its gas supplies, after Kiev failed to settle its huge debt. According to Gazprom chief Alexei Miller, this put the Russian gas supplies to the EU at risk (BBC, 2014b). On July 18, eighteen cities around Donetsk and Lugansk were left without electricity for many days due to casualties in the transformer substations during the conflict between the separatists and the Ukrainian army (BBC, 2014d). During the same month, there were serious difficulties in supplying water and electricity to the Sloviansk and Starobesheve thermal power stations because of damages in the pumping-systems (KyivPost, 2014).

Furthermore, another relevant event in the conflict between Russia and Ukraine occurred in the area of Lugansk and Verbovka on July 2, 2014 when Russia-backed separatists seized the gas compressor station N1 (red-circled in Figure 4), which maintained the necessary pressure to deliver gas through

international transiting pipelines, causing tensions on possible interruption of gas flows in the network International Analysis Centre, National Security of Ukraine (2014).

Additionally, Russia-backed separatists isolated coalmines and coal storages in the eastern part of Ukraine providing coal to its Western part. Separatists did it through conventional attacks and sabotages against infrastructure like bridges, railways, and core coal transportation systems (Bird, 2015).

In conclusion, Russia and the Ukrainian separatists that it supported were able to divide Ukraine by attacking CEI with both conventional and unconventional tactics, as sabotages, riots and cyber-attacks (the latter focused on governmental websites and systems). In this way, they managed to carry on the conflict against the central government maintaining total control over the territory.

NATO'S STRATEGIES TO REACT TO THE UKRAINIAN CRISIS

The conflict between Russia and Ukraine raised the Alliance's worries for the national security of its member states of the eastern flank. Therefore, after strongly condemning Russian actions in Ukraine, NATO took steps aiming both at reassuring allies and partners in Central and Eastern Europe and at deterring further Russian aggression (Belkin, 2014). These steps include the reinforcement of its military troupes in its member states in Eastern Europe. The first nations where NATO troops were strengthened were the Baltic States (Estonia, Latvia and Lithuania), in order "to help bolster defenses of the Baltic states amid fears that Moscow may use the presence of substantial Russian minorities to destabilise Latvia, Lithuania and Estonia" (The Guardian, 2014). In this context, NATO's Enhanced Forward Presence (EFP), which was agreed at the 2016 Summit in Warsaw, is particularly important as it is part of NATO's strategy to strengthen deterrence and defense posture in its eastern flank. In fact, "it represents a significant commitment by Allies and is a tangible reminder that an attack on one is an attack on all".[10]

Additionally, at the 2014 Wales Summit, NATO began the Readiness Action Plan (RAP), which "ensures the Alliance is ready to respond swiftly and firmly to new security challenges from the east and the south" (NATO, 2017b). In so doing, NATO paved the way to the reactivation of the Missile Defense System project in Poland, Czech Republic and Romania in 2016, which produced strong reactions from Russia leading the Alliance to suspend the implementation of the project (Emmot, 2016). The Alliance aimed to increase its military presence and activities in certain countries (Poland, Czech Republic and Romania) to deter Russia from military attacks. NATO's activities included military drills in different fields (military, cyber, energy, search and rescue, etc.), changes in its long-term military posture and capabilities, as the "Spearhead Force" (Very High Readiness Joint Task Force - VHRJT) (NATO, 2017).

Furthermore, NATO can count on the expertise of its Centres of Excellence (COE) that are nationally or multi-nationally funded institutions supporting the Alliance in its work while avoiding the duplication of assets, resources and capabilities already present within the NATO Command (NATO ENSEC COE, 2016). Thus, NATO Centres of Excellence provide support for facing current threats and challenges.

In this context, NATO Energy Security COE (ENSEC COE) plays an important role in supporting the Alliance to ensure energy security in its member states. The protection of critical energy infrastructure is one of the topics on which NATO ENSEC COE works. The Centre conducts several projects on this issue among which it is worth mentioning 'Energy in Conflict'. This is a publication series aiming at analyzing the impact that conflicts have on energy infrastructure that has become one of the main military targets. The 'Energy in Conflict' publication series provides a conceptual "toolbox" on the topic for NATO

members with a twofold aim. Firstly, the Centre provides the necessary support to the Alliance in order to strengthen the protection of critical energy infrastructure in its member states. Secondly, the Centre analyses the role of energy in conflict, which is essential to decision makers and military planners.

CONCLUSION

Energy has played an evolving role in conflicts throughout time. While in the ancient times energy was represented by food, nowadays technological development has made CEI one of the major military targets. The reason is that CEI is fundamental both for the well-being of the society and for military operations. Therefore, destroying CEI means weaken the enemy. This is evident in the conflict between Russia and Ukraine in 2014 as the former destroyed CEI in the latter as a strategy of war. In fact, Russia destroyed pipelines and power plants disrupting energy supplies to the population and jeopardizing energy supply to the EU.

In this context, NATO has reacted by ensuring protection to the member states of its eastern flank. In order to do so, the Alliance has taken several measures aiming at strengthening its troupes in those states such as in the case of the Baltic States that border Russia and at deterring further Russian aggression.

Finally, it is worth mentioning the important role played by the NATO Centres of Excellence that provide support to the Alliance in its work. NATO ENSEC COE is a good example as it supports the Alliance in ensuring energy security in the member states.

BIBLIOGRAPHY

Aladashvili. I. (2014). Baku-Tbilisi-Ceyhan was blown up Not by Kurdish Bomb But by Russian Laptop. Georgian Journal, 18 December. Retrieved from https://www.georgianjournal.ge/military/29027-baku-tbilisi-ceyhan-was-blown-up-not-by-kurdish-bomb-but-by-russian-laptop.html

ANEIR - Foreign Trade Promotion Centre S.A. National Association of Romanian Exporters and Importers. (date not available). Romania-Brief Survey, History. Retrieved from http://www.aneir-cpce.ro/chapter1/his1.htm

Amos. H 2014. Ukraine crisis fuels secession calls in pro-Russian south The Guardian, 23 February. Retrieved from https://www.theguardian.com/world/2014/feb/23/ukraine-crisis-secession-russian-crimea

Baker. P., Herszenhorn, D. M., Kramer, A. E. (2014). Russia seizes gas plant near Crimea border, Ukraine says. The New York Times. 15 March. Retrieved from https://www.nytimes.com/2014/03/16/world/europe/russian-troops-seize-gas-plant-beyond-crimean-border-ukraine-says.html?mcubz=3

BBC. (2014a). Major Ukraine gas pipeline hit by blast. 17 June. Retrieved from http://www.bbc.com/news/world-europe-27891018

BBC. (2014b). Ukraine crisis: Russia halts gas supplies to Kiev. 16 June. Retrieved from http://www.bbc.com/news/world-europe-27862849

BBC. (2014c). Crimea Referendum: Voters 'Back Russia union'. Retrieved from http://www.bbc.com/news/world-europe-26606097

BBC. (2014d). Ukraine Conflict: Part of Luhansk 'retaken' from rebels. 18 July. Retrieved from http://www.bbc.com/news/world-europe-28363086

BBC. (2015). Russia examines 1991 recognition of Baltic States independence. 30 June. Retrieved from http://www.bbc.com/news/world-europe-33325842?SThisFB

Belkin, P. (2014). NATO: Response to the Crisis in Ukraine and Security Concerns in Central and Eastern Europe. Congressional Research Service

Bird, M., Tkachenko, Y., Vdovii, L . (2015). The great looting of Donbass. In "The Donbass

Paradox", TheBlackSea.eu, 10 December. EUObserver. https://euobserver.com/investigations/13142

Curtin, J., Rahman, A. (2014). The Ukrainian Crisis. A Disputes Past and Present. Policy Brief. Harvard

Emmot, R. (2016). U.S. activates Romanian missile defense site, angering Russia. Reuters. 12 May. Retrieved from http://www.reuters.com/article/us-nato-shield-idUSKCN0Y30JX

European Commission. (2016). Association Agreement. Retrieved from https://ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/association-agreement_en

Christopher, A., Mitrokhin, V. (1999). The Mitrokhin Archive: The KGB in Europe and the West. Penguin UK, London

Dugan, J., Stewart, C. (1998) Ploesti: The Great Ground-Air Battle of 1 August 1943. Brassey's Inc., USA, Washington

Gerasimov, V. (2013). The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Military-Industrial Kurier. 27 February. The English version can be retrieved from: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

International Analysis Centre, National Security of Ukraine. (2014). Consolidated news from the NSC News & Analysis Center. 2 July. http://mediarnbo.org/2014/07/04/consolidated-news-from-the-nsc-news-analysis-center-at-1200-july-2-2014/?lang=en

Khan Academy. (2015). Energy Through Time. A Natural Flow From to Big Bang to the Modern Human Society. Retrieved from https://www.khanacademy.org/partner-content/big-history-project/acceleration/other-materials9/a/energy-through-time

KyivPost. (2014). Donbasenergo's Sloviansk thermal power plant reports critical power outage. 3 July. Retrieved from https://www.kyivpost.com/article/content/war-against-ukraine/donbasenergos-sloviansk-thermal-power-plant-reports-critical-power-outage-354571.html

Marine Solutions. (2015). A Remarkable Naval Battle at the Dardanelles: Battle of Aegospotami in 405 BC. Retrieved from http://marinesol.org/a-remarkable-naval-battle-at-the-dardanelles-battle-of-aegospotami-in-405-bc/

Mason, A. (2017). The Incredible Story of The Dambusters Raid, Imperial War Museum United Kingdom. Retrieved from: http://www.iwm.org.uk/history/the-incredible-story-of-the-dambusters-raid

Melman. Y. (2010) Computer virus in Iran actually targeted larger nuclear facility. Haaretz, 28 September. Retrieved from http://www.haaretz.com/computer-virus-in-iran-actually-targeted-larger-nuclear-facility-1.316052

Milosevich, M. (2014). Ukraine, Between Russia and the European Union. Faes papers. N. 173. Madrid

NATO. (2016). Enhanced Forward Presence. Retrieved from: http://www.nato.int/cps/en/natohq/news_127834.htm

NATO. (2014). Readiness Action Plan. Retrieved from: http://www.hq.nato.int/cps/en/natohq/topics_119353.htm

NATO. (2016). Very High Readiness Joint Task Force. Retrieved from:http://www.hq.nato.int/cps/en/natohq/topics_49755.htm?selectedLocale=en

NATO. (2017). NATO Response Force. Retrieved from http://www.nato.int/cps/en/natolive/topics_49755.htm

NATO. (2017a). Boosting NATO's presence in the east and southeast. Retrieved from http://www.nato.int/cps/en/natohq/topics_136388.htm?selectedLocale=en

NATO. (2017b). Readiness Action Plan. Retrieved from http://www.nato.int/cps/en/natohq/topics_119353.htm

NATO ENSEC COE. (2016). Centre of Excellence. Retrieved from https://www.enseccoe.org/en/about/6

NATO ENSEC COE. (2016). Energy in Conventional Warfare. Vilnius

Rid, T. (2013). Cyber War will not take place. Oxford University Press. Oxford

Robertson, J., Riley, M. A. (2014). Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar, Bloomberg. 10 December. Retrieved from https://www.bloomberg.com/amp/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

Russia Today. (2014). Urengoi-Pomary-Uzhgorod gas pipeline explosion. Retrieved from https://www.rt.com/news/166532-gas-pipeline-blast-ukraine/

School of Chemistry (2001). The Bouncing Bomb. University of Bristol. Retrieved from: http://www.chm.bris.ac.uk/webprojects2001/moorcraft/The%20Bouncing%20Bomb.htm

Shevchenko, V. (2014) "Little Green Men" or "Russian Invaders"?, BBC. 11 March. Retrieved from http://www.bbc.com/news/world-europe-26532154

Short, B., De Jong, M., Larry, H. (2016). Energy in Conventional Warfare. Energy in Conflict Series. NATO Energy Centre of Excellence. Vilnius

The Economist. (2016). What are the Minsk Agreements?. Retrieved from https://www.economist.com/blogs/economist-explains/2016/09/economist-explains-7

