Energy Security: Operational Highlights

No 10 • 2016

Contents

Editorial

Col. Gintaras Bagdonas
Director
NATO Energy Security Centre of Excellence

The threats to critical energy infrastructure are at the centre of this issue of 'Energy Security: Operational Highlights' with a particular focus on the attacks coming from the cyber space and from violent non-state actors such as so called "Islamic State", or DAESH. Furthermore, in order to reduce the risks related to the field of energy on which its societies and its operations depend, NATO works towards significantly improving the energy efficiency of the military and valuably contributes to this dimension of energy security.

The relevance of these topics for the international community at the present time is behind the choice to include the following four articles in the current issue of this journal.

Ms. Anna Bulakh, Ms. Piret Pernik and Mr. Emmet Tuohy discuss cyber attacks on critical energy infrastructure with particular emphasis on the supervisory control and data acquisition (SCADA) systems, which are used by several kinds of energy industries. In so doing, they focus on the case of Estonia, which has succeeded in developing effective patterns of public-private sector information sharing about attacks and vulnerabilities in information infrastructure. At the same time, they propose potential means to reduce the risks coming from cyber attacks to critical energy infrastructure. Maj. Remigijus Žilinskas and Mr. Lukas Trakimavičius also discuss cyber attacks to energy industries, but their main focus, after having presented concrete cases of attacks on SCADA systems, is the contribution of the Alliance to the cyber and energy security of its member states. In particular, they draw the attention to NATO's Enhanced Cyber Defence Policy and to the NATO-Istanbul Cooperation initiative Table-Top Exercise on the protection of critical energy infrastructure that was organized and hosted by NATO Energy Security Centre of Excellence. Maj. Remigijus Žilinskas and Mr. Ján Čiampor analyse asymmetric warfare in the context of energy infrastructure. They focus their discussion on violent non-state actors by analysing their military activities and attacks on energy infrastructure. In this context, they investigate the case of DAESH as a relevant case for understanding asymmetric warfare.

Finally, Dr. Sigita Kavaliūnaitė, Dr. Dainius Genys and Dr. Tiziana Melchiorre adopt a comprehensive sociological approach towards NATO's energy security. They analyse the measures adopted by the Alliance to ensure energy security by trying to define its role in the field. In order to do this, they take into consideration sociologist Ronald Inglehart's approach with a focus on his definition of materialist and postmaterialist values, which the authors use to demonstrate that in the 21th century the measures adopted by NATO to ensure energy security are based on a synthesis of these two sets of values.

Estonia's Developing Level Playing Field for Critical Energy Infrastructure Protectors - **a Model for Broader Scale Platforms?**

Ms Anna Bulakh, Mr. Emmet Tuohy, and Ms. Piret Pernik, International Centre for Defence and Security, Estonia

In this paper, the authors outline how critical energy infrastructure (CEI) represents an attractive and vulnerable target for cyber attacks. They begin by addressing possibilities such as zero-day attacks, strikes against the SCADA (supervisory control and data acquisition) systems used by industrial facilities and key infrastructure such as oil pipelines and electrical power generating plants, and risks posed by the increased use of smart grids. Focusing on the case of Estonia, a small and digitally-integrated Baltic country, they also suggest some potential means by which these threats can be mitigated, notably more effective intra- and inter-governmental cooperation and increased use of public-private partnerships.

INTERCONNECTIVITY AND DEPENDENCE ON INFORMATION TECHNOLOGY AS FACTORS OF VULNERABILITY

In recent years, the European Union—together with its member states—have considerably strengthened their pursuit of energy security. These efforts demonstrate the increased importance they place on ensuring a stable supply of energy resources to the final consumer. In order to guarantee reliable energy deliveries and route diversification, the EU in particular has pushed for the development of interconnectivity of energy networks. In 2008 the European Commission issued a Proposal for a Council decision on a Critical Infrastructure Warning Information Network (CIWIN). The aim of the proposal was to assist "the Member States and the European Commission to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of Critical Infrastructure Protection (CIP)". [1]

Ms. Anna Bulakh, International Centre for Defence and Security, Tallinn

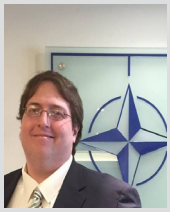
Anna Bulakh is research fellow at the International Centre for Defence and Security (ICDS), Estonia. Her research focuses on energy security, and regional security in the area of the EU's Eastern Partnership, particularly in Ukraine. She extensively writes and comments on the issues of the EU's single energy market, precisely on the energy infrastructure development across the EU and the possibility to bring new sources of energy supplies to Europe. In her research on security risks and conflicts in the EU's Eastern Partnership area, she focuses on energy and its infrastructure as an internal threat and vulnerability exploited by an aggressor. Previously, she conducted research at the Prague Security Studies Institute, Czech Republic and has worked at the ICDS since 2013.

[1] European Commission, Critical Infrastructure Warning Information Network, available at http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

While Europe has succeeded in reducing the risk posed by conventional threats to its energy supplies — both natural and man-made alike — there is a new threat to which the sector is altogether more vulnerable: the one posed by cyber warfare. To put it simply, there are now security concerns at each step along the energy supply chain – from extraction to production, transportation, and final customer delivery – because of the significantly increased reliance, even dependence, on information technology in the sector, combined with the exponential growth in the power and sophistication of cyber attacks.

The largest concern to the security of critical energy infrastructure (CEI)-defined in this paper as the systems that enable the delivery of electricity, gas, and oil from producer to consumer - comes from the interoperability of components within the energy supply chain, with the greatest exposure to new threats coming when technological systems are repaired or improved. This occurs because CEI is commonly monitored and operated by industrial control systems, which rely on standard embedded systems platforms. According to a recent report of the European Union Agency for Network and Information Security (ENISA), the vulnerability of industrial control systems are "more and more like [those of] consumer PCs"; that is, they are "used everywhere and involve a considerable amount of software, often outdated and unpatched".[2]

Energy transmission infrastructure is automated by the use of remotely-controlled SCADA (supervisory control and data acquisition) systems. A SCADA system is an assembly of interconnected equipment for monitoring and controlling physical processes in industrial environments, and is used to automate geographically distributed processes in electricity generation and distribution as well as oil and natural gas refining and pipeline management.[3] Modern SCADA systems use standard interfaces and "off-the-shelf" components such as Unix or Windows operating systems. On the one hand, this has produced considerable improvements in interconnection and efficiency, while on the other one it has significantly increased their vulnerability to the same types of attacks used against Unix and Windows-based systems in other settings.[4] The reliance of these control systems on such technology—as well as the critical real-world importance of power plants, pipelines, and storage facilities that they control—make CEI a very attractive target for cyber attacks.



Mr. Emmet Tuohy, International Centre for Defence and Security, Tallinn

Emmet Tuohy is non-resident research fellow on energy security and the Eastern Partnership countries at the independent research institute of the Estonian Ministry of Defence since 2012. Tuohy is regularly called upon to brief members of parliament and other government and diplomatic officials. He has served as Estonia's representative to the NATO STO Working Group on Energy Security, and delivers lectures and conference presentations throughout Europe. Tuohy has been associate director of Hudson Institute's Center for Eurasian Policy. He was previously awarded a Fulbright research grant to Ukraine and has been visiting researcher at the Institute for Urban History in Lviv. Tuohy has graduated from the Georgetown University School of Foreign Service in Washington, DC.

[2] Pauna, Adrian, Malinos, Konstantinos, Lakka, Matina, et al, Can We Learn from SCADA Security Incidents? (Brussels: ENISA, October 9, 2013), available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

[3] Organization for Security and Cooperation in Europe, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace (Vienna: OSCE, 2013)

[4] Umbach, Frank, Critical Energy Infrastructure Protection in the Electricity and Gas Industries – Coping with Cyber Threats to Energy Control Centers (Berlin: ISPSW, 2010)

ZERO-DAY ATTACKS

US researchers Adam Crain and Chris Strunk have revealed new information identifying a number of areas susceptible to "zero-day attacks" (i.e. attacks exploiting previously unknown vulnerabilities) in industrial control software. Considering that most current attention (however insufficient as it may be) to the security of power systems focuses on issues stemming from their use of IP (i.e. via the open Internet) links, "offline" serial and network communications between servers and substations have been overlooked. And yet, according to Crain and Strunk, it is easier to break a power system via devices of serial communication, which does not require bypassing the layers of firewalls that an attack against an IP network would.[5] The vulnerabilities that Crain and Strunk highlight could allow an attacker to send a master server into an unproductive loop (thereby taking it offline) or block operators from monitoring and controlling operations (thereby virtually ensuring disruptions in energy transmission). Another scenario foresees "remote code-injection into a server", which would enable an attacker to cause power blackouts by opening and closing breakers at substations.[6]

VARIETY OF THREATS REQUIRES BROADER LEVEL RESPONSE

As if this was not enough to be concerned about, there is a number of other challenges to keeping CEI secure. In particular, the emergence as a common tool in cyber warfare of the so-called dormant viruses, which can be planted in a system remotely and lie unnoticed for long periods of time before being activated, raises the specter that they could be deployed against CEI, virtually handing over the infrastructure to attackers. Another vulnerability, highlighted last year by the US National Institute of Standards and Technology (NIST), is raised by the more widespread use of "smart grids". Such electricity grids require the accessing of information dozens of times a day from millions of smart meter "nodes" in business, government, and residential installations.[7] Every single one of these millions of nodes could serve as an entry point to the grid for a hacker determined to cause harm.

In light of all these threats, the response must clearly be on a level broader than that of an individual company or even of a nation-state. Even though the EU's recommendations evolved in sophistication

Ms. Piret Pernik, International Centre for Defence and Security, Tallinn

Piret Pernik is research fellow at the International Centre for Defence and Security. Her research focuses on strategic issues relevant to cyber security, including the analysis of global developments, strategies and policies pursued by nation states and international organisations. She recommends how to shape Estonia's efforts on cyber security and on how to introduce the Estonian experience internationally. She also coordinates cyber security related cooperation with other relevant domestic and international actors. She has worked at the Policy Planning Department of the Estonian Ministry of Defence and served as an adviser to the National Defence Committee of the Riigikogu (Estonian Parliament). She has lectured on international relations in several Estonian universities, and has carried out sociological research projects.

[5] Ashford, Warwick, "US Researchers Find 25 Security Vulnerabilities in SCADA Systems", Computer Weekly, October 18, 2013, available at http://www.computerweekly.com/news/2240207488/US-researchers-find-25-security-vulnerabilities-in-SCADA-systems

[6] Zetter, Kim, "Researchers Uncover Holes That Open Power Stations to Hacking" Wired, October 16, 2013, available at: http://www.wired.com/threatlevel/2013/10/ics/

[7] Chabrow, Eric, "Smart Grid's Unique Security Challege", GovInfo Security, July 2012, available at: http://www.govinfosecurity.com/interviews/smart-grids-unique-security-challenge-i-1603

and effectiveness in series of documents[8] on critical infrastructure protection, they were able to foster neither effective state-to-state cooperation nor perhaps the most important tool of all in combating threats to CEI: public-private partnership (PPPs).[9]

PPPS - A FRAMEWORK FOR BROADER LEVEL RESPONSE

The concept of "partnership" is crucial in developing a framework for the effective protection of critical energy infrastructure on a broader EU level. This is especially true when one takes into consideration the fact that greater interdependency, despite its clear benefits in a variety of areas, still brings with it greater risk, both that an attack might spread to other systems, and that disruptions in one area might have a supply impact on another.

In order to foster the needed PPPs, the European Commission created concrete efforts, notably a secure information and communication system known as CIWIN (the Critical Infrastructure Warning Information Network), which allows government, private sector, and nonprofit experts to exchange information and discuss best practices. While studies and expertise can be exchanged on a voluntary basis using the CIWIN platform, there is a lower degree of openness to reveal information and data on specific attacks on the part of the private sector.