The Guardian. (2014). NATO to bolster of Baltic states amid Ukraine crisis. Retrieved from https://www.theguardian.com/world/2014/mar/24/cameron-nato-baltics-states-defences-ukraine-crisis

The Telegraph. (2015). Minsk agreement on Ukrainian crisis: text in full. Retrieved from http://www.telegraph.co.uk/news/worldnews/europe/ukraine/11408266/Minsk-agreement-on-Ukraine-crisis-text-in-full.html

US Department of Defence. (2007). Irregular Warfare Joint Operating Concept (IW JOC) Version 1.0. Washington

US Government. (2015). Legislative Text and Joint Explanatory Statement to accompany S. 1356 Public Law 114-92. Washington

Yuhas, A. (2014), 'Russian propaganda over Crimea and the Ukraine: how does it work?', The Guardian, 17 March. Retrieved from https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media

The energy dimension of war. The Ukrainian experience An overview of the Ukrainian events in 2014-2016

Oleksandr Sukhodolia, National Institute for Strategic Studies, Ukraine

This article discusses the events related to the Russian attacks on critical energy infrastructure (CEI) in Ukraine between 2014 and 2016. The aim is to better understand the threats to CEI in hybrid warfare by discussing the example of the Ukrainian events in 2014-2016. This allows the author to provide some inputs for developing the necessary measures to ensure CEI resilience. Incorporation of the "energy dimension" into its hybrid warfare concept gave Russia additional tools to influence Ukraine. Political and economic pressure was actively used by Russia up to 2014 and was supplemented by targeted physical actions against CEI later on. Destruction, seizing and looting of CEI, cyber attacks as well as political, economic and psychological pressure have therefore become the main set of tools of the aggressor's strategy against its neighbor demonstrating that CEI damaging is an effective non-military tool of warfare. The analysis of the events in Ukraine shows that CEI protection is a key issue that should be included into national defense policy. This implies that governments and CEI operators need to implement their emergency preparedness planning while establishing close Public - Private Partnership (PPP) and strengthening civil-military cooperation at the same time in order to provide CEI resilience.

Oleksandr Sukhodolia, National technical University, Kiev

Oleksandr Sukhodolia graduated from the Department of Electrical Power Engineering and Automatics of the National Technical University of Ukraine in 1994. He received his PhD in Electrical Engineering in 1999 and his PhD in Public Administration in 2007. He has extensive experience in energy security in the public service. Between 1998 and 2003, he served as Head of Department and Deputy Head of State Committee of Ukraine on Energy Conservation. Between 2007 and 2011, he was Deputy Head of Energy Security Department at the Secretariat of the National Security and Defense Council of Ukraine. Since 2012, he has worked at the National Institute for Strategic Studies of Ukraine as Head of Energy Security and Techogenic Safety Department. His research interests focus on national energy security, and on critical energy infrastructure protection.

INTRODUCTION

Ensuring the uninterrupted functioning of energy infrastructure is not a new challenge for Ukraine. Russia has halted the normal functioning of critical energy infrastructure (CEI) several times since the last century. However, the Russian aggression in 2014 has had a huge impact on the way wars are conducted as they have led to rethink the "energy dimension" of war.

Russia used various tools to attack Ukraine in 2014-2016. It applied sabotage against energy infrastructure as well as psychological, informational and other unconventional tools to disrupt the smooth functionality of the energy sector. This caught Ukraine unprepared for proper resistance showing that energy should be included into national security threats analyses.

Given this background, this paper discusses the events related to the attacks on energy infrastructure in some parts of Ukraine between 2014 and 2016 by defining the non-military tools of warfare that could be perceived as part of the 'hybrid war' and by proposing the measures that could ensure the functioning of the energy sector in the regions involved in the conflict.

The 'energy dimension' of warfare stems from Russia's policy of using the 'energy weapon' in its foreign policy in order to pursue its national interests. Energy, especially the natural gas sector, was used by Russia as a tool to achieve its objectives in its relations with Ukraine as well as with the European Union already in the period before the crisis in Ukraine. According to several reports, until 2006 Russia cut off energy exports about 40 times. (Reuters, 2008; Larsson, 2006)

Although this aspect was repeatedly stressed by many experts in the field, a large part of the Western political elite and of the industry experts prefer to have good relations with Russia as an important energy supplier, trying to interpret the situation exclusively in economic terms without taking into consideration the political aspect of the crisis. By contrast, in its relations with its neighbors Russia has never focused on economic rationality but on politics. Russia has often used the threat of energy supply disruption as an external policy tool instead of basing its policies towards its neighbors on economic considerations.

In the case of Ukraine, the history of its relations with Russia in the energy sector reflects the never-ending Ukrainian struggle for energy independence from Russia. In order to keep Ukraine in its sphere of influence, Russia has been practicing a wide range of tools in the energy sector. Some examples are the following: the monopolization of the energy market (Russia tried to prevent suppliers of gas to Ukraine from entering the market; in fact, Russia denied them the access to the pipelines passing through Russia from the East and through Slovakia, Poland and Hungary from the West); the corruption of government officials and company managers (the involvement of intermediaries in the gas trade between Russia and Ukraine created a wide range of supporters for non-transparent gas market readily lobbing in favour of Russian interests); the prevention of the reform of Ukraine's energy market through the inclusion of long-term prices in the contracts, the "take-or-pay" contract and re-export prohibition clauses; and offering discounts in exchange of political concessions.

The clearest example of the policy that Russia pursues in order to keep Ukraine in its sphere of influence is the progressively tightening control of the Ukrainian gas market between 1998 and 2005 that led to the signing of unfavorable contracts for natural gas supplies in 2009. This was followed by an exchange of gas price discounts with the extension of the long-term lease of the naval base in the Ukrainian Black Sea port in 2010. Another consequence of the Russian policy towards Ukraine was the Ukrainian rejection of the Association Agreement with the EU while securing additional loans from Russia for the purchase of gas in 2013.

OVERVIEW OF THE EVENTS RELATED TO CRITICAL ENERGY INFRASTRUCTURE

The Russian use of energy as a foreign policy weapon in the pre-crisis period (until 2014) contributed to including the energy dimension in the current concept of warfare. In fact, the sequence of energy related events between 2014 and 2016 represents the further set of policy intensification in order to setback Ukraine's move towards democracy and transparency. In other words, by using Clausewitz's famous expression according to which war is a mere continuation of politics "with other means" it is possible to argue that Russia "continued its politics with other means" as it transformed its political actions into a hybrid war. A clear idea of this is given by the detailed overview of the following cases in which critical energy infrastructure (CEI) was damaged (see Table 1).

Malicious actions against CEI

Malicious actions against CEI were initiated in February-March 2014 in Crimea. As a result of the temporary occupation of Crimea, Ukraine lost the control over a considerable part of its public and private assets in the energy sector (Horbulin, 2015).

In April-May, the physical damage of energy infrastructure started after the occupation of the administration buildings in the regions of Donetsk and Luhansk.

Physical damage

On June 7, 2014 the transformer substation providing energy to the Luhansk airport was blown out. At that time, the Luhansk airport was a base for the Ukrainian armed forces. On June 8, a transformer substation in Mariupol was blown down, causing the suspension of power supply to a TV station and its tower. Consequently, the TV signals were interrupted.

In the same month, 11 power lines and 88 transformer substations were damaged in the territory of the Slavyansk district, disrupting power supply. On July 3, 2014 the Slavyansk Thermal Power Plant (TPP) experienced shelling and two transformers and fuel tanks were damaged. This caused a shutdown of the last two working transmission lines. Finally, after heavy shelling the work of the TPP was stopped until the end of the year.

Between 2014 and 2015, in the Luhansk area the damages to transformer substations and power lines separated some areas from the central system, leaving consumers dependent on a single source of electricity. The situation could have easily become critical in case of damaging of this source. Since the summer of 2014, the Luhansk Thermal Power Plant (TPP) came under fire regularly. Shelling repeatedly caused a complete shutdown of the stations with the loss of generating capacity and consequent disruption of electricity supply to the north part of the region, which remained under the control of the Ukrainian forces.

In July and August 2015 the shelling of the Uglegorsk TPP damaged critical elements of the transformer station. That power station, which was the biggest one in the region, stopped generating power, thereby creating a critical situation in the entire electricity system in Ukraine. This created a deficit of pow-

[11] The concept of "hybrid war" that we apply in this paper reflects the definition given by Frank G. Hoffman, namely the "simultaneous and adaptive employment of a fused mix of conventional weapons, irregular tactics, terrorism and criminal behavior in the battle space to obtain political objectives". (Hoffman, 2009)

[12] Some examples of how Russia used a threat or direct acts of an energy supply disruption as an external policy tool are the following: stoppage of gas supply to Ukraine in 2005 and 2009 (to press Ukraine to switch to unfavorable contract conditions); stoppage of oil supply from Russia to Mazeikiai refinery (try to force Lithuania to sell refinery to Russian company); explosions of electricity and gas supply lines to Georgia in winter of 2006 (political and economic pressure on Georgia); cutting the oil supply for Czech Republic in 2008 (demonstration of power of Russia after Czech agreed on antimissile radar placement); explosion of the main transit gas pipeline from Turkmenistan in 2009 (blocking direct supply of Turkmen gas to EU) and other cases (gas disputes: Russia-Ukraine in 1998, 2013-2015; Russia-Belarus in 2004 and 2007; Russia-Poland in 2010; Russia-Bulgaria in 1998 and 2010; Russia-Turkmenistan in 1997, 2005 and oil disputes: Russia-Belarus in 2007 and 2010; Russia-Lithuania and Russia-Latvia in 1998, 2002, 2006). (Reuters, 2008; Larsson, 2006; Smith, 2008; Cienski, 2006; Sindelar, 2006)

[13] These tools have been widely used in some EU countries as well. Non-transparent business culture and the politically motivated behavior of Gazprom did not prevent some high-ranking politicians in the EU member states from being involved in lobbying for implementing some Russian energy projects in the EU. (Horbulin, 2017, p.103-105)

er that put at risk the stable functioning of the central electricity system that threatened blackouts throughout the entire country. The other TPPs were not able to timely provide backup power because of the shortage of coal caused by the territory occupation.

In 2014-2015, the transformer substations were repeatedly de-energized because of the several blackouts in large cities such as Luhansk and Donetsk. In general, during the first year of the warfare only, over 1,000 power outages were reported just in the Donetsk region due to the damages to 35-110 kV power lines. Over 10,000 damages were in 6-10 kV lines and transformer substations. On January 7, 2015 in the Donetsk and Lugansk regions 55 towns were de-energized (partially or completely); 28 transmission lines 220-330 kV, 3 transformer substation 220-330 kV, 44 lines 110-150 kV, 20 substation 110 kV, 86 lines 35 kV, 31 substation 35 kV, 149 lines 6-10 kV, and 780 substation were disabled.

Since the beginning of the conflict, natural gas infrastructure has been repeatedly attacked, too. In May and June 2014 three explosions occurred along the Urengoy-Pomary-Uzhgorod high pressure gas pipeline in the Ivano-Frankivsk region. On June 17, 2014 an explosion occurred along the same pipeline in the Poltava region. However, the gas supply was not interrupted thanks to Ukraine's extensive pipeline system and to the existence of reserve pipelines and roundabout routes. Such configurations show the high level of the resilience of the Ukrainian gas transit system and its preparedness for emergency.

Unfortunately, the internal distributional gas network of Ukraine has some weaknesses that were highlighted by the war. On February 17, 2015 the Uglegorsk TPP and the consumers in the Donetsk region were left without gas because the Novopskov-Kramatorsk pipeline was damaged. On August 23, 2014 the gas distribution station was damaged near Alchevsk, causing suspension of gas supply to Alchevsk, Perevalsk and Alchevsk Iron and Steel Works. On June 12, 2015 the Kramatorsk-Donetsk-Mariupol main gas pipeline was damaged. Considering the fact that this route has no backup pipelines and that Mariupol has no other gas supply routes, the region experienced a curtailment of gas supply. The same happened in Berdyansk and in other cities located nearby. Also, a number of municipal energy companies of these cities were forced to cut off gas consumption. Consequently, the production of goods was reduced leaving the economy without revenue and people with limited services at disposal.