This is not to say that owners and operators of energy networks in Europe are at cross-purposes. By contrast, they all do share the same goal of secure operation, a goal whose accomplishment requires "openness and equal sharing of information between operators, owners, and state authorities."[10] Nevertheless, there is a legitimate concern among private sector entities about revealing current vulnerabilities or past attacks: if such information was made public, the resulting negative publicity could result in a decreased market share or a decline in stock price. Accordingly, one limitation of a purely voluntary as opposed to regulatory approach to information sharing is that private-sector operators face rational incentives against full disclosure of the risks and outcomes of cyberattacks.

EFFECTIVE PATTERNS OF INFORMATION SHARING: THE CASE OF ESTONIA

In recent years, Estonia has succeeded in breaking new ground in developing effective patterns of public-private sector information sharing about attacks and vulnerabilities in information infrastructure. Accordingly, the country could serve as a model for developing a framework of PPP cooperation on information infrastructure—specifically in the energy sector—across Europe.

Thanks in part to its unique comparative advantage in (and dependence on) information technology, and in part to its experiences in responding to what is arguably the world's first major cyber attack against an entire country in 2007, Estonia has pushed its government to adopt clearly defined information security standards.

Systematically, the government has built on its success in raising awareness in the public sector by reaching out to private sector as well. Stakeholders from across government agencies as well as critical-

[8] The need for a response on a broader European level to increase the protection of critical infrastructure was acknowledged by the EU in 2004, when the Commission adopted a communiqué on critical infrastructure protection in the fight against terrorism and a Green Paper on a European program for critical infrastructure protection. The main principles and instruments of implementation were defined in the European Program for Critical Infrastructure Protection (ENCIP) adopted by the European Council in December 2006. However, none of these documents were very detailed in nature. It was not until 2008 that the first step-by-step approach to developing a common understanding and framework for protecting critical infrastructure was set forth in a European Council directive.

[9] Umbach, Critical Energy Infrastructure Protection, ibid.

[10] European Commission, Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (Brussels: EC, November 2012)

infrastructure operators and other private sector companies were involved in the process of drafting and implementing the country's first National Cyber Security Strategy (2008-13).

Among many successful examples of private-public partnerships in Estonia are: the participation of telecommunication company representatives in the Cyber Security Council (an advisory board to the National Security Council) as well as the bringing together of IT managers and risk specialists from the private and public sectors within the framework of the Protection of Critical Infrastructure Committee, established in 2011. These examples were reflected elsewhere in the EU in 2012, when business leaders were invited by the UK government on a similar basis to work together on updating the UK's national Cyber Security Strategy.

It is also worth mentioning one further example of a working model of private-public cooperation in cyber security on a voluntary (and individual) basis: the Cyber Defence Unit of the National Defence League (Estonia's reserve military forces), which is made up of IT and cyber related experts on leave from their regular jobs for their regular annual period of active military service.[11] This unit has recently served as the model for the Cyber Security Corps—a rapid response team comprised of volunteers from government, education and business sectors related to cyber security—implemented by the Michigan National Guard.[12]

MOVING FORWARD: PPP AS A SOURCE OF STABILITY IN A WORLD OF INSTABILITY

The status quo of insecurity regarding cyber threats toward critical energy infrastructure demands a new level of transparency beyond the intra-organizational level. Instead, it is of national and international strategic importance that corporate leaders and shareholders agree to cooperate and put their vulnerabilities on the table. The private sector has to understand that the price of "keeping silent and doing nothing to counter cyber threats is far greater than the cost of having a strategic security framework in place."[13] Moreover, public-private cooperation is not a unidirectional pathway of commands from the latter to the former, but a win-win process that goes in both directions. For companies, it is of great interest to get early information on government strategies, new mechanisms and standards, legal amendments, and so on, all of which affect their corporate bottom lines—to say nothing of the strategic value of being present in, and helping to shape, the policymaking process. Of course, this latter possibility—namely, of the extent to which companies can directly influence decision-making—raises other issues about distorted incentives for corporations to participate in the process. Nonetheless, on the whole, when companies are motivated—by the use of careful incentives by government—to invest their resources into developing better security measures, they benefit both themselves and national security at the same time.

TESTED MODELS AS GUIDELINES FOR IMPROVING INFORMATION SHARING PLATFORMS

As noted above, in the modern era, CEI depends completely on data transmitted by various types of information technology, all of which are vulnerable to attacks that create risks of energy supply disruption. Estonia and countries like the UK and the

[11] Pernik, Piret, Tuohy, Emmet, Cyber Space in Estonia: Greater Security, Greater Challenges (Tallinn:, ICDS, August 2013)
[12] Chabrow, Eric, "State Creates 'Cyber National Guard'", Data Breach Today, November 7, 2013, available at: http://www.databreachtoday.com/interviews/state-creates-cyber-national-guard-i-2099
[13] Brown, Mark, "Last Word: Action Station", SC Magazine, August 2013, available at http://www.scmagazineuk.com/last-word-action-stations/article/308570/

US have demonstrated an effective model for bringing private and public sector players from different sectors and "teams" onto the same playing field. This approach has already given important results. It can serve as a model role for other EU members to make constructive use of existing but underutilized platforms for information sharing such as CIWIN. In such a way, players from both sectors in all European countries can help develop a true level playing field at the European level, ensuring security across a far greater area than ever before—and just in time before the next attack strikes.

REFERENCES

Ashford, Warwick, "US Researchers Find 25 Security Vulnerabilities in SCADA Systems", Computer Weekly, October 18, 2013;

Brown, Mark, "Last Word: Action Station", SC Magazine, August 2013;

Chabrow, Eric, "Smart Grid's Unique Security Challenge", GovInfo Security, July 2012;

European Commission, Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (Brussels: EC, November 2012);

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

Pauna, Adrian, Malinos, Konstantinos, Lakka, Matina, et al, Can We Learn from SCADA Security Incidents?(Brussels: ENISA, October 9, 2013);

Pernik, Piret, Tuohy, Emmet, Cyber Space in Estonia: Greater Security, Greater Challenges (Tallinn:, ICDS, August 2013);

Zetter, Kim, "Researchers Uncover Holes That Open Power Stations to Hacking" Wired, October 16, 2013;

Umbach, Frank, Critical Energy Infrastructure Protection in the Electricity and Gas Industries – Coping with Cyber Threats to Energy Control Centers (Berlin: ISPSW, 2010);

www.computerweekly.com;

www.enisa.europa.eu;

www.govinfosecurity.com;

www.scmagazineuk.com;

www.wired.com

The Perils of Cyber-attacks **Against the Energy Industry**

Maj. Remigijus Žilinskas and Mr. Lukas Trakimavičius

This article discusses the cyber attacks on the energy industry, which have become increasingly sophisticated and dangerous over the last years. To this aim, some relevant examples of cyber attacks to the Supervisory Control and Data Acquisition (SCADA) systems, which are essential for the well functioning of energy companies, are illustrated. Additionally, the measures and the policies adopted by the North Atlantic Treaty Organization (NATO) are analysed. In this context, the NATO Enhanced Cyber Defence Policy and the NATO-Istanbul Cooperation initiative (ICI) Table-Top Exercise (TTX) on the protection of critical energy infrastructure organized by NATO Energy Security Centre of Excellent (ENSEC COE) are particularly meaningful. Therefore, this article clearly shows how serious cyber attacks on the energy industry are nowadays and how important protection and preparedness are for NATO member states.

INTRODUCTION

Over the past few years the Baltic Sea region countries have been developing new projects related to Liquefied Natural Gas (LNG) terminals to improve their energy security. The LNG terminal in Klaipėda (Lithuania) started working in December 2014[1], whereas the LNG terminal in Świnoujście (Poland) is planned to be ready for commercial use in May 2016[2]. Estonia and Finland also intend to build LNG importing infrastructure in the nearest future.[3] The construction of new LNG terminals will benefit these countries by increasing the diversification of their gas supplies. However, it will also create security threats in the region.

In the near future, cyber-attacks on critical energy infrastructure (which the governmental agencies define as assets or systems that contribute to the production, generation, storing, transmission, or distribution of energy and that are essential for the functioning of the society and of the economy) is one of the main threats to the energy industry in the Baltic Sea region. Throughout time, they have become more sophisticated and dangerous. Indeed, they can cause not only temporary operational disturbances, but also great financial harm and physical damage[4].

This article discusses the cyber-attacks against the energy sector by highlighting the

Maj. Remigijus Žilinskas, NATO Energy Security Centre of Excellence, Vilnius

Maj. Remigijus Žilinskas (OF-3, LTU A) is Subject Matter Expert at the NATO Energy Security Centre of Excellence, Vilnius. He graduated from the Lithuanian Military Academy in 2000. Besides military education and training, he has masters' degrees in public administration and international relations from the Lithuanian Law University and the International Relations and Political Science Institute in Vilnius. He also attended a postgraduate course on defence and security at the politico-strategic level at the European Institute of International Relations (IERI) in Brussels, Belgium. He currently is a Ph.D. student at the Gen. Jonas Zemaitis Military Academy of Lithuania and Vytautas Magnus University in Kaunas. His research interests focus on security and defence studies, civil-military relations and public administration.

efforts that NATO is making to counterbalance them. To this aim, this study is divided into two sections. The first one focuses on the attacks on the SCADA systems by providing some relevant examples. The second section analyses the measures and the policies adopted by NATO in the field. In this context, the Enhanced Cyber Defence Policy and the

SCADA'S – THE ACHILLES' HEEL OF THE ENERGY INDUSTRY

Recent years have been marked by a significant proliferation of cyber-attacks against energy companies, which have become increasingly sophisticated both in scope and in scale. When this kind of offensive maneuver against information and communication

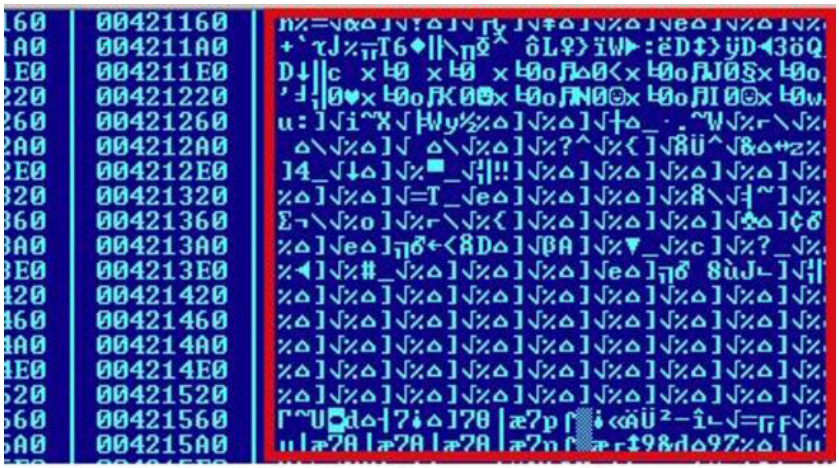


Figure 1. 'Shamoon' malware covers its tracks by crippling infected systems after stealing data
Source: http://www.topnews.in/seculert-shamoon-malware-covers-its-tracks-crippling-infected-systems-after-stealing-data-2364028

NATO-Istanbul Cooperation initiative (ICI) Table-Top Exercise (TTX) on the protection of critical energy infrastructure organized by NATO Energy Security Centre of Excellent are particularly meaningful.

technologies began in the late 1980s, attacks simply aimed to disrupt the operational capabilities of energy companies by crashing their computer software via coordinated barrages of millions of requests. These actions

Mr. Lukas Trakimavičius, Independent Energy & Security Analyst

Lukas Trakimavičius is an independent energy and security analyst whose interests focus on European, Eurasian oil and gas industries, Russian foreign policy and the Post-Soviet region. His work has been featured in books published by the Yale University Press, the Harvard University Press as well as in publications such as The Hill or the World Politics Review. He currently is an MSc student at the London School of Economics and Political Science. Lukas holds a BA from the University of Exeter and has worked as an intern in the Doctrine and Concept Development Division of the NATO Energy Security Centre of Excellence in Vilnius.