During the fiercest phase of the conflict, militants repeatedly attacked water canals and pumping stations necessary for water supply as well as power lines. The militants also prevented pumping stations from being repaired by firing on the people in charge of the repairs. As a result, some villages in the Donetsk area had no water supply and electricity for several weeks. Also, between June 2014 and June 2015, 10 people from the staff of Donetskoblenerho (that is the electricity distribution system operator – DSO) died and 16 were wounded while working to repair the electrical system.

In this context, some other types of malicious actions should be mentioned. In June 2015, the Troitske village in the Luhansk region was left without electricity because of the fighting. It was not possible to restore the power supply because the transformers were turned into scrap by militants and locals. Several reports on the dismantling of power lines around Donetsk, Horlivka, Luhansk, and the Stakhanov area show that this is a criminal dimension of warfare (as well as dismantling of tram lines in Luhansk, some railroads lines around Donetsk, industry plants supply lines etc).

Dismantling of industrial plants equipment with consequent shipment to Russia as well as scrapping energy infrastructure became a very widespread and lucrative business in the occupied territory. In fact, in Donbass, several cases of massive destruction of infrastructure eventually occurred because of both the fighting and of robbery and looting.

Cyber-attack

Cyber-attacks are considered as the first ever known external intrusion in the CEI system causing outages.[14] An example is the case occurred on December 23, 2015 when some regional electricity distribution companies became objects of cyber-attack (Lee, Assante, Conway, 2016). The attackers used malware in order to get direct remote access to Supervisory Control And Data Acquisition (SCADA) systems, to blind its operators with the aim to cause undesirable changes in the distribution infrastructure and to delay the restoration of power supply by deleting the software of SCADA servers.

The attack caused the switching off of the power distribution substations (seven 110 kV and 23 35 kV substations). This led to the disconnection of consumers from the system and forced several companies to use manual operations. Power outages lasted up to 4 hours and affected more than 220, 000 customers.

Seizure of the Ukrainian CEI

Apart from destruction, critical energy infrastructure was seized by the Russian military units. For example, two offshore drills and pipelines as well as the infrastructure on the shore providing production and gas supply from the offshore fields in the Black Sea (the Odessa field) were captured. Also, a gas compressor station, which pumps gas from a field in the Azov Sea shelf (Strilkove), was taken under control by Russia in the Kherson region.

Ukraine did not react to the seizures adequately. After capturing the Parliament and the Government buildings of the Autonomous Republic of Crimea on February 27, 2014, it took only two weeks to also capture the Chornomornoftogaz energy company and expensive drilling rigs including fields in the Black Sea on March 4, 2014. During this period, Ukraine failed to respond because the government did not understand the importance of CEI, despite the fact that the Russian troops were only few kilometers away.

The shortage of anthracite coal, mined mainly in the occupied territory of Donbas, threatened to stop half of Ukraine's thermal power plants and some municipal boilers that could endanger the stability of energy supply throughout the country. Ukraine was therefore forced to face an emergency situation in the electricity sector, restricting the normal functioning of industries and imposing a limitation of the electricity supply to consumers.

Furthermore, an informational warfare campaign conducted by Russia threatened the stability of citizens' support to the newly elected Government of Ukraine. This situation forced Ukraine to make concessions on the question of electricity supply to occupied Crimea as well as to import electricity or coal from Russia in order to ensure the "habitual life standards" of the population. During the periods of electricity disruption caused by the damage of the TPP, Ukraine had to buy very expensive electricity from Russia as an emergency measure.

Furthermore, the stopping of the delivery of coal because of the disruption of transportation routes forced Ukraine to purchase coal from Russia, which had been stolen from the Ukrainian mines by the separatists (OSCE Special Monitoring Mission to Ukraine 2015). This means that the war against Ukraine was financed with Ukrainian resources. In addition, blockade of coal supply was among the means of Russia to force Ukraine to agree on requirements of self-proclaimed authorities and forming a basis information manipulations and pressure on Ukraine.

Based on the analysis of the events, the actions against CEI could be divided into two main groups. The first one includes unintentional actions, where disruption of CEI is a kind of "accidental" consequence of the fight-

[14] Later investigations revealed that the attackers were from the Internet sector, belonging to Russian internet providers. (Ministry of Energy of Ukraine, 2016)

[15] "Habitual life standards" is the style of livelihood and everyday routine to which people become accustomed.

[16] Unintentional actions represent the main cause of the damages to CEI in the Luhansk and the Donetsk regions.

ing. The second one refers to the targeted acts aiming at the deliberate disruption of the functionality of various CEIs.

In general, targeted actions, which could be classified as means of "hybrid warfare" (see Table 1), create serious problems to every country.

ACTION	EXAMPLES
Hindering the functioning of and/or seizing CEI	Seizure of CEI in Crimea, in the Kherson region and in some territories of Donbass. Blocking the delivery of coal from coal mines with the disruption of transportation routes Cyber-attacks against electrical energy networks that lead to blackouts in Western Ukraine
Destruction of the power supply system	Shelling thermal power plants (TPP) Disabling power station equipment, power lines, and transformers
Destruction of the gas supply system	Repeated damage of gas networks and distribution stations that provide gas to consumers in the Luhansk and Donetsk regions
Demolition of industrial units and infrastructure	Dismantling of industrial enterprises, mines, tram- and railways, power lines. Repeated damage of water canals and pumping stations of water supply
Preventing the restoration of CEI	Militants repeatedly shelled the pumping station for water supply, power lines and transformers and prevented its repair with firing.

Table 1: Typical targeted actions against energy infrastructure

THE ENERGY DIMENSION OF WARFARE IN THE NATIONAL SECURITY AND DEFENSE POLICY

Given the analysis above, two important lessons for national security can be identified.

The first lesson is that energy infrastructure is a very attractive target in modern warfare. Thanks to the high level of technological development, modern societies have become excessively dependent on stable energy supplies. Therefore, the intentional destruction of energy infrastructure and the disruption of energy supply could be interpreted as a deliberate attempt to spread discontent in the population and to provoke social and political unrest. From this point of view, these attempts can be considered as part of the non-military "energy dimension" of warfare and should consequently be taken into consideration in the planning of the national defense policy.

The analysis has shown that the targeted actions against CEI in Ukraine can also be identified as non-military means of warfare because of the following effects (see Table 2): (1) psychological pressure, in order to spread panic, social tension and discontent with the government; (2) economic losses, due to the seizure of CEI and energy resources, thus imposing an additional economic burden on the country or getting additional resource for war; and (3) local advantages, by achieving a better position to conduct certain operations (e.g. combat collision, terms of contracts, ceasefire negotiation) or by forcing the government to undergo certain actions (e.g. payments, sale or purchase of resources).

Psychological pressure	Economic losses	Tactical benefits
The threat to rupture the sustainable functionality of the Ukrainian unified energy system (due to lack of fuel- coal, natural gas- for power generation)	Seizure of energy production units and infrastructure (industry, resources, infrastructure)	Protection against possible attacks by means of positioning military troops nearby the infrastructure that is dangerous to attack (chemical plants or power plants and supply networks, gas pipelines)
Stopping power supply (damage to TPP and transformer substations, gas pipelines disruption)	Payment for stolen resources, goods and services (Ukraine compensates bills for energy supply to the occupied territories, while consumers in these areas do not pay)	Getting advantages in military operations (inability to leave the site of defense because of the need to protect infrastructure units such as power plants, transportation hubs, airports)
Termination of water supply to towns because of the breakdown of the pumping stations (damage of electrical networks, pipelines, preventing repairs)	Robbery at the Ukrainian state coal mines and sales of the stolen coal to Ukraine under the guise of Russian contracts	Getting advantages in political negotiation processes (ensuring favorable conditions for contracts to supply electric power to Crimea, exerting pressure to be in a better position during peace talks)

Table 2: Energy tools of war

The second lesson is that big part of the damage to CEI in Ukraine was caused by "unintentional" actions that resulted in unplanned and peripheral harm to CEI. However, the consequences were the same as in the case of intentional targeted actions, namely the disruption of the energy flow. These actions should be taken into consideration in the development of emergency response and defense policies.

It is necessary to have a two-level set of measures to ensure CEI protection, namely measures aiming at reducing the number of possible threats and measures aiming at responding to crises.

The first set of measures, which are used to manage "unintended acts", could be implemented in some cases within the preparedness system designed for peacetime. The system of CEI protection should be designed to ensure the continuity of the functions of an infrastructure and be realized through "preventive action planning", by giving special attention to ensuring physical protection, interconnectivity of CEI and availability of reserve capacities.

"Targeted acts" against CEI require the necessity of predicting the possible intentional attacks. This means the necessity to implement procedures concerning the evaluation of the risks to face both for the government and for the CEI operators, but also to establish a close Public - Private Partnership (PPP). An important aspect of this system is that targeted malicious acts require the exchange of sensitive information between the involved actors as well as the readiness of the military and law enforcement personnel to activate additional measures. These actions too should be included in the national defense policy.

Furthermore, the analysis of the events con-

cerning the functioning of CEI in Ukraine clearly shows that a number of tools could be useful to protect it. The following ones are some examples: a) enacting an "emergency preparedness plan" including the involvement of law enforcement and Army forces for CEI protection according to an established level of threats; b) increasing the awareness of the armed forces and of the law enforcement units on the importance of energy security, including the resilience of CEI; c) strengthening civil-military cooperation and encouraging the voluntary support in securing energy supply to households; d) creating reserves of energy resources and generating capacities (mobile generators and fuel), e) using the technical capabilities of the armed forces f) introducing additional organizational and technical measures to protect CEI against accidental damage caused by the fighting; g) establishing a communication channel between the fighting parties with the help of third parties if necessary (the third party is needed in order to overcome distrust between the fighting parties); h) securing the ceasefire during the repair work to restore the infrastructure (electricity, gas and water supply); i) establishing an international monitoring mission to prevent deliberate infrastructure damage and obstruction of CEI restoration ; j) avoiding the positioning of the military units nearby CEI if possible (firing against the military positioned nearby CEI could be extremely dangerous for CEI); k) coordinating the CEI protection in the areas of the conflict between the armed forces and the law enforcement agencies to prevent looting.

Today, Ukraine is in the process of translating the lessons learned into practical tasks. Ukraine has taken some steps forward to modernizing its physical protection of CEI and modernizing its legal and institutional base for the implementation of its critical infrastructure protection policy. Examples of practical measures are:

- revising the system of territorial defense, where some parts of the infrastructures were put under protection;
- reestablishing the National Guard of Ukraine as a law enforcement unit with heavy weaponry, that was able to repel the attack against protected objects and was tasked to take critical infrastructure under protection;
- strengthening the physical protection of transport and energy infrastructure with special agencies;
- improving the cooperation of local authorities with military and law enforcement forces (State Service of Ukraine for Emergency Situations, Army Forces, National Guard, Security Service) in order to strengthen the protection and recovery of critical infrastructure.

Additionally, some legislation concerning critical energy infrastructure protection was approved (President of Ukraine, 2015; President of Ukraine, 2016).

CONCLUSION

In conclusion, the Ukrainian experience in the context of the "hybrid war" demonstrates that it is necessary to implement a proactive energy security policy in order to resist the attempts of an aggressor aiming at negatively affecting the functioning of the energy sector.

As for the CEI protection policy in particular, it is necessary to rethink the paradigm of protection and to include those threats that had not been previously considered by the "peacetime" system. The reality of the tar-

[17] As for the energy sector, the requirements for such system are contained in the EU regulation №994/2010 on measures to ensure the security of gas supply, which requires that national governments develop a Preventive Action Plan and an Emergency Plan in the area of gas supply. (Official Journal of the European Union, 2010)

[18] An example of international monitoring is the OSCE Special Monitoring Mission (SMM) to Ukraine that facilitated the ceasefire and monitored the process of demining and of repairing a major water-supply pipelines as well as power lines. The SMM team was in close contact with the Ukrainian and Russian representatives of the Joint Coordination Centre as well as with the Ukrainian Armed Forces and the "DPR" "commanders" on site to help keeping the ceasefire (OSCE Special Monitoring Mission to Ukraine, 2016)

geted actions should be intended not only as acts of armed terrorist groups with light weapons but also as policies of terrorist states using heavy armory. It is also fundamental to include the energy dimension of warfare into the national defense policy and to raise the awareness of the Army and of the law enforcement forces on energy security.

At the same time, most measures supporting a smooth functioning of CEI should be implemented through the "emergency preparedness planning". In this context, one of the priorities is the development of a system for critical infrastructure protection. Ukraine started working in that direction by conceptualizing a policy on CEI protection and on the development of a legislation framework (President of Ukraine, 2016b; President of Ukraine, 2017).

BIBLIOGRAPHY

Biriukov, D., Kondratov, S., Nasvit, O. Sukhodolia, O. (2015). Green Paper on Critical Infrastructure Protection Paper. The NISS Analytical Report. Retrieved from http://en.niss.gov.ua/content/articles/files/Green-Paper-engl-4bd7c.pdf

Cienski, J. (2006). Baltic lessons for EU in dealing with a resurgent Russia. Financial Times. 24 November. Retrieved from http://www.ft.com/cms/s/0/05ff71f8-7b60-11db-bf9b-0000779e2340.html#axzz4KzXdkUYa

Hoffman, Frank G. (2009). Hybrid vs. Compound War. Armed Forces Journal. 1 October. Retrieved from http://www.armedforcesjournal.com/hybrid-vs-compound-war/

Horbulin, V. (2015). Donbas and Crimea: the price of return. NISS. Kiev. Retrieved from http://www.niss.gov.ua/content/articles/files/Razom_kRym_donbas-4ab2b.pdf

Horbulin, V. (2017). The World Hybrid War: Ukrainian Forefront. NISS. Kiev. Retrieved from http://www.niss.gov.ua/public/File/book_2017/HW_druk_fin+site_changed.rar

Larsson, R. (2006). Russia's Energy Policy: Dimensions and Russia's Reliability as an Energy Supplier. Scientific Report. FOI. Stockholm

Lee, R. L., Assante, M. J., Conway, T. (2016). Analysis of the cyber Attack on the Ukrainian Power Grid. Defense Use Case. E-ISAC. Washington

Ministry of Energy of Ukraine. (2016). Information of Ministry of Energy of Ukraine. 12 February. Retrieved from http://mpe.kmu.gov.ua/minugol/control/uk/publish/printable_article?art_id=245086886

Official Journal of the European Union. (2010). 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. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0001:0022:EN:PDF

OSCE Special Monitoring Mission to Ukraine. (2015). Latest from OSCE Special Monitoring Mission (SMM) to Ukraine, based on information received as of 19:30hrs, 12 October 2015. Retrieved from http://www.osce.org/press-releases

OSCE Special Monitoring Mission to Ukraine. (2016). Latest from OSCE Special Monitoring Mission to Ukraine, based on information received as of 19:30hrs, 13 March 2016. Retrieved from http://www.osce.org/ukraine-smm/227321

President of Ukraine. (2015). Decree of the President of Ukraine № 555/2015 that enacts the Decision of the National Security and Defense Council of Ukraine. Military Doctrine of Ukraine. 2 September. Retrieved from http://zakon2.rada.gov.ua/laws/show/555/2015/paran17#n17

President of Ukraine. (2016). Decree of the President of Ukraine № 92/2016 that enacts the Decision of the National Security and De-

fense Council of Ukraine. Concept for the Development of the Defense and Security Sector. 4 March. Retrieved from http://zakon2.rada.gov.ua/laws/show/92/2016

President of Ukraine. (2016a). Decree of the President of Ukraine № 96/2016 on the Cyber Security Strategy of Ukraine. 27 January. Retrieved from http://www.president.gov.ua/documents/962016-19836

President of Ukraine. (2016b). Decree of President of Ukraine № 8/2017 that enacts the Decision of the National Security and Defense Council of Ukraine. About the improvement of measures on providing critical infrastructure protection. 29 December. Retrieved from http://www.president.gov.ua/documents/82017-21058

President of Ukraine. (2017). Decree of President of Ukraine № 37/2017 that enacts the Decision of the National Security and Defense Council of Ukraine. About urgent measures on neutralization of energy security threats and strengthening of critical infrastructure protection. 16 February. Retrieved from http://www.president.gov.ua/documents/372017-21302

Reuters. (2008). FACTBOX: Russian oil and gas export interruptions. 28 August. Retrieved from http://www.reuters.com/article/idUSLS57897220080828

Sindelar, D. (2006). Georgia: Tbilisi Accuses Moscow Of Energy Sabotage. 13 January. Radio Free Europe. Retrieved from http://www.rferl.org/content/article/1064976.html

Smith, K. C. (2008). Russia and European Energy Security. Divide and Dominate. Center for Strategic and International Studies. CSIS Press. Washington.

Critical Energy Infrastructure: **Identification and Protection**

Moniek de Jong, NATO Energy Security Centre of Excellence, Lithuania
Larry Hughes, Dalhousie University, Canada

Infrastructure is essential to modern societies. Some infrastructure, such as that for water supply and communications, is considered critical because its disruption would affect most, if not all, of society. The importance of energy to modern society means its infrastructure is considered "uniquely critical" as most other infrastructure relies on it, directly or indirectly. A society's energy infrastructure is organized into an energy system, a hierarchical network of processes responsible for the transportation and conversion of energy, from suppliers to the services meeting the energy demands of end-users. As with infrastructure in general, some energy infrastructure is also considered critical. In order to effectively and efficiently protect critical energy infrastructure, the critical processes in the energy system must be identified. To assist the energy analyst, this paper describes several methods that are available to facilitate the identification process. After identifying the critical entities, an inventory of the possible threats should be the next priority. The paper shows how each threat can be assessed according to its likelihood and the system's vulnerability to it. Given the importance of critical energy infrastructure, the paper describes how countermeasures can be developed for the protection of infrastructure from threats without the unnecessary allocation of assets or funds. Importantly, it explains how protection measures can increase the energy security of the energy system.

Moniek de Jong, NATO Energy Security Centre of Excellence, Vilnius

Moniek de Jong is a Dutch energy researcher. She is engaged in independent energy security research dealing with topics like European Union natural gas diversification, energy policy, energy risks and climate change. She has collaborated with Professor Larry Hughes from Dalhousie University, in Halifax, Canada, on several papers dealing with energy security, European and Canadian climate change goals and risks in energy systems. Ms. De Jong holds a Master in International Relations and Organizations from the University of Groningen, in Groningen, the Netherlands and a Master in Energy Security Studies from the Masaryk University, in Brno, the Czech Republic. Previously, she was an intern at the NATO Energy Security Centre of Excellence in Vilnius, Lithuania.

INTRODUCTION

Prior to the widespread availability of high-density energy sources such as coal and crude oil in the 19th and early parts of the 20th centuries, almost all of the world's energy was supplied from various forms of biomass: woody biomass for cooking and heating, agricultural biomass for transportation (fodder for horses and other draught animals), and fats, such as tallow and whale oil, for lighting (Malanima, 2013; Malanima, 2010). By the middle of the 20th century, new sources of high-density energy were being made available, such as natural gas and uranium (IEA, 2015).

However, before these high-density sources of *primary* energy could be used to meet the fundamental anthropogenic energy needs of heat (for low- and high-temperature energy applications), transportation, and light, they had to be extracted from the earth and moved to where they could be converted into a usable form of *secondary* energy, such as petrol and diesel in oil refineries and electricity in power stations.

Since sources of secondary energy production are often hundreds of kilometres from where the energy will be used, transportation networks have been developed to carry the energy to where it will be consumed. However, in most cases, secondary energy requires one final conversion to meet the tertiary energy needs of the energy service, examples of which are shown in Table 1.

Although great changes have taken place over the past 250 years in the types of energy consumed and how they are consumed, there are three common activities. First, whatever source (e.g., tallow or natural gas), it must be extracted, second, it must be converted from one form to another (e.g., wood to heat or coal to electricity), and third, it must be transported (e.g., wood from the forest to the farm or natural gas from an offshore gas field to storage).

These activities are not energy, they are the physical entities organized into an energy system that extracts energy from nature, converts it from one form to another, and transports it from one location to another without changing it. To function, these entities consume energy to perform their tasks. This raises an important point: in order to benefit from an energy service, it is necessary that the following conditions be met (Hughes, 2012):

• There needs to be a supply of secondary energy (which implies that there is a primary energy source available for conversion). However, if the source of primary energy is lost or any of the entities are unable to function, it may not be possible to meet the energy requirements of the energy service.

Dr. Larry Hughes, Dalhousie University, Halifax

Dr. Larry Hughes is a professor in the Department of Electrical and Computer Engineering at Dalhousie University in Halifax, Nova Scotia, Canada. His research focusses on energy security in energy systems, energy transformation, and climate change. Dr. Hughes has published widely, both in academic journals such as *Applied Energy, Energy, and Energy Policy*, and in the mainstream media, such as the *Globe* and *Mail and Policy Options*. He is often quoted in the mainstream media and his research has influenced corporate and government energy policy in Nova Scotia. Between September 2015 and March 2016, he was a Visiting Professional at NATO ENSECCOE.

Service	Example	Secondary energy source	Secondary to tertiary conversion	Secondary energy source
Transportation	Aircraft	Jet fuel	Internal combustion engine	Distance travelled
	Elevator	Electricity	Electric motor	Vertical motion
Heating	Space heating	Natural gas	Furnace	Heat (hot air)
	Hot water	Electricity	Electric kettle	Heat (boiled water)
Transportation	Lighting	Electricity	Light bulb	Light (Lumens)
	Mobile phone	Electricity	Electricity to radio waves	Sound (Decibels)
	Computer	Electricity	Electricity to data	Information

Table 1: Examples of energy services and tertiary energy

• The person using the service should be able to pay for the cost of the energy required to meet its energy requirements.

• The energy supplied meets certain standards, usually environmental, to protect both humans and the environment.

If any of these conditions cannot be met, the energy service may not function, potentially affecting those using the service. In other words, the availability of affordable and environmentally acceptable supplies of energy is essential to the social and economic wellbeing that is, the *energy security*, of any society.

To ensure the continuation of our way of life, it is important for those responsible for the energy security of an energy system or the entities that comprise the system:

1. To know which parts of a system are critical to its operation

2. To understand the risks associated with each part of the system

3. To adapt the system and its internal structure so that it is resilient to these risks

Points '1' and '2' deal with the *identification* of the risks faced by part of the system, while '3' refers to existing and future protection of the system.

Given the importance of the entities or in*frastructure* that comprise a jurisdiction's energy system, a focus of governments and energy providers has been to maintain and improve the energy security of the jurisdiction. This paper is an introduction to energy systems, energy security, and explains how risks to the infrastructure can be identified and how the infrastructure can be protected.

The paper is organized as follows. In the next section, some of the concepts associated with critical infrastructure are discussed, including what critical infrastructure can mean to supranational and national governments as well as to individuals. The third section introduces energy systems and energy security before defining critical energy infrastructure. Methods of identifying the risks and threats facing an energy system's infrastructure are described in the fourth section, while techniques for protecting the infrastructure are covered in the fifth section. The paper con-

cludes with a brief review of what has been presented. Two appendices are included; the first presents a method that can be used to identify critical infrastructure in energy systems, while the second summarizes the military's role in critical infrastructure and critical energy infrastructure protection.

CRITICAL INFRASTRUCTURE

Infrastructure is defined by the Collins English Dictionary as *"the basic structure of an organization, system, etc."* (infrastructure, 2014), while the American Heritage Dictionary defines it as, *"The basic facilities, services, and installations needed for the functioning of a community or society, such as transportation and communications systems, water and power lines, and public institutions including schools, post offices, and prisons"* (infrastructure, 2011). From these two definitions, infrastructure can be thought of as the basic physical facilities that are needed for the functioning of society.

Critical is defined as *"forming or having the nature of a turning point; crucial or decisive"* or *"extremely important or essential"* (critical, 2011).

Some infrastructure is considered to be critical and is therefore referred to as critical infrastructure. The term is used widely:

• The European Union defines critical infrastructure as *"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"* (European Union, 2008).

• In the United States, it is described as anything that provides *"the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health"* (Homeland Security, 2016).