[1] Čeponytė, Jurgita, How will Lithuania's LNG terminal work?, in Delfi, September 18, 2014, available at http://en.delfi.lt/lithuania/energy/how-will-lithuanias-lng-terminal-work.d?id=65876624. See also Reuters, Lithuania installs LNG terminal to end dependence on Russian gas, in Mail Online, October 27, 2014, available at http://www.dailymail.co.uk/wires/reuters/article-2809932/Lithuania-installs-LNG-terminal-end-dependence-Russian-gas.html

[2] Radio Poland, Polish LNG terminal in Świnoujście to open May '16, available at http://www.thenews.pl/1/12/Artykul/221380,Polish-LNG-terminal-in-Swinoujscie-to-open-May-16

[3] Martewicz, Maciej, Bujnicki, Piotr, Poland to Get Baltic LNG Terminal on Time as Costs Increase, available at http://www.bloomberg.com/news/articles/2014-08-05/poland-to-get-lng-terminal-on-time-as-costs-discussed-pbg-says.

[4] Butrimas, Vytautas, National Security and International Policy Challenges in a Post Stuxnet World, in Lithuanian Annual Strategic Review, vol. 12, 2013-2014, p.12

Figure 2. Stanlow Oil Refinery

Source: http://www.geograph.org.uk/photo/3667941

were known as distributed denial of service.

Nowadays, the energy industry has been mainly threatened by two types of attacks[5], namely Night Dragon and Shamoon. Night Dragon was a relatively unsophisticated cyber espionage intrusion campaign, used by Chinese hackers to steal sensitive intellectual property from energy (oil, gas and petrochemical) companies employing technical attacks on their public-facing.[7]

Shamoon is the powerful computer worm that in 2012 managed to infect and delete the content of around 30,000 hard drives of Aramco, the Saudi Arabian state-owned oil and gas company.[8]

Although Night Dragon or Shamoon can seriously damage energy companies, the grea-

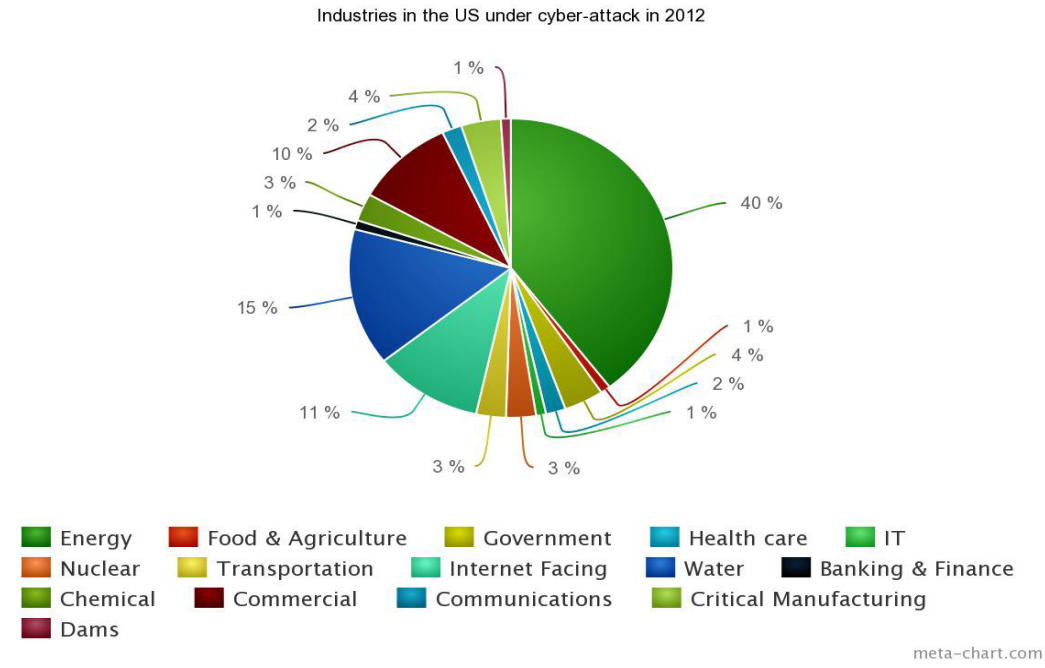


Figure 3. Industries in the US under cyber-attack in 2012
Source: https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2012.pdf

[5] North Atlantic Treaty Organization, Cyber Timeline, in NATO Review Magazine, available at http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

[6] In this context, it is worth mentioning the Denial of Service (DDoS) attacks, which are another type of cyber hostility. They overload and effectively shut down companies' servers

[7] Kirk, Jeremy, 'Night Dragon' attacks from China strike energy companies, available at http://www.networkworld.com/article/2199766/network-security/-night-dragon--attacks-from-china-strike-energy-companies.html

[8] Clayton, Blake, Segal, Adam, Addressing Cyber Threats to Oil and Gas Suppliers, available at http://www.cfr.org/content/publications/attachments/Energy_Brief_Clayton_Segal.pdf. See also Bronk, Christopher Tikk-Ringas, Eneken, The Cyber Attack on Saudi Aramco, available at http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

test threats to critical energy infrastructure come from the cyber-attacks aiming at causing physical damage via the SCADA systems. First introduced in the 1960s, the SCADA systems became widely used to monitor and control various plants in several kinds of industries such as telecommunications, energy, and oil and gas refining. These systems have hugely improved the efficiency of the supervision processes in these plants as means to be hijacked. Consequently, performance, reliability and flexibility of SCADA systems are robust, while their security is often weak.

The most notorious example of an attack against a SCADA system in the energy industry was Stuxnet, an extremely sophisticated internet worm, allegedly created by the United States (U.S.) and Israel. Stuxnet managed

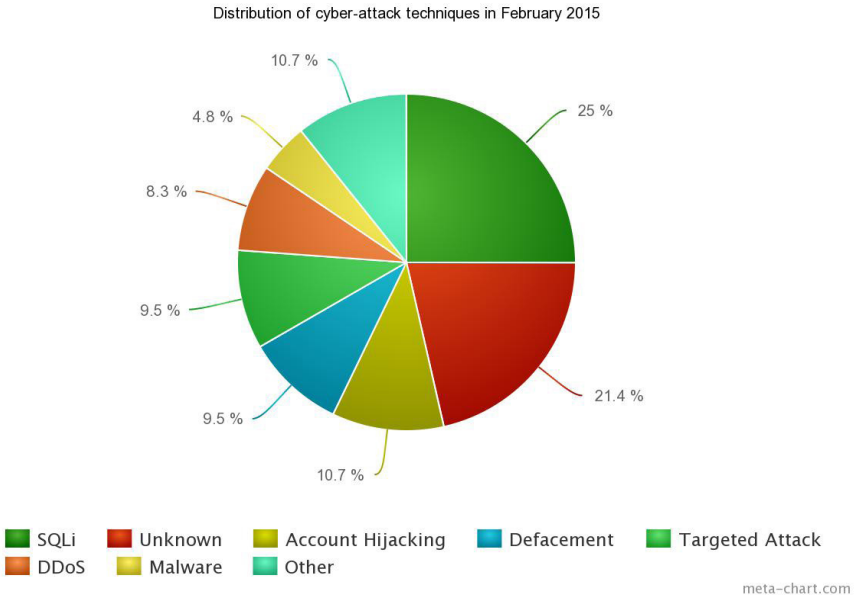


Figure 4. Distribution of cyber-attack techniques in February 2015
Source: http://www.hackmageddon.com/2015/03/09/february-2015-cyber-attacks-statistics/

they are used to monitor temperature, pressure, valve position, tank levels, actuators and other equipment.

However, the main problem with these systems is security because they were initially conceived to maximize functionality, with little attention paid to security. Some SCADA systems can be easily reached through internet or within radio range, while some others with a so called 'air gap' (which means that SCADA systems are physically disconnected from the internet) require more improvised to infect the Iranian fuel factory systems in Natanz through USB drivers because of 'air gaps'.[9] The 500-kilobyte internet worm succeeded in infecting 14 industrial sites in Iran, including a uranium-enrichment plant, and in seriously undermining Iran's uranium purification efforts.

According to Ralph Langner[10], "the development of Stuxnet did require nationstate resources – especially for intelligence gathering, infiltration, and most of all for testing".[11] Stuxnet demonstrated that the idea of attacks

[9] Peretti, Kimberly, Slade, Jared, State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction, available at http://www.alston.com/Files/Publication/0470bf82-1589-4200-be02-de03a3aea95b/Presentation/PublicationAttachment/35553890-a8a6-4eb5-b7bf-e6397539d409/14-183-State-Sponsored-Cybercrime.pdf
[10] Ralph Langner is one of the responsible people for deciphering the code of Stuxnet.
[11] Langner, Ralph, To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, available at http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

emanating from the cyber space doesn't belong to the realm of science fiction anymore. It also made clear that nation states can seriously undermine the energy security of energy companies. Nevertheless, in spite of the magnitude of Stuxnet, it is rather unlikely that a nation could use similar worms[12] against several countries at the same time. [13] The reason is that most hacker groups do not possess the necessary capabilities to create such malicious programs.

Although internet worms such as Stuxnet are very difficult to create, a nation state or a cyber-terrorist group could be able to devastate the energy sector of an entire country with a single laptop thanks to the fact that computer equipment has become affordable in recent years. Indeed, if the intruder has the technological know-how for infiltrating into a SCADA system of a gas or oil pipeline, it could generate false data and provoke a massive explosion. Consequently, the intruder could cause malfunction or even self-destruction of pumping stations, catalytic crackers, fast-spinning centrifuges or other kinds of equipment.

Moreover, SCADA systems can also be affected by the so called 'logic bombs'.[14] A clear example is the Siberian pipeline sabotage in 1982, when the US sold the Soviet Union a chip triggering a very large explosion in the Siberian pipeline that was supposed to bring natural gas to the centre of the Union.[15] The 'logic bombs' against pipelines are extremely dangerous for the safety of states, especially of those relying on only one pipeline like Latvia. As Economics Minister Vjačeslavs Dombrovskis said, "Latvia currently stands on an 'energy island'; we have access to only one gas pipeline, and a regional interconnection is the only feasible solution, which will ensure energy independence".[16]

HOW CAN NATO CONTRIBUTE TO THE CYBER AND ENERGY SECURITY OF ITS MEMBER STATES?