• Whereas the United Kingdom's definition includes anything that has an *"impact on delivery of the nation's essential services; economic impact (arising from loss of essential service) and impact on life (arising from loss of essential service)"* (Centre for the Protection of National Infrastructure, n.d.).

• Others have defined critical infrastructure as *"all assets that are so vital for any country that their destruction or degradation would have a debilitating effect on the essential functions of the government, national security, national economy or public health"* (Yusta, Correa, & Lacal-Arantegui, 2011; Hull, Belluck, & Lipchin, 2006).

Based on the definitions, critical infrastructure can thus be considered as being any infrastructure that is essential for the nation's functioning, and its people's safety and health. These definitions all focus on the national or supranational scale of critical infrastructure, but infrastructure can also be critical within these jurisdictions (see Figure 1). For example, if the national infrastructure is still working, but for some reason an individual's or a region's infrastructure is not. In this case, the infrastructure is still critical to the individual or the region, but is not critical on the national level. As critical infrastructure is normally only reviewed on the national

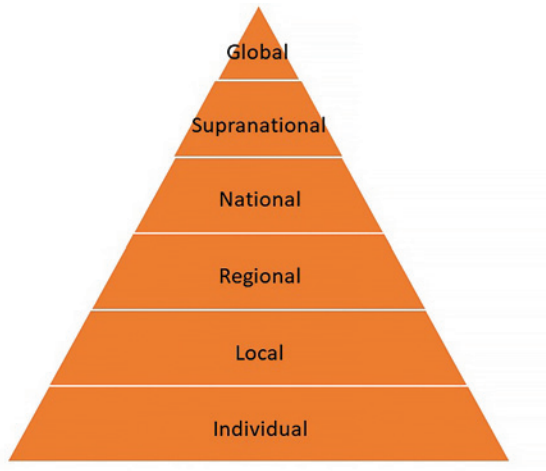


Figure 1: An example of levels and critical energy infrastructure

level and not on lower levels, many aspects are excluded and give an unrealistic overview of the potential risks facing the infrastructure within the jurisdiction.

The figure can also be used to demonstrate the hierarchy of levels by using the example of water service to a building. For example, should the water supply be disrupted by accidently damaging the building's connection to the water main, then water distribution in the building is disrupted. The water connection to the building can be considered critical infrastructure to anyone associated with the building. However, if the neighbouring buildings are unaffected by the broken connection, then the water main connection is not critical infrastructure to them as they continue to receive water. Thus, the local infrastructure is still intact (minus one building). The higher you get the smaller the non-functioning of the water supply to the building gets. One building without water supply does not have a debilitating effect on the country's water supply, the critical water infrastructure is functioning normally. All the other buildings have access to water. In order to restore water service the broken connection needs to be replaced.

The other way, "top-to-bottom" view shows that if the national critical infrastructure is not working, for example because of droughts there is no supply water left in the reservoirs, then everybody below the national layer is affected. The regional infrastructure, local infrastructure and the individual layers are also left without water services. In this case, in order to restore water supply, the water reservoirs need to be filled (rain or transporting water to the reservoir).

The increasing use of information and communications technology (ICT) in critical infrastructure in recent years, means that critical infrastructure can be discussed on two different levels, the physical and the cyber (Genge, Kiss, & Haller, 2015). An entity's physical infrastructure is, for example, the pipes, pumps, and wires, that are needed to supply the service. The cyber infrastructure is the software and digital framework to support the physical infrastructure, or in some cases it is part of the supply system (in case of information and communications infrastructure).

CRITICAL ENERGY INFRASTRUCTURE

Energy has many meanings, such as the *"capacity of a body or system to do work"* or *"a source of usable power, as fossil fuel or electricity"* (energy, n.d.).

For the purposes of this report, energy can refer to primary energy (such as coal, crude oil, natural gas, water, uranium, biomass, wind, or sunlight), secondary energy (primary energy that has been converted into, for example, electricity, diesel, or kerosene), and tertiary energy (secondary converted into a service, such as transportation, heating and cooling, and lighting).

Energy systems

Energy infrastructure is any facility or entity that converts one type of energy to another or transports a flow of energy from one entity to another. It can also refer to energy management technology, such as metering and modern power plant controls. An energy system consists of entities linked together forming chains from energy sources to end-users (Ikeonu, 2014; Vasenin, 2013; Hughes, 2012). An example of a system's infrastructure and chains include electricity infrastructure (generating station, transmission and distribution grids, substations, and transformers), natural gas infrastructure (storage, transmission, distribution, and furnaces), and petroleum infrastructure (refineries, tank farms, pipelines, and fuel stations) (OSCE, 2013).

The American Heritage Dictionary defines system as "a group of interacting, interrelated, or interdependent elements forming a complex whole" (system, 2011). An energy system is one that is responsible for transporting and converting primary or secondary energy to meet the energy needs of an end-user, such as a sector or a service (as tertiary energy) within the sector. The end-user

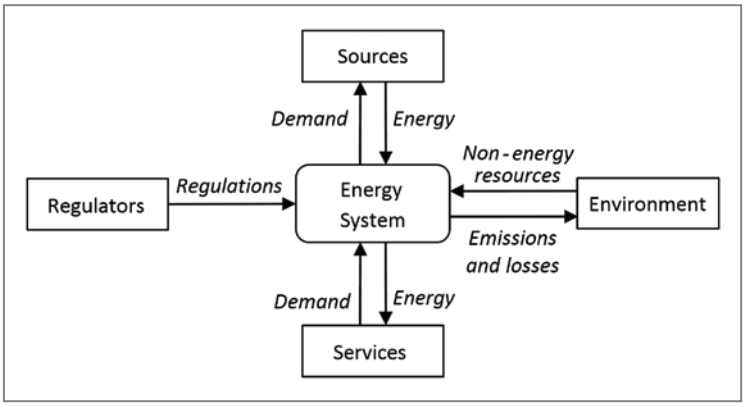


Figure 2: An energy system and its external entities (from (Hughes, 2012)

and the holder of the natural resource can be considered external actors. Figure 2 is a representation of an energy system with its external actors.

An energy system is comprised of multiple entities, some of which are responsible for energy conversion and others energy transportation. An energy entity receives a request for energy, the $Demand_{IN}$ flow, from a downstream entity (either another converting or transporting entity) process or a service). In turn, it requests an amount of energy, specified in a $Demand_{OUT}$ flow, from an upstream entity (either a process or an energy source); the efficiency of the entity determines $Demand_{OUT}$. The upstream entity is expected to respond with the requested amount of energy, $Energy_{IN}$, which should equal $Demand_{OUT}$. The entity then converts or transports this flow of energy, making it available to the downstream entity as $Energy_{OUT}$, in this case, equal to $Demand_{IN}$. The entity's actions are dictated by its internal structure and a set of rules, $Policy_{IN}$, which it is expected to follow. The entity typically accesses the environment: using those things it requires, $Environment_{IN}$, and emitting waste or other byproducts, $Environment_{OUT}$. Figure 3 is an example of a linear energy chain. Different entities have different functions.

A jurisdiction relies on an energy system to meet its energy requirements and the energy system is responsible for a jurisdiction's energy security (Hughes, de Jong, & Wang, 2016). Combining the previously established definition of critical infrastructure and the above discussed overview of energy systems has led to the following definition of critical energy infrastructure "any infrastructure that, if experiencing an increase in stress, either by itself or in combination with other infrastructure, results in a disruption of some

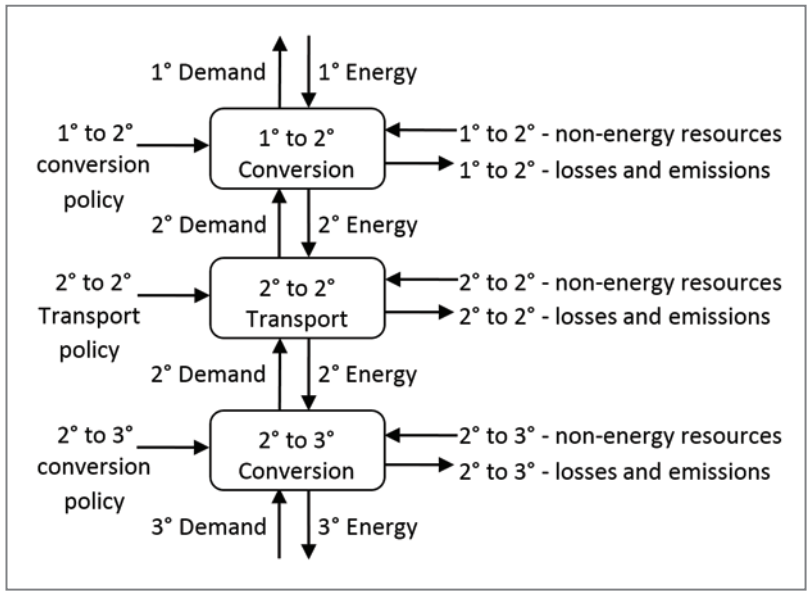


Figure 3: A linear energy chain (1°, 2°, 3° denote primary, secondary, and tertiary, respectively)

or all of jurisdiction's energy services or energy suppliers, or both."

Energy infrastructure is important because of its function in society and its effect on the operation of other critical infrastructure (Lauge, Hernantes, & Sarriegi, 2014; Yusta, Correa, & Lacal-Arantegui, 2011). Other sectors that depend on electricity are emergency services, military services, communications sector, water, health care and other energy sectors like oil and gas (Homeland Security, 2017). The United States Department of Homeland Security also underscores the importance of energy to other critical infrastructure with the observation that *"the Energy Sector [is] as uniquely critical because it provides an 'enabling function' across all critical infrastructure sectors"* (DHS, n.d.). Quite simply, without energy, the operation of many other sectors cannot be sustained. The energy sector has been declared *"uniquely critical"* by Presidential Policy Directive 21, because it has the ability to affect fifteen other critical infrastructure sectors (Hemme, 2014). The energy sector is thus of crucial importance to society, making its infrastructure *critical*.

Identifying critical energy infrastructure

The entities in an energy chain can be represented as a directed graph of edges and nodes. In such a representation, a node is an energy entity and the edge is a flow from one entity to another. A system can consist of linear and non-linear chains of entities.

A linear chain is one in which the $Energy_{OUT}$ flow from one entity is also the $Energy_{IN}$ flow to a single, downstream neighbour, as shown in Figure 4. Remove one of the entities and the flow is disrupted. An example of a linear system is the Yamal natural gas pipeline that transports natural gas from Russia to Europe (see Figure 5).

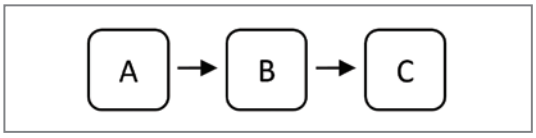


Figure 4: Linear chain

Figure 5: Yamal pipeline (Gazprom, 2017)

In a non-linear chain, at least one entity has two or more upstream or downstream neighbours: the flows either converge to a single entity from its upstream neighbours or diverge from a single entity to its downstream neighbours (see Figure 6). Non-linear chains have the advantage of diversity, allowing the convergent entity (such as 'D' in Figure 6) to potentially reduce the risk associated with the loss of an upstream neighbour. Similarly, the risk associated with the loss of a downstream neighbour can be reduced for a divergent entity (such as 'P' in Figure 6). However, despite these advantages, 'D' and 'P' are examples of potential single-points-of-failure – should ei-

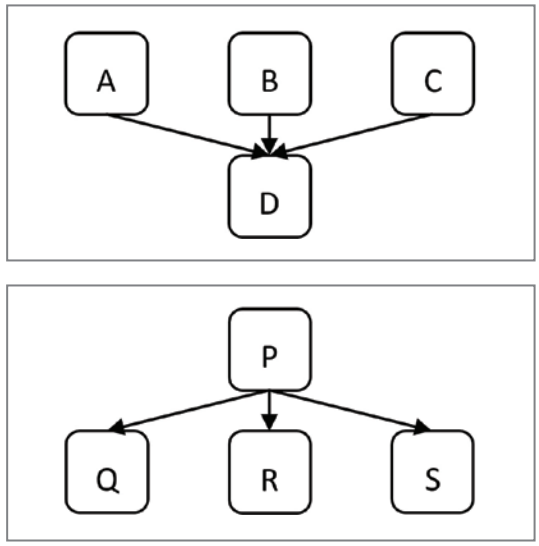


Figure 6: Non-linear chain with converging flows (left) and diverging flows (right)

ther fail, the flow of energy through the chain will be disrupted (Ulbrich, et al., 2012); they are considered critical.

Converging flows are for example the supply of electricity generated through different power plants and sources. Consider a country with a wide variety of power plants (e.g., coal, natural gas and nuclear) and that has additional renewable energy sources. They all supply the electricity grid, but when one of the plants is taken offline, the electricity is still being supplied to the grid by the other generators. An example of a diverging flow is the distribution of refined oil products to different fuel stations, one refinery will supply multiple fuel stations. Should one fuel station disappear from the infrastructure, the refinery and the other fuel stations will still function.

Non-linear chains meet the EU's N-1 rule: An entity must survive the loss of one of its 'N' input flows (European Parliament, 2010). In this case, the entity has two flows, losing one of them does not result in its shutdown. Multiple neighbours are not a guarantee of energy security either, especially if the flows between entities are unequal – the loss of a flow could result in disruption of the chain, despite the apparent advantage of diversity (Ranjan & Hughes, 2014). For example, in Figure 6, one, or some combination, of the nodes 'A', 'B', 'C', 'Q', 'R' and 'S' could also be critical to the functioning of the infrastructure.

In some cases, a non-linear chain can be circular, with EnergyIN flows available from both sets of neighbours and EnergyOUT flows to both. There are also circular flows, an example of a circular chain is Amber Grid, Lithuania's natural gas pipeline system (Amber Grid, 2014). Amber grid is an interesting example of critical energy infrastructure protection. Any entity in Amber grid has two convergent flows, a linear left-flow and a linear right-flow. Breaking an entity (a flow) on one side is of no consequence, because the flow exists on the other side. Another example is the reverse flow of natural gas from the European Union to Ukraine. In this case every entity has the option of two in- and out- flow from both sides. Natural gas can flow from east to west or from west to east.

Critical energy infrastructure part

After identifying what kind of system the energy infrastructure is, the next step is the identification of the specific parts of the energy infrastructure that ensure continued functioning. In order to effectively and efficiently implement countermeasures to reduce the risks facing the infrastructure.

The critical path method (CPM) can be used to determine how infrastructure functions and which nodes are the most critical. In CPM every activity in the chain is described and also the time required to fulfill its task is indicated (Santiago & Magallon, 2009). For example, when talking about getting crude oil from producer to consumer there are different routes to take. The United States can import crude oil from Canada and transport it to its refineries, but should Canadian oil production stop (for whatever reason) then the United States will have to import more crude oil from Venezuela or the Middle East. These crudes will have a longer transport time than the Canadian crude. The same applies to Europe; Middle Eastern crude will reach a European refinery the fastest when transported through the Suez canal. Should the canal be blocked, the crude would have to travel around Africa to reach its European market. This would lead to delays of delivery and could lead to the non-functioning of the system for a certain period of time.

In order to identify what part of the energy infrastructure is critical an analysis of the system needs to be done. Augutis et al. discuss identifying critical energy infrastructure in Lithuania. They focus on a single point in the infrastructure that is critical for its functioning (Augutis, Martišauskas, & Krikštolaitis, 2015).

This can also be done manually when dealing with smaller systems to analyze the effect of the removal of each entity from the system; however, when dealing with more complex systems software might be necessary to analyze the infrastructure. Other options are to look at combinations of nodes that can be critical for the functioning of the infrastructure. As in some cases the non-functioning of two nodes in the infrastructure can have more consequences for the service than the non-functioning of one node. Appendix 1 presents one such method and its software implementation is applied to a hypothetical energy system.

THREATS

Approaches to determining which entities are critical to the energy system was shown above. After deciding if the entity is critical, it is necessary to identify the threats posed to an entity and the entity's vulnerability to the threat (Hughes, de Jong, & Wang, 2016). Assessing the threats should lead to the development of countermeasures to reduce the likelihood of disruption of the infrastructure. If there are insufficient countermeasures and there is a high likelihood of the threat occurring, the entity—and hence those relying on the entity—may be disrupted. The loss of an energy supply or the failure of an entity – within a chain can result in a deterioration of the jurisdiction's energy security (Hughes, 2012).

Threats to energy infrastructure can be divided into two categories: internal and external.

Internal threats

Internal threats can be further divided into accidental, adversarial and structural threats (Robles, et al., n.d.; Farrell, Zerriffi, & Dowlatabadi, 2004; European Commission, 2016). Examples of internal accidental threats to energy infrastructure are inadvertently reading a meter incorrectly - consequently letting pressure build-up too high - and could lead to terminating operations; not following security protocols, or bringing an infected memory stick into the entity.

Adversarial internal threats can be a disgruntled employee that has access to the infrastructure and also knows the structure.

Structural threats can be ageing equipment, for example the East Harlem gas explosion that was attributed to a 127-year old gas main and led to the termination of gas services to part of the city (Sanchez, 2014).

External threats

External threats can be divided into four categories; accidental, adversarial, natural disasters and resource (Robles, et al., n.d.; Farrell, Zerriffi, & Dowlatabadi, 2004; European Commission, 2016). An example of natural disaster is the 2011 earthquake and subsequent tsunami that led to the shut-down of the Fukushima Daiichi nuclear power plant (Hayashi & Hughes, 2013) or hurricanes Katrina and Rita that destroyed offshore rigs and caused a shortage of fuel in the United States (Parfomak, 2008). Other natural disasters that can pose a threat to energy infrastructure are floods, extreme weather events and tornadoes.

Critical energy infrastructure failure induced by adversarial threats are occurring more frequently in recent years, especially cyber-attacks. The Shamoon malware was used in 2012 to disable and paralyze computers of Saudi Aramco (OSCE, 2013). Of course, adversarial threats are not only cyber-attacks, but also terrorist actions, sabotage, product tampering and bombings (Robles, et al., n.d.; Li, Rosenwald, Jung, & Liu, 2005). External accidents can also threaten the operations of the energy infrastructure (Robles, et al., n.d.). An example is the 1996 black-out in fourteen states in the United States, caused by a high voltage line touching a tree branch (Amin, 2005). The resource threat is that the source of the resource has been completely explored, such as the fears surrounding peak oil around 2008.

Cyber threats

Because of the dual-layer of critical energy infrastructure - the physical and the cy-

ber structure (Genge, Kiss, & Haller, 2015) - critical energy infrastructure has received an additional set of threats. The increased and continued automatization of many parts of the energy infrastructure in recent years have made energy infrastructure vulnerable to cyberthreats (OSCE, 2013; Cazorla, Alcaraz, & Lopez, 2015). Malware is the weapon of choice for cyber-attacks on energy infrastructure; see previously mentioned Shamoon malware (JangJaccard & Nepal, 2014; OSCE, 2013). However, other forms of cyber-intrusion have taken place in critical energy infrastructure, the Slammer worm for example clogged the Davis-Besse nuclear power plant network in 2003 and made safety readings inaccessible to employees (Kesler, 2011). Also, the case of the Symantec's Dragonfly/ Energetic Bear attacks on energy suppliers have proven that energy infrastructure is being targeted through cyber-attacks and not just physical attacks (Bronk, 2015). In some cases an employee of the entity is the unwitting accomplice of the culprit, by innocently opening an e-mail attachment from a seemingly authorized source (Jouini, Rabai, & Aissa, 2014).

Also, cyber threats appear on different levels. The implementation of smart grids could lead to new threats on the individual level. Electronic devices could be regulated and monitored by outsiders and used to manipulate energy demand from private homes (Wang & Lu, 2013). Also, the applications to regulate energy usage through mobile devices is exposing homeowners to cyber-threats. Transmitting and receiving information digitally can offer cyber criminals another route to threaten the electricity system. This could potentially lead to the national electric grid being disabled.

In order to minimize these threats from materializing there has to be some form of protection in place to counter these threats or to completely remove the possibility of them from happening.

PROTECTION

Critical energy infrastructure protection is measures taken to ensure that critical energy infrastructure can continue normal functioning. Critical energy infrastructure protection is an important aspect of critical energy infrastructure. Without taking measures to protect it, the infrastructure would remain as critical as it was during the initial analysis. In that case stress in the form of threats can cause an infrastructure to stop functioning. Stress occurs when an event or threat influences the functioning of one or more entities. An entity can become more resilient by changing its functioning or structure (adapting leads to more resilience). Resilience is "the ability of a system to resist, absorb, recover from, or successfully adapt to a change in environment or conditions" (Moteff, 2012). Resilience can be divided into four different dimensions: technical, organizational, economic, and social (Labaka, Hernantes, & Sarriegi, 2016).

The goal of critical energy infrastructure protection is to address threats pre-emptively instead of reactively protecting energy infrastructure (Hemme, 2014). Countermeasures to these threats will increase the resilience of the system and decrease the likelihood of these threats happening. Governments have created different institutions, and programs dealing solely with the protection of critical infrastructure; for example, the United States Department of Homeland Security – their suggestions for critical infrastructure protection are: invest in physical and cyber risk management products and plans, educate employees about critical infrastructure security and resilience, plan for business continuity, share threat and incident information, report suspicious activity and prepare for all hazards at home and at work (DHS, n.d.), or the European Union's Programme for European Critical Infrastructure – their suggestions are identifying critical infrastructures and learning how to better protect them, funding information sharing and alerting systems, the development of ways to assess

interdependence between ICT and electricity transmission networks, and the creation of a 'good practices' manual for policy makers (European Commission, 2016), and there are different journals that deal with critical infrastructure protection – such as the International Journal of Critical Infrastructure Protection. Not only countries are involved in critical energy infrastructure protection, inter-governmental organizations like NATO are also involved. In Appendix 2, the military and its relations to critical energy infrastructure are discussed in more detail.

Most energy infrastructure tends to be operated by private companies and no longer by the state. This has added to the complexity of protection of critical energy infrastructure as states rely on the critical infrastructure for the functioning of society and private companies rely on them for revenue to continue their operations. Both have different incentives for ensuring the functioning of critical energy infrastructure, but states still exert some control by imposing regulations on energy entities for their functioning and protection. The operators of the entity have in-depth knowledge of the infrastructure and are therefore better at determining the weak points than outsiders (Giannopoulos, Filippini, & Schimmer, 2012).

Countermeasures

There are different ways to protect critical energy infrastructure. Physical and cyber protection like creating barriers to the infrastructure, such as the "guns, gates and guards" approach (Englefield, 2014). This approach entails protecting critical energy infrastructure by closing off certain areas and thereby restricting their access through gates, placing guards at these gates and in addition guards can carry guns to further protect the infrastructure. Since it is financially and physically impossible to completely protect infrastructure (e.g., a pipeline that is thousands of kilometers long) (OSCE, 2013), or to manually control/observe every process in a power plant, choices need to be made. Hence, the identification process to locate the exact location for the use of the protection measures.

Protection is more than barriers; having spare parts in stock or plans for how to minimize the down-time of a critical energy infrastructure is also protection. This can be done when the likelihood of a threat materializing is high, but you cannot stop it because of uncertainty over the exact location (e.g. an electricity transmission network). Or it is financially a sound option to repair the transmission wires when faulty, instead of spending large sums of money on protecting the wires from breaking in the first place.

As mentioned before there are internal and external threats and different threats demand different protection measures. Threats from a disgruntled employee (internal adversarial) are the most difficult to counter, because they have access to the infrastructure, have extensive knowledge of the system's functioning and will more easily find the critical part of the system. These threats are therefore difficult to prevent (Liu, Wang, & Camp, 2008). There are limited options to preventing insider threats: increased security profiling of employees and ensuring limited access to systems could help decrease the risks of insider attacks.