Protecting Critical Energy Infrastructure (CEI) from cyber-attacks is very difficult. Indeed, they can be defined as 'black swans', namely "events or occurrences that deviate beyond what is normally expected of a situation and that would be extremely difficult to predict".[17] Therefore, the most feasible strategy for NATO to counteract cyber attacks and to keep abreast with the rapidly changing threat landscape is to adopt effective preventive measures. In order to do so, NATO has adopted a new Enhanced Cyber Defence Policy, which was endorsed by Allied defence ministers in June 2014. NATO's policy "establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communication systems owned and operated by the Alliance".[18] The policy also defines the necessary procedures for assistance to Allied nations, and the integration of cyber defence into operational planning (including civil emergency planning). It outlines ways to take awareness, education, training and

[12] In addition to Stuxnet, state-funded malwares like Havex, Sandworm, Black Energy, Regin and Cleaver also exist.
[13] Butrimas, Vytautas, Ypatingos svarbos infrastruktūrų kibernetinis saugumas, http://www.lsta.lt/files/seminarai/2015-01-29%20LMA_seminaras/03_Ypatingos%20svarbos%20infrastrukturu%20kibernetinis%20saugumas.pdf
[14] "Logic bombs are small programs or sections of a program triggered by some event such as a certain date or time, a certain percentage of disk space filled, the removal of a file, and so on. For example, a programmer could establish a logic bomb to delete critical sections of code if she is terminated from the company. Logic bombs are most commonly installed by insiders with access to the system".
Technology Institute, Security laboratory, available at http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door
[15] Since the late 1960s, the US technology (especially the computer one) development was envied by the Soviet Union that lacked the industrial mindshare to match the US in innovation and research. Therefore, the Soviet Union decided to purchase and copy the US technology, which allowed to maintain near parity by avoiding the exorbitant costs of development.
Shein, Rob, Zero-Day Exploit:– Countdown to Darkness, Rockland: Syngress Publishing Inc., 2004, p. 3
[16] En, Elta, Gas pipeline via Poland, Lithuania will end Latvia's energy dependence, in Lithuania Tribune, 10 October 2014, available at http://en.delfi.lt/nordic-baltic/gas-pipeline-via-poland-lithuania-will-end-latvias-energy-dependence.d?id=66079816#ixzz3UgIX5STX
[17] Financial Times, Definition of Black Swan, available at http://lexicon.ft.com/Term?term=black-swan

Figure 5. Klaipėda (LTU) liquefied natural gas floating storage and regasification unit terminal or Klaipėda LNG FSRU (taken by NATO Energy Security Centre of Excellence, Dec 2014)

exercise activities, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations. Finally, it "foresees boosting NATO's cooperation with industry based on information sharing and cooperative supply chain management".[19]

The importance of the Enhanced Cyber Defence Policy is also emphasized in the NATO Wales Summit Declaration of 2015. It stresses the commitment of the Allies to further develop national cyber defence capabilities and to enhance the cyber security of national networks upon which NATO depends for its core tasks with the aim to make the Alliance resilient and fully protected. The Declaration also identifies bilateral and multilateral cooperation as the key to enhance the cyber defence capabilities of the Allies. Therefore, integrating cyber defence into NATO operations and operational and contingency planning, and enhancing information sharing and situational awareness among Allies are major goals to ensure NATO's cyber security.[20]

Additionally, in 2008 seven NATO nations[21] and the Allied Command Transformation established a Cooperative Cyber Defence (CCD) Centre of Excellence (CoE) in Tallinn, Estonia. It is "a NATO-accredited research and training facility dealing with education, consultation, lessons learned, research and development in the field of cyber security".[22] Its mission is "to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation". [23]

It is also worth noting that NATO provides assistance mainly through its Computer Incident Response Capability (NCIRC) Rapid Reaction Team, which is the centre of gravity of the Alliance's fight against cyber

[18] NATO Multimedia Library, Cyberspace security, available at http://www.natolibguides.info/cybersecurity
[19] Ibidem
[20] NATO, Wales Summit Declaration, 2014, available at http://www.nato.int/cps/en/natohq/official_texts_112964.htm
[21] The founding nations of the CCD COE are Estonia, Germany, Italy, Latvia, Lithuania, Slovak Republic and Spain. In November 2015, Greece, Turkey and Finland joined the Centre. CCD COE, History, available at https://ccdcoe.org/history.html
[22] CCD COE, About Cyber Defence Centre, available at https://ccdcoe.org/about-us.html
[23] Ibidem

crime.[24] It was established as a result of the NATO cyber defence policy, which was revised by defence ministers in 2011. The Team is in charge of assisting the member states that ask for help in the event of an attack of national significance.[25]

Furthermore, cyber security is also an area of work of the NATO Energy Security Centre of Excellence (ENSEC COE) in Vilnius, Lithuania. It was established in 2012 and "operates as a widely recognized international military organization with the aim of providing qualified and appropriate expert advice on questions related to operational energy security".[26] Contributing to the request of NATO Emerging Security Challenges Division, the Centre organized and hosted the NATO-Istanbul Cooperation initiative (ICI) Table-Top Exercise (TTX) on the protection of critical energy infrastructure on October 20-23, 2014. The event was open to NATO members as well as to Istanbul Cooperation Initiative (ICI) partner countries. The main aim of the exercise was "to support national authorities in building resilience through improved disaster preparedness, planning, prevention and response, while strengthening their capability to manage potential civil emergencies. Energy security exercises are critical to maintaining and strengthening relationships between business sectors, national government institutions and international organisations".[27]

The exercise focused on several scenarios involving the security of critical energy infrastructure and including Liquefied Natural Gas (LNG) shipment incidents, cyber risks for energy-related port infrastructure, and the information domain. Lectures on the energy security awareness and on the protection of critical energy infrastructure were also organized.[28] This exercise is a perfect example of the cooperation of different nations and entities in order to prepare for eventual cyber attacks against their energy industry.

CONCLUSION

Cyber attacks against the energy industry have become increasingly dangerous and sophisticated over the last few years. One of the main reasons for this is that computer equipment has become more affordable allowing intruders to get the necessary means to make a cyber attack. However, this is not always the case since some internet worms such as Stuxnet are very difficult to create. Furthermore, the policies and measures adopted by NATO in order to protect the critical energy infrastructure of its member states are very important in this regard. For instance, the Enhanced Cyber Defence Policy is particularly valuable, since it 'confirmes that cyber defence is part of the Alliance's core task of collective defence'. Consequently, the Alliance provides assistance to its nations in the field in case of an attack to their computer technology. Additionally, the exercise on the protection of critical energy infrastructure organized by NATO ENSEC COE is a good example of how NATO and Partner nations could prepare in advance to counteract cyber attacks to their energy industry.

REFERENCES

Bronk, Christopher Tikk-Ringas, Eneken, The Cyber Attack on Saudi Aramco, available at http://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

Butrimas, Vytautas, National Security and International Policy Challenges in a Post Stuxnet World, in Lithuanian Annual Strategic Review, vol. 12, 2013-2014, p.12

Butrimas, Vytautas, Ypatingos svarbos

[24] NATO, NATO Rapid Reaction Team to fight cyber attacks, available at http://www.nato.int/cps/en/natolive/news_85161.htm
[25] Ibidem
[26] NATO ENSEC COE, Centre of Excellence, available at http://www.enseccoe.org/en/about-us/centre-of-excellence.html
[27] NATO ENSEC COE, NATO-ICI Table Top Exercise on the "Protection of Critical Energy Infrastructure", available at http://www.enseccoe.org/en/news/nato-ici-table-tc6a.html

infrastruktūrų kibernetinis saugumas, http://www.lsta.lt/files/seminarai/2015-01-29%20LMA_seminaras/03_Ypatingos%20svarbos%20infrastrukturu%20kibernetinis%20saugumas.pdf

CCD COE, History, available at https://ccdcoe.org/history.html

CCD COE, About Cyber Defence Centre, available at https://ccdcoe.org/about-us.html

Čeponytė, Jurgita, How will Lithuania's LNG terminal work?, September 18, 2014, available at http://en.delfi.lt/lithuania/energy/how-will-lithuanias-lng-terminal-work.d?id=65876624

Clayton, Blake, Segal, Adam, Addressing Cyber Threats to Oil and Gas Suppliers, available at http://www.cfr.org/content/publications/attachments/Energy_Brief_Clayton_Segal.pdf

En, Elta, Gas pipeline via Poland, Lithuania will end Latvia's energy dependence, in Lithuania Tribune, 10 October 2014, available at http://en.delfi.lt/nordic-baltic/gas-pipeline-via-poland-lithuania-will-end-latvias-energy-dependence.d?id=66079816#ixzz3UgIX5STX

Financial Times, Definition of Black Swan, available at http://lexicon.ft.com/Term?term=black-swan

Langner, Ralph, To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, available at http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

Martewicz, Maciej, Bujnicki, Piotr, Poland to Get Baltic LNG Terminal on Time as Costs Increase, available at http://www.bloomberg.com/news/articles/2014-08-05/poland-to-get-lng-terminal-on-time-as-costs-discussed-pbg-says

NATO, NATO Rapid Reaction Team to fight cyber attacks, available at http://www.nato.int/cps/en/natolive/news_85161.htm

NATO Multimedia Library, Cyberspace security, available at http://www.natolibguides.info/cybersecurity

NATO, Cyber Timeline, in NATO Review Magazine, available at http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

NATO ENSEC COE, Centre of Excellence, available at http://www.enseccoe.org/en/about-us/centre-of-excellence.html

NATO ENSEC COE, NATO-ICI Table Top Exercise on the "Protection of Critical Energy Infrastructure", available at http://www.enseccoe.org/en/news/nato-ici-table-tc6a.html

Peretti, Kimberly, Slade, Jared, State-Sponsored Cybercrime: From Exploitation to Disruption to Destruction, available at http://www.alston.com/Files/Publication/0470bf82-1589-4200-be02-de03a3aea95b/Presentation/PublicationAttachment/35553890-a8a6-4eb5-b7bf-e6397539d409/14-183-State-Sponsored-Cybercrime.pdf

Radio Poland, Polish LNG terminal in Świnoujście to open May '16, available at http://www.thenews.pl/1/12/Artykul/221380,Polish-LNG-terminal-in-Swinoujscie-to-open-May-16

Reuters, Lithuania installs LNG terminal to end dependence on Russian gas, in Mail Online, October 27, 2014, available at http://www.dailymail.co.uk/wires/reuters/article-2809932/Lithuania-installs-LNG-terminal-end-dependence-Russian-gas.html

Shein, Rob, Zero-Day Exploit:– Countdown to Darkness, Rockland: Syngress Publishing Inc., 2004

Technology Institute, Security laboratory, available at http://www.sans.edu/research/security-laboratory/article/log-bmb-trp-door

Energy Infrastructure in Asymmetric Warfare: **The Case of the "Islamic State"**

Maj. Remigijus Žilinskas and Mr. Ján Čiampor

Over the last few years, asymmetric warfare has been strictly linked to the military activities of violent non-state actors (VNSA). This article analyses asymmetric warfare with particular attention to energy infrastructure (EI) and in relation to VNSA such as the so called "Islamic State" or DAESH (IS) in Iraq and Syria. After investigating the energy infrastructure targeted by VNSA with the help of the Global Terrorism Database, we discuss the attacks of the IS to energy infrastructure in the Middle East and the anti-IS military operation led by the United States. The analysis demonstrates that specific measures must be adopted to counteract the military activities of VNSA for which EI is an important target to seriously weaken their opponents, namely state and non-state actors.

INTRODUCTION

The recent surge in violence in the Middle East, due to the military efforts of the so called "Islamic State" (IS)[1] in Iraq and Syria, requires policy makers and military planners to consider the importance of energy infrastructure (EI) in asymmetric warfare. We mainly refer to infrastructures related to energy extraction (oil and natural gas wells, mines), transportation (oil tankers, pipelines, road and rail carriers, electric power lines) and conversion (refineries, power plants). These infrastructures are attractive targets of violent non-state actors given their importance for states' economy and people's well-being.[2] Therefore, it is necessary that governments adopt appropriate energy infrastructure protection measures. These measures are activities that deter or mitigate attacks against EI caused by people, natural disasters and accidents, and are concerned mainly with the protection of infrastructure and its capability to deliver antici-

Maj. Remigijus Žilinskas, NATO Energy Security Centre of Excellence, Vilnius

Maj. Remigijus Žilinskas (OF-3, LTU A) is Subject Matter Expert at the NATO Energy Security Centre of Excellence, Vilnius. He graduated from the Lithuanian Military Academy in 2000. Besides military education and training, he has masters' degrees in public administration and international relations from the Lithuanian Law University and the International Relations and Political Science Institute in Vilnius. He also attended a postgraduate course on defence and security at the politico-strategic level at the European Institute of International Relations (IERI) in Brussels, Belgium. He currently is a Ph.D. student at the Gen. Jonas Žemaitis Military Academy of Lithuania and Vytautas Magnus University in Kaunas. His research interests focus on security and defence studies, civil-military relations and public administration.