With the cyber-dimensions, different forms of protections have increased as well. The countermeasures are focused on protecting sensitive information, system integrity and also proving access to the system for those who should have access to it (Jang-Jaccard & Nepal, 2014; Jouini, Rabai, & Aissa, 2014). Cyber-attacks can be done by an adversary with limited resources and no physical access to the infrastructure. They have a lower risk of detection and can, in theory, be done from the comfort of the adversary's home. The examples of cyberthreats mentioned before make cyber protection of critical energy infrastructure not only relevant on the national level, but at the individual level as well. Risk analysis will help determine the most suitable countermeasure for a specific threat.

Risk analysis

By doing a risk analysis the operator of the infrastructure can assess the different threats the infrastructure is exposed to, the vulnerability to the threat, the impact of the threat and the likelihood of the threat occurring. It is also important to repeat this analysis periodically, because circumstances can change.

There are many methods available for the analysis of risk to energy infrastructure (Ang, Choong, & Ng, 2015; Jun, Kim, & Chang, 2009; Checchi, Behrens, & Egenhofer, 2009; Gupta, 2008; Marrero, Puch, & Ramos-Real, 2015; Matsumoto & Andriosopoulos, 2016; Weisser, 2007; Wu, Wei, & Liu, 2007; Zhang, Ji, & Fan, 2013). The impact on the infrastructure is usually assessed by the financial losses, as this provides the operator of the infrastructure with a costbenefit comparison for countermeasures. Assessments are often limited to a specific part of the infrastructure, reflecting the requirements of the operators (Giannopoulos, Filippini, & Schimmer, 2012). When countermeasures are taken and a threat still materializes, the affected entity should recover as quickly as possible and return to normal functioning (Hughes, 2015). After recovery, the system should re-assess the threat, its vulnerability, and likelihood of occurrence, and if necessary take the appropriate steps to minimize the threat from happening again - adapt to protect itself from the same threat (Hutchison, Waage, & Bennett, 2016).

Layers of critical energy infrastructure protection

Unlike Assaf (2008) - who divided the critical infrastructure protection regulatory continuum into governmental ownership to regulations to market-based approaches - our approach shows that critical infrastructure protection is divided into different levels and that markets (private companies) are willing and capable of protecting their critical infrastructure to a certain level. But in the end, it is the government that picks up where the market ends or in cases where protection is too important to leave to the private companies, such as nuclear facilities (one of the reasons for the heavy regulatory system associated with nuclear power). Private companies are also willing to provide protection, but at a limited cost. It is likely that states will take the responsibility where private companies are ending theirs – this is the company's boundary. States will provide security in the form of police or military presence for critical energy infrastructure or enforce regulation to force private companies to take the necessary countermeasures. Examples are nuclear power plants that have the potential to cause disruption of society in case of breaching its structure and refineries that could negatively affect a country's economy and the availability of fuel should it be damaged.

Similar to the scaling of critical infrastructure, the protection of critical energy infrastructure can also be scaled. Protection can take place on different levels. A light bulb in a residence is critical energy infrastructure to the resident. The resident unknowingly does a risk analysis, determining the necessary countermeasures; for example, buying a spare light bulb or having an emergency supply of candles. This is critical energy infrastructure protection on the individual – home – level. The protection of individual critical energy infrastructure is typically the individual's responsibility. The state usually does not provide people with a spare light bulb or candles in case the bulb burns out. On a higher layer, for example, local, electricity supply to a city might be disrupted and despite a back-up light bulb, the lights will not come on. A back-up generator might protect an individual from black-outs, but in the end it is the electricity company that should restore service to the city. The countermeasure should be taken by the company and not by the individual.

The highest level is when critical energy infrastructure is protected by an international alliance, such as NATO's presence off of the Horn of Africa to protect, amongst other things, shipments of energy products (Rühle & Grubliauskas, 2012). NATO's naval pres-

ence off the Horn of Africa protected critical energy infrastructure as no single energy company had the financial means to provide the necessary countermeasures to protect shipping. Without NATO the availability of global energy would have been put at risk. This would have subsequently put lower layers at risk of non-functioning critical energy infrastructure. Disrupted supply of crude oil to refineries would lead to a disruption of refined goods to the markets (e.g., petrol or diesel). In the end the individual would be affected by the disruption on the global layer. Figure 1 shows the way the responsibility of protection of critical energy infrastructure is transferred from individual to the highest actor. Indirectly, the global protection measures also positively influence the individual's energy security.

Also, climate change can be considered a threat to critical energy infrastructure. Existing offshore rigs might need to be restructured, nuclear power plants, refineries and LNG terminals will need to be moved or protected, because rising sea levels could endanger their functioning. Also rising sea levels might negatively affect existing shipping lanes. In order to protect against these events happening, international cooperation is taking place to ensure these threats do not materialize.

As the examples have shown critical energy infrastructure protection is not only a case of protection on the national level, it is much more. Individuals are part of protecting critical energy infrastructure.

Counter intuitively, the implementation of countermeasures on a specific part or entity of the critical energy infrastructure might make other parts or entities more vulnerable. For example, protecting the most important node in a natural gas pipeline system might cause adversaries to shift their attention to other nodes in the system that are not that as well protected. Targeting a certain combination of nodes might also be a more effective strategy for adversaries.

The protection of critical energy infrastructure requires the detailed study and analysis of the energy system and the jurisdiction it serves. Different threats demand different countermeasures and different systems and entities also require different countermeasures. Implementing countermeasures at one location might lead to the exposure of another. There is no "one-size fits-all" solution.

CONCLUDING REMARKS

Energy has been a crucial part of our lives. In the 20th century, essential energy sources were found in areas that were far away from their consumers. These resources needed to be transported to their consumers and converted into usable products (from primary to secondary and tertiary).The system of converting and transporting energy sources has become more complex. The system became important for the functioning of society, as energy was used for different sectors. The functioning of the energy system has been defined by governments as critical infrastructure. Critical infrastructure also exists on lower and higher layers than the national (individual, or global level). In order to ensure proper functioning of the energy infrastructure, governments demand protection measures to be taken. The protection measures increase the security of the system and in turn increase energy security. In order to effectively and efficiently implement protection measures, the critical part of the system, or entity needed to be identified for the functioning of the system. This can be done using simple to more complex methods of elimination. Multiple methods have proven their value for identification. The system can take different forms (e.g., linear, converging), this can also influence the critical nodes within the system.

After identifying the critical infrastructure, an assessment of the threats that could potentially lead to the non-functioning of the infrastructure should be performed. There are different kinds of threats the infrastructure could be exposed to. They should be ranked, the vulnerability of the infrastructure to the

threat and likelihood of the threat materializing should be reviewed. After the assessment it is necessary to examine the different options for protection of critical energy infrastructure. The diversity of the systems and threats is translated into a plethora of protection measures that could be implemented. Also, the acceptance that some threats are unavoidable is discussed. The preparedness of the critical energy infrastructure to address threats, even unavoidable, are key in their recovery to normal functioning.

Besides national critical energy infrastructure protection, there are also lower layers of critical infrastructure. The protection of critical energy infrastructure on higher layers helps make lower layers more secure and increase energy security. This does not mean that no protection measures need to be taken on the lower layer, as an individual risk analysis might expose more threats.

This paper has examined the basic principles of energy systems, critical energy infrastructure and its identification and subsequent protection. The importance of continued risk analysis of critical energy infrastructure cannot be overstated.

APPENDIX 1: EXAMPLE OF CRITICAL INFRASTRUCTURE IDENTIFICATION

Most methods that focus on identification use some form of elimination of nodes and edges. In this appendix an example method is given to identify critical entities of critical infrastructure. First, the hypothetical energy system is discussed. In the second part the method used to determine what part is critical is explained. And finally the results have will be discussed.

Figure 7 is a representation of a hypothetical energy system. The numbered boxes are the entities responsible for the conversion and transportation of energy, while the arrows connecting the boxes indicate the maximum possible energy flow from one entity to another.

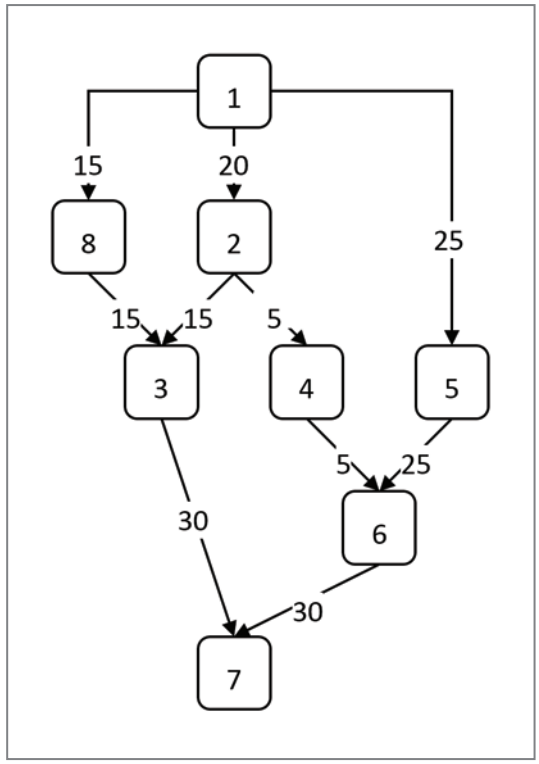


Figure 7: Representation of a hypothetical energy system

The entities are defined as follows:

1. The source or supplying entity with divergent flows to its three downstream neighbours. It can supply up to 60 units of energy.

2. An entity with a divergent flow, taking 20 units of energy from the upstream and supplying 15 units to entity 3 and 5 units to entity 4.

3. An example of an entity with a convergent flow, combining two flows of 15 units (from entities 2 and 8) into a single 30 unit flow to entity 7.

4. An entity taking 5 units of energy from 2 and supplying it to entity 6.

5. An entity taking 25 units of energy from 1 and supplying it to entity 6.

6. An entity with convergent flows, combining two flows of 5 and 25 units of energy from entities 4 and 5, respectively, into a single 30 unit flow for entity 7.

7. The end-use energy service entity. Two 30 unit flows converge to meet its demand (from entities 3 and 6). For the purposes of this example, entity 7 only requires 35 units of energy.

8. An entity taking 15 units of energy from entity 1 and supplying it to entity 3.

For the purposes of this example, the entities are assumed to have no losses and, with the exception of the energy service, have no minimum operational threshold.

The problem confronting the energy analyst is deciding which of the entities is critical to the uninterrupted operation of the energy service, entity 7. The removal of nodes and edges can be analyzed using static or dynamic analysis. Static analysis being the removal of a node or edge without the need for redistribution and dynamic analysis requires the distribution of the flow through other nodes (Rosas-Casals, Valverde, & Sole, 2006). In our example dynamic analysis will be applied.

METHOD

The method used to determine the critical parts of Figure 7 is described in this appendix.

Determining if an entity is critical involves stopping all or part of its output flows of energy and, from this, deciding whether sufficient energy would reach the energy service to allow it to continue operating. While this is a trivial exercise for a simple energy system consisting of a limited number of entities, it can be overwhelming, tedious, and error-prone when the system is comprised of tens or hundreds of entities.

A method for determining the effects on the energy service of each entity stopping its energy flow(s) can be implemented in software. Each entity can be represented in terms of a number of attributes common to all entities, such as its upstream neighbours (i.e., the entities supplying it with energy), the demand from its downstream neighbour, and its current state (i.e., Normal, if operating correctly, or Disruption, if an event has occurred to stop it from operating). The software can then "walk" through the system, determining whether those entities operating correctly are able to produce sufficient energy to meet the energy demands of the energy service.

This method has been implemented in a programming language known as VBA. The data is supplied in an Excel spreadsheet. The program reads the data from the spreadsheet and writes the results to the same spreadsheet.

RESULTS

The example energy system shown in Figure 7 was encoded in an Excel spreadsheet and the program was executed, the resulting output is listed here (in bold):

First test is not critical infrastructure - Ein: 35

The software first determines if the system can supply the energy service with the energy it needs. If so, no part of the infrastructure is found to be critical. The energy to the energy service (Ein) is 35 units, which is the minimum required by the energy service.

1 - Source is critical infrastructure - Ein: 0

The source (entity 1) is considered critical – its removal results in zero units of energy reaching the energy service.