[1] Also referred to as Islamic State of Iraq and the Levant (ISIL); Islamic State of Iraq and Syria (ISIS); Islamic State of Iraq and ash-Sham; or Daesh. In spite of its name, the nature of the actor is 'non-state'. Its statehood is self-proclaimed and not diplomatically recognised.
[2] As used by Williams P. Violent Non-State Actors and National and International Security. 2008.

pated services.[3]

In this context and considering the challenges in differentiating between various armed actors, we adopt the broader term "violent non-state actors" (VNSA). These latter (e.g. terrorist groups, insurgents and paramilitary forces)[4] have asymmetric power capabilities if compared to their opponents, namely state and non-state actors. Asymmetry is interpreted as a wide disproportion of power between the warring parties, primarily in military and economic resources and capabilities. The asymmetry is essentially due to three conditions. The first one is that power disparities are not marginal but extreme. The second condition is that the extreme imbalance in resources available to the parties is compensated by the imbalance in resources needed to effectively confront the enemy. Finally, the higher power resources of the stronger actor lead to asymmetric high damage and high number of victims of the weaker actor. [5]

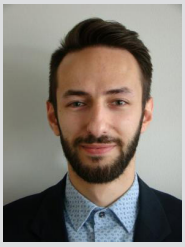
Also, when speaking about VNSA and asymmetric warfare, we mainly refer to militant insurgent and terrorist groups. According to the U.S. Department of Defense, both insurgency and terrorism involve the unlawful uses of violence with the aim to seize, nullify, or challenge political control of a region and/or extract political concessions that are unattainable through less violent means.[6] Although terrorist and insurgent groups have traditionally been considered as distinct, some authors claim that the differences between the two have become less evident.[7] By using the framework of VNSA, we strive to overcome ambiguities in definitions and try to place these acts in a context of a more complex reality.

In this article, we discuss the relevance of energy infrastructure in asymmetric warfare. In so doing, we first analyse the EI targeted by VNSA in general with a focus on contemporary VNSA and their military activities concerning EI. To this aim, the Global Terrorism Database has been used.[8] Then, we analyse the recent military operations of the IS related to EI in the Middle East and the anti-IS military operation led by the United States.

TARGETING ENERGY INFRASTRUCTURE

In their struggle against a ruling authority or in their effort to establish an autonomous national territory, VNSA use a broad spectrum of tactics, including blackmail, kidnappings, covert political and military operations, coercion, assassinations of government officials, and direct attacks against military personnel and officials. Additionally, attacks against energy infrastructure represent an attractive measure to strike the enemy interests and to weaken their military capabilities.

Mr. Ján Čiampor, Centre for Energy Studies, Brno



Ján Čiampor is a Master's degree student in International Relations and Energy Security at the Masaryk University in Brno, Czech Republic. He currently is a research assistant at the Centre for Energy Studies in Brno. His professional experience includes traineeships in the Czech Liaison Office for Research, Development and Innovation in Brussels and in the NATO Energy Security Centre of Excellence where he has conducted research on critical energy infrastructure protection.

[3] Radvanovsky R. and McDougall A. Critical Infrastructure: Homeland Security and Emergency Preparedness. 2010.
[4] Williams P. Violent Non-State Actors and National and International Security. 2008.
[5] Stepanova E. Terrorism in Asymmetrical Conflict: Ideologies and Structural Aspects. 2008.
[6] U.S. Department of Defense. Department of Defense Dictionary of Military and Associated Terms. 2015.
[7] Moghadam A., Berger R. and Beliakova P. Say Terrorist, Think Insurgent: Labeling and Analyzing Contemporary Terrorist Actors. 2014
[8] START. Global Terrorism Database. 2015; Attacks against energy infrastructure are coded under "Utilities".

Country	Number of attacks (2000-2014)
Pakistan	515
Colombia	239
Iraq	171
Yemen	158
India	56
Philippines	54
Nigeria	50
Egypt	41
Turkey	28
Algeria	23
Afghanistan	21

Figure 1. Number of asymmetric attacks against EI by country

Source: START. Global Terrorism Database. 2015.

Energy systems are a source of economic power but also a source of weakness. In many countries wherein asymmetric attacks have occurred, EI was an important target or an instrument of warfare. The reasons for this are essentially three. Firstly, the entire infrastructure behind oil and refined products industry is quite complex and is vulnerable to exploitation and damage by VNSA with belligerent purposes. For example, refined products that are transported by truck (e.g. truck convoys over long distances) are specifically relevant in this context. Trucks carrying explosive fuels represent an easy target for VNSA. They can be hijacked as a source of revenues or used as a weapon with substantial explosive capacity. Even small amounts of gasoline would be enough to cause a significant damage. In this context, it is worth mentioning the analysis of the Army Environmental Policy Institute that concludes that 10-12% of total casualties for the U.S. Army in Afghanistan and Iraq were related to supply operations, mostly fuel and water transport.[9] Also, according to the U.S. Transportation Command (USTRANSCOM), ground convoys were attacked 1,100 times in 2010. These numbers do exclude convoys moving along the fuel supply lines between operating and patrol bases. Between 2003 and 2007 in Iraq and Afghanistan, more than 3,000 Army personnel and contractors were wounded or killed in action from attacks on fuel and water resupply convoys.[10]

Secondly, asymmetric attacks against energy export infrastructure such as pipelines can lead to considerable revenue losses for the central government, and thus can substantially weaken its military capabilities. Oil can also be siphoned directly from pipelines to either fuel the VNSA forces or to sell the commodity to finance military activities. Centralized energy systems controlled by the government might also attract asymmetric attacks in order to damage the government's credibility in the eyes of its citizens and potential investors. In so doing, it can undermine its funding and economic stability. For instance, the VNSA

[9] Army Environmental Policy Institute. Sustain the mission project: Casualty factors from fuel and water resupply convoys. 2009, p. 17; Sullivan P. The Energy-Insurgency Revolution Nexus: An Introduction to Issues and Policy Options. 2014.

[10] U.S. Army. DLA Energy FY 2010 Net Sales in Afghanistan, BAH Final Report. 2010; for general information on fuel sales; data on actual price provided by the Department of Defense, Office of the Under Secretary of Defense/Comptroller. Energy for the warfighter: Operational energy strategy Retrieved from http://greenfleet.dodlive.mil/files/2011/06/OSD_op_energy_sttgy_rpt_to_congress_sm.pdf

such as the Revolutionary Armed Forces of Colombia (FARC) have carried out at least 239 attacks against EI, particularly pipelines such as the Caño Limon-Coveñas oil pipeline[11], the second most important pipeline in the country. In Pakistan, the Balochs insurgents have carried attacks on government and on foreign companies' infrastructure such as gas pipelines and transmission towers. Since 2000, there have been at least 515 attacks against EI in Pakistan and several blackouts caused by attacks against EI.[12]

Thirdly, VNSA operating in oil rich regions such as the Middle East and North Africa (MENA) pose a threat to stability of global energy prices. These groups, such as al-Qaeda cells, expressed interest in attacking EI targets in the past. Economic warfare against EI received higher priority in al-Qaeda's strategy after the U.S. intervention in Afghanistan and Iraq in the early 2000s. Al-Qaeda called for economic jihad against energy infrastructure in order to weaken Western military capabilities, since oil dependency is perceived by al-Qaeda as the West's greatest strategic vulnerability.[13] In the period between 2000 and 2014, 463 attacks against EI took place in the MENA region, mostly in Iraq and Yemen. In 2006, al-Qaeda attempted to attack the world's largest oil producing center Abqaiq in Saudi Arabia.[14] If the attack had been successful, it would have not only crippled Saudi oil production, but it would also have harmed the interests of Western countries by disrupting the global oil market with an inevitable increase of prices.

"ISLAMIC STATE" – A CASE OF EI IMPORTANCE IN ASYMMETRIC WARFARE

IS is a militant movement that has proclaimed itself as the Caliphate in the territory of western Iraq and eastern Syria - territories encompassing about six and a half million residents. The group has demonstrated the ability to conduct asymmetric warfare across large swathes of territory and has also engaged in conventional military battles against Syrian and Iraqi forces. In addition, after occupying the territory for a certain period, IS has shown the ability to rule the area, administer social services and even collect taxes.[15]

One of the features of IS warfare is targeting energy infrastructure. IS forces have been vandalizing Kurdish oil infrastructure in northern Iraq in order to deny the Kurd autonomous government a major source of revenue.[16] In March 2015, IS militants set oil wells on fire near the city of Tikrit, in order to thwart an attack by Shi'ite militias and government forces.[17] For a long time, one of the strategic targets of IS military forces has been the Baiji refinery, the largest one in Iraq. Since June 2014, when the IS captured the city, the belligerents have continuously been fighting over this strategic asset. In May 2015, IS militants took control of a part of the refinery complex and cut supply lines to a group of government forces. Later in May, IS forces set large parts of the refinery on fire, in an effort to thwart advancing government forces.[18] The Baiji refinery still remains one of the most important economic assets in Iraq. Before June 2014 it produced about half of Iraq's refined products. In addition to the lost export revenues, Bagdad was forced to import hundreds millions of dollars' worth of fuel. As a result, the Iraqi government and its military capabilities have been critically hampered by IS' activities.

In addition to attacking EI, IS has been seizing and operating significant oil and gas networks in both Syria and Iraq. Since 2014, IS has made strategic efforts to take control of the regional oil production capacities. It

[11] START. Global Terrorism Database. 2015.
[12] Ibid.
[13] Toft P., Duero A. and Beliaskus A. Terrorist targeting and energy security. 2010.
[14] START. Global Terrorism Database. 2015.
[15] STRATFOR. The Difference between Terrorism and Insurgency. 2014.
[16] Daly J. C. K. "The Islamic State's Oil Network". Terrorism Monitor. 2014, p.7-10.
[17] Hameed S. and Evans D. "Islamic State torches oil field near Tikrit as militia advance". Reuters. 2015.
[18] Al Jazeera. "ISIL fighters set Iraq's Beiji oil refinery ablaze". 2015
[19] Gordon M. R. "Iraqi Forces and Shiite Militias Retake Oil Refinery from ISIS". NY Times. 2015.

This map is without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Figure 2. Iraq hydrocarbon resources and energy infrastructure

Source: IEA. World Energy Outlook. 2012.

has launched several military operations in key areas of northern Iraq, seized several oil fields and small refineries and, above all, it has fought over the aforementioned Baiji refinery until October 2015, when it definitely lost control over it.[19] With an estimated daily production of as much as 50 000 – 100 000 barrels of oil, IS makes several million dollars every day,[20] making oil revenues IS' main source of funding.[21] Oil sales are made on the black market, where oil is sold at lower prices, although generating large cash flows.

Considering that oil sales have been IS' main source of funding, one of the priorities of the U.S.-led Operation Inherent Resolve has been focused on targeting the group's oil infrastructure with air strikes, thereby reducing its financial resources and ability to conduct operations and wage war. This has been particularly important in the absence

[20] Daly J. C. K. "The Islamic State's Oil Network". Terrorism Monitor. 2014, p.7-10.
[21] Shatz H. J. "How ISIS funds its reign of terror". New York Daily News. 2014.

of ground forces, which the U.S. and its allies have been reluctant to commit with. Meanwhile, much oil-related infrastructure is easily identified and targeted from aerial and satellite photography. In the period between June 2014 and November 2015, the air strikes destroyed 260 oil infrastructures across Syria and Iraq,[22] causing IS considerable financial hardship.

CONCLUSION

Violent non-state actors employ a broad spectrum of tactics in their military effort against the enemy whether it is a government or an international company. According to our findings, attacks against energy infrastructure, which are potentially vulnerable and critically important elements of society, are therefore an attractive target or an instrument in asymmetric warfare. Taking into consideration the aforementioned facts, we have come to the following conclusions.

Firstly, energy infrastructure can be used as a physical weapon itself, or can be targeted in order to exert pressure on governments or discredit their legitimacy. Secondly, VNSA also directly target the operations of foreign companies whom they perceive as exploiters of local communities and energy riches, and thus want to expel them from their territories. Thirdly, VNSA have expressed profound interest in energy infrastructure. Control over oil wells and other EI generates substantial revenues and provides the actors means to continue with their military efforts. In addition, EI has been considered as an attractive military target for VNSA forces.

Fourthly, in counter-insurgency operations, specific measures must be taken in the area of critical energy infrastructure protection. Considering that VNSA tend to attack the fuel supply lines of the enemy forces (e.g. truck convoys, storage depots and distribution centers), substantial efforts must be put into protecting these infrastructures in order to avoid loss of lives, supplies, combat power and financial resources. Counterinsurgency operations and asymmetric conflicts have thus increased the number of challenges to logistics forces.

Lastly, since energy resources are used by VNSA as a significant source of revenues, military efforts should be directed towards such targets in order to cut the belligerent actors' financing and thus hamper their military capabilities. Moreover, the governments threatened by local VNSA must develop measures to protect energy infrastructure and make their energy systems resilient. Protecting EI is essential for maintaining national military capabilities, social stability and welfare.

REFERENCES

Al Jazeera. "ISIL fighters set Iraq's Beiji oil refinery ablaze". 2015. Retrieved from http://www.aljazeera.com/news/2015/05/isil-fighters-set-iraq-baiji-oil-refinery-ablaze-150525122055089.html

Army Environmental Policy Institute. Sustain the mission project: Casualty factors from fuel and water resupply convoys. 2009. Retrieved from http://www.aepi.army.mil/docs/whatsnew/SMP_Casualty_Cost_Factors_Final1-09.pdf

Daly J. C. K. "The Islamic State's Oil Network". Terrorism Monitor. 2014, p.7-10. Retrieved from http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=42942&no_cache=1

Gordon M. R. "Iraqi Forces and Shiite Militias Retake Oil Refinery from ISIS". NY Times. 2015.

Hameed S. and Evans D. "Islamic State torches oil field near Tikrit as militia advance". Reuters. 2015. Retrieved from http://www.reuters.com/article/2015/03/05/us-mideast-crisis-iraq-idUSKBN0M10Z420150305

IEA. World Energy Outlook. 2012.

Moghadam A., Berger R. and Beliakova P. "Say Terrorist, Think Insurgent: Labeling and Analyzing Contemporary Terrorist Ac-

[22] U.S. Department of Defense. Operation Inherent Resolve: Targeted Operations against ISIL Terrorists. 2015.

tors." Perspectives on Terrorism Vol 8, No. 5, 2014: 1-17. Retrieved from http://www.terrorismanalysts.com/pt/index.php/pot/article/view/374/745

Radvanovsky R. and McDougall A. Critical Infrastructure: Homeland Security and Emergency Preparedness. 2010.

Shatz H. J. "How ISIS funds its reign of terror". New York Daily News. 2014. Retrieved from http://www.nydailynews.com/opinion/isis-funds-reign-terror-article-1.1931954

START. Global Terrorism Database. 2015.

Stepanova E. Terrorism in Asymmetrical Conflict: Ideologies and Structural Aspects. 2008. SIPRI. Retrieved from http://books.sipri.org/files/RR/SIPRIRR23.pdf

STRATFOR. The Difference between Terrorism and Insurgency. 2014. Retrieved from https://www.stratfor.com/weekly/difference-between-terrorism-and-insurgency

Sullivan P. "The Energy-Insurgency Revolution Nexus: An Introduction to Issues and Policy Options." Journal Of International Affairs Vol. 68, No. 1, 2014: 117-146. Retrieved from http://ezproxy.muni.cz/login?url=http://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,uid&db=bth&AN=100052750&lang=cs&site=eds-live&scope=site

Toft P., Duero A. and Beliaskus A. "Terrorist targeting and energy security." Energy Policy Vol 38 No. 8, 2010: 4411-4421. Retrieved from http://linkinghub.elsevier.com/retrieve/pii/S0301421510002600

U.S. Department of Defense. Department of Defense Dictionary of Military and Associated Terms. 2015. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

U.S. Department of Defense. Operation Inherent Resolve: Targeted Operations against ISIL Terrorists. 2015. Retrieved from http://www.defense.gov/News/Special-Reports/0814_Inherent-Resolve

US Army. DLA Energy FY 2010 Net Sales in Afghanistan, BAH Final Report. 2010.

Williams P. Violent Non-State Actors and National and International Security. 2008. ISN ETH Zurich

Ensuring Energy Security in NATO: **a Sociological Approach**

Dr. Sigita Kavaliūnaitė, Dr. Dainius Genys, and Dr. Tiziana Melchiorre

This article analyses the measures adopted by the North Atlantic Treaty Organization (NATO) to ensure energy security by trying to define its role in the field. To this aim, this study uses Ronald Inglehart's sociological approach with a focus on materialist and postmaterialist values. These latter can be identified in the dynamics of NATO's transformation process and growing attention to energy. Indeed, during the last decade, NATO's main aim in the field was to achieve a more efficient use of energy in the military sector by increasing its efforts to secure energy supply. In so doing, NATO valuably and profitably contributes to the field of energy security in the North-Atlantic area. At the same time, its strategies and policies do not create any duplication of other international actors that also deal with energy, such as the European Union (EU), which is one of NATO's most important partners.

INTRODUCTION

Ensuring energy security has become a hot topic on the agenda of the North Atlantic Treaty Organization (NATO) over the last decade. The 'gas wars' between Ukraine and Russia in 2005-2006 and in 2009[1] clearly demonstrated that ensuring energy security is a priority for states, and in 2014 the Ukrainian crisis made this issue even more urgent.[2] In this context, energy efficiency is seen as an important instrument to reinforce energy security because more efficient use means having more energy re-

Dr. Sigita Kavaliūnaitė, NATO Energy Security Centre of Excellence, Vilnius

Dr. Sigita Kavaliūnaitė joined Energy Security Centre of Excellence in 2013 as a delegate from Lithuanian Ministry of Foreign Affairs. She is responsible for analysis and research on energy security issues in the areas of concern to NATO. Prior to delegation, Dr. Sigita Kavaliūnaitė worked in various positions at the Lithuanian Diplomatic Service, including the position of Counsellor of Economic Security Policy Department and postings to the Embassies in the UK and USA. She holds a PhD in Social Sciences and a Master in Economics and has been periodically participating in international events on security and strategic policy issues, carrying out research projects, preparing scientific papers and lecturing in universities.

[1]The Orange Revolution in 2004, which was caused by protests against the corruption in the presidential elections, spelt the end of the preferential rates for Russia. Ukraine demanded higher prices for gas transit, while Russia insisted on higher prices for gas consumed by Ukraine. Negotiations remained deadlock and in 2005 Gazprom cut off supplies. Three days later, a comprise five-year deal was signed, but in 2009 gas supplies to Ukraine and to Europe were suspended for about two weeks because of debts and of re-emerged irreconcilable differences over prices. After long negotiations, new contracts were signed and supplies were resumed (Telegraph, November 1, 2011)

[2]Already in the Twentieth century, some events had made it clear that energy supplies could not be given for granted. The oil embargo in 1973 served as a turning point in global and domestic markets because it showed that energy supplies could be disrupted and that energy prices could not be always affordable. (Bahgat, 2011; Looney, 1992).

serves at disposal. At the same time, it also has multiple positive consequences in the military field, such as the reduction of the logistic footprint, the increase in the operational capabilities of troops (e.g. by reducing the need for fuel and water convoys and, consequently, decreasing escorts and casualties), the increase in the level of the energy security of operations (e.g. by reducing the risk related to reliance on fuel delivery), the reduction in the cost of the energy supply chain, the limitation of the carbon footprint of Armed Forces, and other related environmental protection and resource conserving gains.

Given this background, the research questions on which this paper investigates are the following ones. What measures has NATO adopted to increase energy security in the area of its concern? Can these measures be explained with a sociological approach? Given the kind of measures that it adopts, what is the role of NATO in the field of energy?

In order to answer these questions, the discussion will focus on the following two concepts, which are defined according to the International Energy Agency's approach[3]. Energy security is "the uninterrupted availability of energy sources at an affordable price" (International Energy Agency, 2015). Energy efficiency, which is strictly linked to the energy security concept, "is a way of managing and restraining the growth in energy consumption. Something is more energy efficient if it delivers more services for the same energy input, or the same services for less energy input" (International Energy Agency, 2015).

From a theoretical perspective, this article will use Ronald Inglehart's sociological approach while breaking away from it in one aspect. While Inglehart's theory focuses on the political, economic and cultural differences between states, this article does not since a deeper and more complex study would be necessary. Therefore, this article will adopt a more simple approach by considering NATO as a whole.

This paper will be divided into three sections. The first one is an overview of the main aspects of Inglehart's theory that will be applied to the case of NATO in the field of energy. The second section discusses the measures adopted by NATO to ensure energy security in the context of Inglehart's theoretical approach. Finally, the third section analyses and defines the role of NATO in the field.

RONALD INGLEHART'S THEORY

Ronald Inglehart's theory says that "economic development, cultural change and political change go together in coherent and, to some extent, predictable patterns" (Inglehart, 1997). He argues that certain changes are foreseeable because some socioeconomic trajectories are more likely than others. This is the case of industrialization, which is accompanied by mass mobilization and diminishing differences in gender roles. Industrialization is part of modernization, which Inglehart defines as "the overwhelming economic and political forces that drive cultural

Dr. Dainius Genys, Energy Security Research Centre, Vilnius

Dr. Dainius Genys is sociologist at the Energy Security Research Centre of the Vytautas Magnus University. He has recently completed the post-doc project "The Impact of Energy Threats to Lithuanian Social Cohesion" at the Lithuanian Energy Institute. He has been visiting fellow at: Hariman Institute, Russian, Eurasian and East European Studies, NATO Energy Security Centre of Excellence, Maxwell School for Citizenship and Public Affairs, Eco Energy Ltd and the Harry S. Truman Research Institute for the Advancement of Peace. Genys is a member of the Lithuanian sociological association, the European sociological association, the Advancement of the Baltic Studies Association and the Energy Policy Research Group. He has participated in many projects financed by the Lithuanian Research Council and the European Commission.

[3]The International Energy Agency was the result of a process initiated by the Washington Energy Conference in 1974 in response to the 1973 crisis (Culshaw et al, 2015)

change" (Inglehart et al, 2000), together with "occupational specialization, bureaucratization, centralization, rising educational levels and a configuration of beliefs and values closely linked with high rates of economic growth" (Inglehart, 1995). However, Inglehart says that advanced industrial societies experience postmodernization, namely a 'second syndrome of changes' in which economic growth becomes less central, while cultural and institutional changes occur. They emphasize the quality of life and democratic political institutions (Inglehart, 1995).

This paper focuses in particular on the materialist/postmaterialist value priorities component of Inglehart's theory. Materialist values are stability, security, physical integrity, economic and military strength. Postmaterialist values are higher quality of life, ideas, greater citizen involvement in decision-making at government and community levels, and environmental protection. Inglehart conceptualizes materialist and postmaterialist values on a single continuum with materialist values at one end and postmaterialist ones at the other one. The centre of the continuum is characterized by a mix of both sets of values. (Inglehart, 1997; Braithwaite et al, 1996). While materialist values prevail in modernization, postmaterialist values prevail in postmodernization.