2 - Fork is not critical infrastructure - Ein: 35

The disruption of entity 2 (fork) does not affect the operation of the energy service as it will still have 40 units of energy available to it (25 units from entity 6 and 15 units from entity 3).

3 - Join is critical infrastructure - Ein: 30

If entity 3 (join) is disrupted, the energy service stops because a maximum of only 30 energy units can reach it (from entity 6). Entity 3 is therefore critical.

4 - Entity is not critical infrastructure - Ein: 35

Disrupting entity 4 does not disrupt the operation of the energy service, meaning it is not critical. There are still 55 units of energy available to the energy service.

5 - Entity is not critical infrastructure - Ein: 35

Disrupting entity 5 does not disrupt the operation of the energy service, meaning it is not critical since the energy service has 35 units of energy available to it.

6 - Join is critical infrastructure - Ein: 30

Entity 6 (a join) is critical because if it is disrupted, 30 units of energy are no longer available to the end-user.

7 - End-user is critical infrastructure - Ein: 0

Not surprisingly, disrupting the end-user means it has no energy to operate. It is critical.

8 - Entity is not critical infrastructure - Ein: 35

Disrupting entity 8 does not disrupt the operation of the energy service, meaning it is not critical. The energy service has 45 units of energy available.

Entities 1, 3, 6 and 7 are thus critical for the infrastructure. With the above results, an energy analyst can proceed to determine what part of the energy infrastructure are critical.

APPENDIX 2: THE MILITARY AND CRITICAL INFRASTRUCTURE

The functioning of all critical infrastructure is important for society and also for the military. The armed forces are even considered a critical infrastructure as part of government services. The military depends on the functioning of most critical infrastructure for their activities (water, communications and of course energy infrastructure) (Lynn, 1994). Considering the privatization of energy infrastructure, the usage of military assets for protecting them is not likely. Private companies hire private security and cannot hire the military. In some energy entities, for example nuclear power plants, military personnel might be used for protection, but their presence would have to be regulated by the government. Their presence would be because of the presence of radio-active material and the scale of the harm that could be done by it. Important shipping channels, like Suez and Panama, might also get national military protection.

When the military is used for protecting critical energy infrastructure, it is on the national or international level. As Rühle and Grubliauskas have indicated, NATO can ensure safe shipping routes for energy shipments in order to maintain stable international energy markets (2012). NATO can be a facilitator in protecting critical energy infrastructure for NATO-members and partner countries. Also, in times of conflict the military can be used to protect energy infrastructure vital for warfare (in the past the presence of functioning oil refineries and oil fields have played a crucial role in the outcome of war). It is important that the military knows how to protect energy infrastructure and where the bottlenecks are. For national security reasons the military might be included into the discussion of critical energy infrastructure identification and protection, but in peacetime the need for military inclusion in national critical energy infrastructure identification and protection is absent.

BIBLIOGRAPHY

Amber Grid. (2014). Actual gas flow. Retrieved from Amber Grid: https://www.ambergrid.lt/en/

Amin, M. (2005). Scanning the technology: Energy infrastructure defense systems. Proceedings of the IEEE 93, issue 5, 861-875.

Ang, B., Choong, W., & Ng, T. (2015). A framework for evaluating Singapore's energy security. Applied Energy 148, 314–325.

Assaf, D. (2008). Models of critical information infrastructure protection. International Journal of Critical Infrastructure Protection 1, 6-14.

Augutis, J., Martišauskas, L., & Krikštolaitis, R. (2015). Energy mix optimization from an energy security perspective. Energy Conversion and Management 90, 300-314.

Bronk, C. (2015). Two securities: How contemporary cyber geopolitics impacts critical infrastructure protection. International Journal of Critical Infrastructure Protection 8, 24-26.

Cazorla, L., Alcaraz, C., & Lopez, J. (2015). Awareness and reaction strategies for critical infrastructure protection . Computers & Electrical Engineering 47, 299–317.

Checchi, A., Behrens, A., & Egenhofer, C. (2009). Long-Term Energy Security Risks for Europe: A Sector-Specific Approach. CEPS Working Documents No. 309. critical. (2011). American Heritage Dictionary of the English Language. Retrieved February 20, 2016, from http://www.thefreedictionary.com/critical

DHS. (n.d.). Critical Infrastructure Security. Retrieved from Department of Homeland Security: http://www.dhs.gov/topic/critical-infrastructure-security

energy. (n.d.). Collins English Dictionary – Complete and Unabridged. Retrieved February 20, 2016, from http://www.thefreedictionary.com/energy

Englefield, C. (2014). Radioactive source security: Why do we not yet have a global protection system? Nuclear Engineering and Technology 46, issue 4, 461–466.

European Commission. (2016, February 11). Protection of critical infrastructure. Retrieved from European Commission: http://ec.europa.eu/energy/en/topics/infrastructure/protection-criticalinfrastructure

European Parliament. (2010, October 20). Regulation (EU) No 994/2010 concerning measures to safeguard security of gas supply and repealing Council Directive. Brussels.

European Union. (2008). The Council of the European Union, Council Directive 2008/114/EC of 8 December 2008. Official Journal of the European Union.

Farrell, A. E., Zerriffi, H., & Dowlatabadi, H. (2004). Energy infrastructure and security. Annual Review of Environment and Resources 29, 421-469.

Gazprom. (2017). Yamal. Retrieved from Gazprom: http://www.gazprom.com/about/production/projects/pipelines/active/yamal-evropa/

Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. International Journal of Critical Infrastructure Protection 10, 3-17.

Giannopoulos, G., Filippini, R., & Schimmer, M. (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. JRC Technical Notes, 1-53.
Gupta, E. (2008). Oil vulnerability index of oil-importing countries. Energy Policy 36, 1195–1211.

Hayashi, M., & Hughes, L. (2013). The Fukushima nuclear accident and its effect on global energy security. Energy Policy 59, 102-111.

Hemme, K. (2014). Critical Infrastructure Protection. El Paso: University of Texas.

Homeland Security. (2016, January 8). What Is Critical Infrastructure? Retrieved from

Homeland Security: http://www.dhs.gov/what-critical-infrastructure

Homeland Security. (2017, October 3). Critical Infrastructure Sectors. Retrieved from

Homeland Security: https://www.dhs.gov/critical-infrastructure-sectors

Hughes, L. (2012). A generic framework for the description and analysis of energy security in an energy system. Energy Policy 42, 221–231.

Hughes, L. (2015). The effects of event occurrence and duration on resilience and adaptation in energy systems. Energy 84, 443-454.

Hughes, L., de Jong, M., & Wang, X. Q. (2016). A generic method for analyzing the risks to energy systems. Applied Energy 180, 895-908.

Hull, R., Belluck, D., & Lipchin, C. (2006). A framework for multi-criteria decision making with special reference to critical infrastructure: Policy and risk management working group summary and recommendations. NATO Security through Science, 355-369.

Hutchison, M., Waage, F., & Bennett, D. (2016). Cyber Resiliency: Bridging a Cyber Capability Gap in 2025 . Small Wars Journal.

IEA. (2015). World Energy Outlook 2015. Paris: International Energy Agency.

Ikeonu, I. (2014). Infrastructure services under regional trade agreements. Multi-year Expert Meeting on Trade, Services and Development. Geneva: UNCTAD. infrastructure. (2011). The American Heritage Dictionary of the English Language. Boston, MA.: Houghton Mifflin Company. Retrieved February 20, 2016, from http://www.thefreedictionary.com/infrastructure

infrastructure. (2014). Collins English Dictionary – Complete and Unabridged. Retrieved February 20, 2016, from http://www.thefreedictionary.com/infrastructure

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences 80, issue 5, 973–993.

Jouini, M., Rabai, L. B., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science 32, 489 – 496.

Jun, E., Kim, W., & Chang, S. H. (2009). The analysis of security cost for different energy sources. Applied Energy 86, 1894–1901.
Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack. Strategic Insights 10, issue 1, 15-25.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. Technological Forecasting & Social Change 103, 21–33.

Lauge, A., Hernantes, J., & Sarriegi, J. M. (2014). Critical Infrastructure dependencies: A holostic dynamic and quantitative approach. International Journal of Critical Infrastructure Protection 8, 16-23.

Li, H., Rosenwald, G. W., Jung, J., & Liu, C.-C. (2005). Strategic Power Infrastructure Defense. Proceedings of the IEEE 93, issue 5, 918-933.

Liu, D., Wang, X., & Camp, J. (2008). Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection 1, 75-80.

Lynn, J. A. (1994). Feeding Mars: Logistics in Western Warfare From the Middle Ages to the Present. Basic Books.

Malanima, P. (2010). The Path Towards the Modern Economy - The Role of Energy. Rivista di Politica Economica, 1-30. Retrieved March 2, 2016, from http://www.paolomalanima.it/default_file/Page477.htm

Malanima, P. (2013). Energy Consumption in the Roman World. In W. Harris (Ed.), The An-

cient Mediterranean Environment between Science and History (pp. 13-36).
Retrieved March 2, 2016, from
http://www.paolomalanima.it/default_file/Page477.htm

Marrero, G. A., Puch, L. A., & Ramos-Real, F. J. (2015). Mean-variance portfolio methods for energy policy risk management. International Review of Economics and Finance 40, 246–264.

Matsumoto, K., & Andriosopoulos, K. (2016). Energy security in East Asia under climate mitigation scenarios in the 21st century. Omega 59, 60–71.

Moteff, J. D. (2012). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service, 1-24.

OSCE. (2013). Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Vienna: Organization for Security and Co-operation in Europe.

Parfomak, P. W. (2008). Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options. CRS Report for Congress.

Ranjan, A., & Hughes, L. (2014, July). Energy security and the diversity of energy flows in an energy system. Energy, 73, pp. 137-144. doi:10.1016/j.energy.2014.05.108

Robles, R. J., Choi, n.-k., Cho, E.-s., Kim, S.-s., Park, G.-c., & Lee, J.-H. (n.d.). Common Threats and Vulnerabilities of Critical Infrastructures. International Journal of Control and Automation, 17-22.

Rosas-Casals, M., Valverde, S., & Sole, R. V. (2006). Topological Vulnerability of the European Power Grid under Errors and Attacks. Santa Fe Institute.

Rühle, M., & Grubliauskas, J. (2012). NATO and Energy Security: Infrastructure Protection and Beyond. Turkish Policy Quartely 11, issue 3, 65-73.

Sanchez, R. (2014, March 17). New York explosion exposes nation's aging and dangerous gas mains. Retrieved from CNN: http://edition.cnn.com/2014/03/15/us/aging-gasinfrastructure/

Santiago, J., & Magallon, D. (2009). Critical Path Method. Stanford.

system. (2011). American Heritage Dictionary of the English Language. Retrieved February 20, 2016, from http://www.thefreedictionary.com/system

Ulbrich, P., Hoffmann, M., Kapitza, R., Lohmann, D., Schmid, R., & Schröder-Preikschat, W. (2012). Eliminating Single Points of Failure in Software-Based Redundancy. EDCC.

Vasenin, V. A. (2013). Critical Energy Infrastructure: Cyberterrorism Threats and Means of Protection. Journal of Software Engineering and Applications 6, 23-33.

Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges . Computer Networks 57, issue 5, 1344–1371.
Weisser, H. (2007). The security of gas supply—a critical issue for Europe? Energy Policy 35, 1–5.

Wu, G., Wei, Y.-M., & Liu, L.-C. (2007). An empirical analysis of the risk of crude oil imports in China using improved portfolio approach. Energy Policy 35, issue 8, 4190–4199.

Yusta, J. M., Correa, G. J., & Lacal-Arantegui, R. (2011). Methodologies and application for critical infrastructure protection: State-of-the-art. Energy Policy 39, 6100-6119.

Zhang, H.-Y., Ji, Q., & Fan, Y. (2013). An evaluation framework for oil import security based on the supply chain with a case study focused on China. Energy Economics 38, 87–95.

Notes

NATO Energy Security Centre of Excellence

Šilo g. 5A (K-22), LT-10322 Vilnius,
Lithuania
Phone: +370 5 203 26 86
Fax: +370 706 71010
Email: info@enseccoe.org
www.enseccoe.org

ISSN 2335-7975