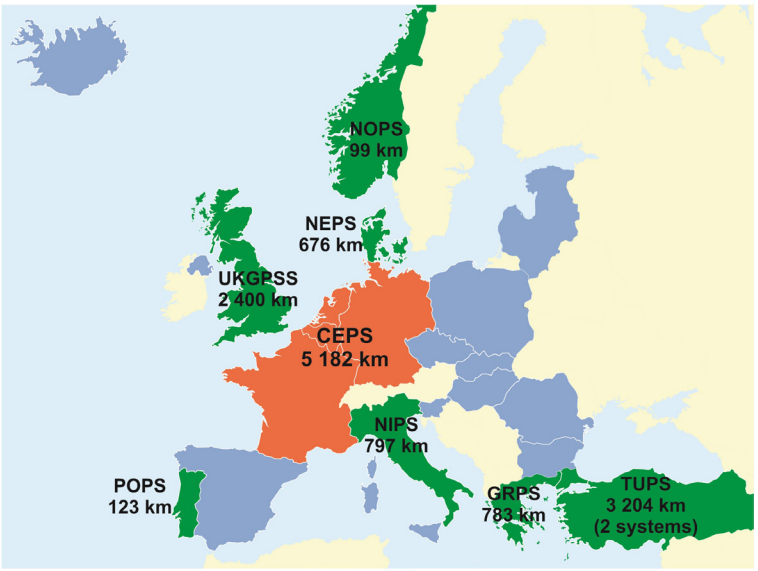


Figure 1. Map of the States covered by the NATO Pipeline System

Source: Presentation of NATO ENSEC COE Deputy Director, LTC Nicolas Henry during workshop "Hybrid threats: overcoming ambiguity, building resilience", September 10- 11, 2015, Vilnius

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

Dr. Tiziana Melchiorre holds a PhD in International Relations from the Department of Economic History of the Stockholm University. During her PhD program, she studied at the Centre d'Etudes et de Recherches Internationales-Sciences Po in Paris and conducted her research in Stockholm, Istanbul, Paris, Brussels and Riga. She also holds the Interdisciplinary Master in East European Research and Studies and a bachelor (Laurea) in International Sciences and Diplomacy with a specialization in European Studies from the Bologna University. She has shortly worked as researcher at the University of Stockholm and previously as trainee at the European Commission and at the Council of the Baltic Sea States. She has worked as intern and as editorial contributor at NATO Energy Security Centre of Excellence.

ENERGY SECURITY AND EFFICIENCY DYNAMICS IN NATO

NATO[4] has evolved from where it was in both 1949 and the 1990s. In 1949, when it was founded, the defence of the member states' territory according to art.5[5] of the Treaty was the main worry of the Allies. The fear of a military attack from the Soviet Union was felt as real during the Cold War. Therefore, according to Inglehart's theoretical approach, in 1949 the materialist values prevailed (therefore modernization) because physical integrity (which is here intended as the territorial defence of states) was a priority. To this aim, the guarantee of fuel supply to NATO Armed Forces was of utmost importance. The establishment of the NATO Pipeline System (NPS) served and still serves this purpose. It consists of ten distinct storage and distribution systems for fuels and lubricants. It is approximately 12,000 kilometers long and has a storage capacity of 5.5 million cubic metres (NATO, 2012).

Furthermore, during the Cold War, economic growth was particularly important. Indeed, the question of whether East or West was the better society could be decided by which one achieved the greatest economic growth (Inglehart, 1995). The arms and the space races between the United States (US) and the Soviet Union are good examples of the importance that economic growth had during the Cold War. In the context of the arms race in particular, NATO had a special place because it was the organization in charge of deploying advanced Armed Forces.

In the 1990s, the collapse of the Soviet Union deeply changed the geopolitical asset of Europe, provoking an identity dilemma in NATO.[6] However, the Alliance was able to reformulate itself as an organization which successfully stretched out to include former adversaries in Eastern and Central Europe. In so doing, it constructed for itself an identity as a promoter of democracy also in the former Soviet area of influence (Flockhart, 2011). In this period, focus on postmaterialist values prevailed (therefore postmodernization) with the quality of life becoming increasingly relevant. The changes occurred in the geopolitical asset of the international system were accompanied by economic and cultural changes, which led NATO members to focus on the core values of the organiza-

[4] In 1949, there were 12 founding members of the Alliance: Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom and the United States. The other member countries are: Greece and Turkey (1952), Germany (1955), Spain (1982), the Czech Republic, Hungary and Poland (1999), Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, Slovenia (2004), and Albania and Croatia (2009) (NATO, 2015)

[5] According to art.5 of NATO, "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security" (NATO, 2015a)

[6] Many discussions have been held among scholars and experts about the opportunity to maintain NATO alive. For instance, in the field of international relations, neorealists criticize institutional neoliberals for having underestimated the importance of institutions established to strengthen the security of states. Neorealist Mearsheimer argues that this is due essentially to the fact that the relationship between Europe and the USA has not changed after the end of the Cold War and NATO still provides stability on the European Continent. Mearsheimer states that "America has continued to serve as Europe's pacifier by maintaining a significant military presence on the continent and keeping NATO intact". Also, "most Europeans have not only welcomed America's continued presence in their midst, but they have largely accepted the idea that the United States has a moral and strategic responsibility to run the world". Waltz agrees with Mearsheimer as he says that one of the reasons explaining the survival of NATO is the willingness of its members to continue supporting their common values. Waltz also states that the most important reason of NATO's survival is that the United States wants it.
Waltz, K. (2000). Structural Realism after the Cold War. International Security. vol. 25(1). pp.18-26. See also Mearsheimer, J. (2010). Why is Europe peaceful today?. European Consortium for Political Research. Chicago: University of Chicago. p.2. For further discussions, see Melchiorre, T. (2014). Regional cooperation organizations in a multipolar world. Comparing the Baltic and the Black sea regions. Acta Universitatis Stockholmiensis. Stockholm Studies in Economic History 63. pp.22-24 and Mastny, V. (1999). NATO at Fifty: Did NATO Win the Cold War? Looking Over the Wall. Foreign Affairs (May/June). Retrieved from https://www.foreignaffairs.com/articles/1999-05-01/nato-fifty-did-nato-win-cold-war-looking-over-wall

tion constituting its identity. They are peace among states, freedom, and the principles of democracy, individual liberty and the rule of law. They seek to promote stability and well-being in the North Atlantic area (NATO, 2015a).

In the 21st century, NATO is a synthesis of materialist and postmaterialist values, and therefore of both modernization and post-modernization. Modernization is due to three elements. Firstly, in 2004 NATO enlargement, which was the result of the geopolitical changes occurred after the end of the Cold War, opening the opportunity of including former adversaries into the Alliance. Secondly, in 2014 the Ukrainian crisis made the necessity of the Allies to protect their territory urgent again. This is especially true for the states that had belonged to the Soviet sphere of influence. Thirdly, new NATO members continued the democratization process that had already begun in the 1990s. Postmodernization is due to the persistence of the founding values of the Alliance, which have been discussed above. They are contained not only in the Treaty of the Alliance, but also in the 2010 Strategic Concept[7], which "restates our [of NATO member states] firm commitment to keep the door to NATO open to all European democracies that meet the standards of membership, because enlargement contributes to our goal of a Europe whole, free and at peace. (...) NATO member states form a unique community of values, committed to the principles of individual liberty, democracy, human rights and the rule of law."[8]

In this context, it can be argued that while energy security as a whole is attributable to modernization, one of its dimensions, namely energy efficiency[9], is instead part of the post-modernization process. The reason is that energy security as a whole is necessary for survival and better life possibilities, while its energy efficiency dimension is evolving and gaining importance in more economically developed societies. Energy security is becoming increasingly relevant in the NATO of the 21st century. It is one of the most important challenges of this century. For this reason, during the last decade, NATO included the notion of energy security in its framework step by step.[10] The Wales Summit in 2014 is particularly meaningful since it stresses the necessity for the Allies of continuing to consult and further develop their capacity to energy security. In particular, they "will enhance our [of the Allies] awareness of energy developments with security implications for Allies and the Alliance; further develop NATO's competence in supporting the protection of critical energy infrastructure; and continue to work towards significantly improving the energy efficiency of our military forces (...)" (NATO, 2014a). Additionally, the Strategic Concept that was adopted during the Lisbon Summit in 2010 emphasizes the necessity to protect the "vital communication transport and transit routes on which international trade, energy security and prosperity depend". (NATO, 2014a). Therefore, it is clear

[7] "The Strategic Concept is an official document that outlines NATO's enduring purpose and nature and its fundamental security tasks. It also identifies the central features of the new security environment, specifies the elements of the Alliance's approach to security and provides guidelines for the adaptation of its military forces".
NATO. (2014). Strategic Concepts. Retrieved from http://www.nato.int/cps/en/natohq/topics_56626.htm

[8] The aim of the 2010 Strategic Concept is to well define the role of NATO after its identity crisis in the 1990s.
NATO. (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010. See also Flockhart, T. (2011)

[9] Henry, N. (2015), Editorial. In Energy Security: Operational Highlights, NATO Energy Security Centre of Excellence, n. 9, p.2

[10] NATO first referred to energy security in its 1999 Strategic Concept which stated that NATO's security could be affected not only by an attack to one of its Allies, but also by other factors, such as the disruption of the flow of vital resources. The Riga Summit in 2006 stressed the necessity of playing a role in the field. In 2008, the Bucharest Summit was the next step in the definition of a NATO acquis in the field of energy security. The Allies identified the principles governing NATO's approach in the field and outlined options and recommendations for further activities.
Stepper, P., Szàlkai. (Winter 2014-2015). NATO's Energy Security Agenda and its Possible Applications in the South Caucasus. Caucasus International. Vol.4(3-4)

that dealing with energy security is essential for NATO especially since some of its member states (e.g. Estonia, Latvia and Lithuania) are over dependent on foreign energy suppliers, especially from Russia. This has been particularly clear with the Ukraine crisis in 2014, which has shown again that energy disruptions are possible and that the shortage of energy supplies could jeopardize the life of people in NATO's member states. Thus, the awareness of the risks for its members has pushed NATO to develop a kind of acquis for energy security, which is contained in its official documents like the Strategic Concepts and the Declarations. Beside the traditional forms of political consultations, NATO has institutionalised expertise generation and information sharing on energy security issues through the activities of NATO Energy Security Centre of Excellence (NATO ENSEC COE) in 2012 (NATO, 2014a). It is "a widely recognized international military organization with the aim of providing qualified and appropriate expert advice on questions related to operational energy security" (NATO Energy Security Centre of Excellence, 2015). Its mission includes searching for and developing cost effective solutions for the support of military requirements and energy efficiency in the operational field, and interactions with academia and industry (Czulda et al, 2015). NATO ENSEC COE focuses, inter alia, on promoting energy innovations in the military by testing its innovative technologies in military units, trying to affect the 'culture' of energy consumption in the military and proposing tools for a better energy consumption management. In this context, the project "Energy Efficiency: Cultural Change" is particularly interesting since it aims to identify the cultural means which facilitate (or hinder) turning energy into a critical enabler for military operations and an efficient capability in power projection in areas of concern to NATO. Identifying these cultural means should allow NATO to strengthen and expand the culture of energy efficiency within militaries. In addition, behaviours sustaining enhanced energy efficiency in military should produce budget savings - without limiting operational capabilities – and produce other multiple positive consequences. The project is divided into two main parts. The first (completed) one consists of theoretical research aiming at creating 'cultural change' enablers and models. The second part includes field and practical research, which will test theoretical models within the Euro-Atlantic military community (e.g. interviews, workshops, surveys, discussions, etc). It will be developed by probing military stakeholder's views while mapping their level of awareness about energy efficiency issues, developing interactive environment (e.g. through advanced research workshops) and recommendations in respect of tools that lead to behavioural change as a precondition for turning energy into military capabilities' enabler.

Figure 2. Advanced Research Workshop "Towards Energy Efficiency Through Behaviour Change in the military", November 3, 2015, Vilnius, NATO ENSEC COE

Another example is NATO's Smart Energy Team (SENT)[11] that was launched at the end of 2012 to advance energy efficiency in the military. This Team is part of NATO's Smart Energy programme. Since 2011, it has been trying to find ways to improve the energy efficiency of Allied Armed Forces through a wide range of technologies and techniques, such as increased use of renewable energy and better energy management. SENT's first field-trip was experienced by a team of experts from 8 nations that visited an energy camp set up by Defence Research & Development Canada near Montréal (NATO, 2013). In 2013, SENT took active part in the multinational military

exercise 'Capable Logistician[12] 2013' (CL 13) with Smart Energy Camp[13] in Slovakia. Its two goals were raising the awareness of the importance of energy efficiency and to create a better understanding of the need for interoperability, as well as to help SENT to formulate recommendations for improving NATO's standards and best practices on saving energy. This initiative was repeated in Hungary in 2015, when 'Capable Logistician 2015' (CL15) was organized.

Figure 3. Workshop 'Smart Energy in CL15: from Observation to Recommendation' during the CL15 exercise
Source: http://www.enseccoe.org/en/events/gallery.html

On that occasion, "14 private companies, the Bundeswehr (BAAINWg) and the U.S. Army contributed over 50 pieces of equipment and highly trained personnel to provide Smart Energy production, storage, distribution and consumption, as well as portable and wearable soldier power solutions".[14] In this context, NATO ENSEC COE took active part as a co-organizer of the workshop 'Smart Energy in CL 15: from Observation to Recommendation' by offering expertise and knowledge to test the interoperability of energy efficient technologies for the military.

These initiatives and measures, which aim at saving energy and its costs, well serve the purposes contained in the Wales Summit Declaration. The Allies must "reverse the trend of declining defence budgets, to make the most effective use of our funds and to further a more balanced sharing of costs and responsibilities. Our overall security and defence depend both on how much we spend and how we spend it. Increased investments should be directed towards meeting our capability priorities, and Allies also need to display the political will to provide required capabilities and deploy forces when they are needed" (NATO, 2014a). Therefore, a more efficient use of energy is important because it can help the Alliance to use funds more efficiently, in such a way that the budget for defence can be increased to the benefit of the security of NATO members.

In sum, NATO is committed to increase energy security with a focus on energy efficiency, which has become essential for the security and for the well-being of both civilians and military. Additionally, this section has demonstrated that Inglehart's approach can be used to explain the development of energy security in NATO during the modernization and postmodernization periods and how this process is driven by both materialistic and postmaterialistic values.

THE ROLE OF NATO IN THE FIELD OF ENERGY

While the previous section has discussed the measures adopted by NATO in the energy field, this third section aims at explaining which role the Alliance plays in energy security by showing that it has two main roots. The first one is military. It reflects the need to conduct practical and logistical planning to

[11] SENT is jointly directed by the Lithuania-based NATO Energy Security Centre of Excellence and by the Joint Environment Department of the Swedish Armed Forces. It is composed of experts from eight nations, including six Allies (Canada, Germany, Lithuania, the Netherlands, the United Kingdom and the United States) and two partners (Australia and Sweden). (NATO, 2013a)

[12] Capable Logistician (CL) "is a bi-annual NATO standardization and interoperability Field Training Exercise designed to address NATO interoperability challenges on the coalition battlefield. The exercise is a fixed facility field trial with a tactical scenario that involves a Humanitarian Assistance Crisis Response Operation (CRO)".
Mapes, Steve. Capable Logistician 2015. Retrieved from http://www.natolibguides.info/ld.php?content_id=14631254

[13] The CL 13 Smart Energy Camp included representatives of the British Ministry of Defence, the Royal Dutch Army, the German Fraunhofer Institute Chemical Technology and NATO.
(NATO, 2013a)

[14] NATO Multimedia Library. Smart Energy: Exercises. Retrieved from http://www.natolibguides.info/c.php?g=48577&p=1610951

protect energy supplies with the aim to maintain the stability and the security of the Allies as well as NATO's operational capacity. This implies taking into consideration military threats to energy facilities and supply lines and routes. Therefore, energy security is very much linked to national security because it can lead to state-to-state conflicts (North Atlantic Council, 2013). The second root focuses on political threats to energy security and became prominent in the framework of NATO with the Ukraine-Russia gas dispute in 2005-2006 (Monaghan, 2008). Indeed, the Riga Summit, which was held that year, announced for the first time that energy security is a concern for NATO that, consequently, should play a role in that field. On that occasion, US Senator Richard Lugar argued that "because an attack using energy as a weapon can devastate a nation's economy and yield hundreds or even thousands of casualties, the Alliance must avow that defending against such attacks is an article Five commitment" (Stepper et al, Winter 2014-2015). Therefore, the Riga Declaration highlighted the importance of infrastructure security and required the member states to consult on most immediate risks in the field of security (Stepper et al, Winter 2014-2015). This is also emphasized in the 2010 Strategic Concept, which states that the Alliance will "develop the capacity to contribute to energy security, including protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning" (NATO, 2010).

Furthermore, NATO can contribute to several areas in the field of energy including, among others, information sharing, and planning and response. As Andrew Monaghan puts it, "since the Alliance would be working with other organisations, governments and actors of different types, these [broad areas] are likely to vary in degree on a case-by-case basis. But there is a clear range of niche roles for NATO in both areas. Some of these roles may be considered more passive, such as the alliance reducing its own fuel consumption, others more active, for instance contributing assets; some reactive, such as contributing civil defence and emergency management assets, others anticipatory, such as planning and providing training" (Monaghan, 2008).

In the field of information sharing, NATO can valuably contribute to energy security by acting as an important bridge between its member states through its North Atlantic Council (NAC)[15] that provides a forum for consultations on all issues affecting the peace and the security of the Allies. In this context, the role of NATO ENSEC COE is essential. Also, NATO can contribute through its coordinated military assets and expertise, which is an area where the Alliance has particular proficiency and expertise. The Wales Summit Declaration states that NATO will continue contributing to "build on the experience gained in recent operations and improve our interoperability through the Connected Forces Initiative (CFI)".[16] NATO "provides the structure for Allies to train and exercise coherently; reinforces full-spectrum joint and combined training; promotes interoperability, including with partners; and leverages advances in technology, such as the Federated Mission Networking framework, which will enhance information sharing in the Alliance and with partners in support of training, exercises and operations. Therefore, NATO can provide protection of energy sources and of transportation means in military security terms" (Monaghan, 2008). In the field of response, NATO can contribute with the necessary assets to respond to energy related emergencies, especially those concerning critical energy infrastructure (NATO, 2015d).

Additionally, NATO cooperates with other international actors such as the European Union (EU), which is one of its most important partners. The Wales Summit Declaration, for

[15] NAC is the principal political decision-making body within NATO (NATO, 2015)
[16] The Connected Forces Initiative (CFI) "aims to enhance the high level of interconnectedness and interoperability Allied forces have achieved on operations and with partners. CFI combines a comprehensive education, training, exercise and evaluation programme with the use of cutting-edge technology to ensure that Allied forces remain prepared to engage cooperatively in the future" (NATO, 2015d)

instance, states that NATO and the EU will continue working together in areas of common interests. It emphasizes that "we [NATO] look forward to continued dialogue and cooperation between NATO and the EU. Our consultations have broadened to address issues of common concern, including security challenges like cyber defense, the proliferation of weapons of mass destruction, counter-terrorism, and energy security" (NATO, 2014a).

NATO's and EU's activities and policies in the field of energy security are necessary to each other because the Alliance is mainly focused on a military security perspective, while the EU has a more comprehensive approach and aims at achieving three main objectives: a) to secure energy supplies to ensure the reliable provision of energy whenever and wherever needed; b) to ensure that energy providers operate in a competitive environment that ensures affordable prices for homes, businesses, and industries; c) to make energy consumption sustainable, through the lowering of greenhouse gas emissions, pollution, and fossil fuel dependence (European Commission, 2015). These objectives are also relevant for NATO since continued and reliable provision of energy is essential not only for civilians, but also for military. Affordable prices of energy are also necessary for cost efficiency in the military field. Additionally, protecting the environment is an important goal also for NATO since it is included in its energy security policies. This is explicitly affirmed in the 2010 Strategic Concept. It states that "key environmental and resource constraints, including health risks, climate change, water scarcity and increasing energy needs will further shape the future security environment in areas of concern to NATO and have the potential to significantly affect NATO planning and operations" (NATO, 2010).

The Alliance recognized the challenges coming from the environment already in 1969, when it established the Committee on the Challenges of Modern Society (CCMS).[17] It has been providing a unique forum for NATO and its partner countries to share knowledge and experience on social, health and environmental matters, both in the civilian and military sectors. In 2006 it merged with the NATO Science for Peace and Security (SPS) Programme.[18] Furthermore, the Specialist Team on Energy Efficiency and Environmental Protection (STEEEP) "aims to integrate environmental protection and energy efficiency regulations into technical requirements and specifications for armaments, equipment and materials on ships, and for the ship to shore interface in the Allied and partner nations' naval forces" (NATO, 2015g).

In sum, in the field of energy security NATO's strategies and policies are relevant for its member states, but also in the broader international context, especially in relation to the activities of other international actors such as the EU.

CONCLUSION

This article has discussed the measures adopted by NATO to ensure energy security with a focus on one of its dimensions, namely energy efficiency. Also, NATO's role in the field has been defined by using Inglehart's sociological approach with a focus on materialist and postmaterialist values.

The analysis has shown that in the 21st century NATO is driven by a synthesis of these two sets of values. The reason is that NATO defends the territorial integrity of its members that is a materialist value, but it also protects the values contained in its documents, which can be defined as postmaterialist values (e.g. democracy, well-being) according to Inglehart's theoretical approach. In this context, ensuring energy security has become an urgent matter because it is essential both to

[17] The Committee on the Challenges of Modern Society deals with problems affecting the environment and the quality of life through 3-5 year pilot studies, shorter term projects, conferences, workshops and roundtables. It conducts its activities through teams of national experts. (NATO, 2015e)

[18] "The Science for Peace and Security (SPS) Programme is a policy tool that enhances cooperation and dialogue with all partners, based on scientific research, innovation, and knowledge exchange. The SPS Programme provides funding, expert advice, and support to security-relevant activities jointly developed by a NATO member and partner country" NATO. (2015f).

ensure the protection of lives and to continue affirming the values of the Alliance.

Furthermore, the analysis has shown that during the last decade NATO has developed a kind of acquis for energy security which is contained in its documents such as the Summit Declarations and its 2010 Strategic Concept, which define the role of NATO in the field. This latter is twofold. On the one hand, it reflects the need to conduct practical and logistical planning to protect energy supplies with the aim to maintain the stability and the security of the Allies as well as NATO's operational capacity. On the other one, NATO deals with the political threats to energy security that became prominent in NATO with the Ukraine-Russia gas dispute in 2005-2006.

Additionally, NATO valuably and profitably contributes to energy security without duplicating the activities of other international actors dealing with this issue, such as the European Union (EU), which is one of its most important partners. The work of the Alliance and the one of the EU are useful to each other as the contribution that they give is different. While the Alliance can provide support from a military security perspective, the EU's activities are more comprehensive and essentially address civilians.

Therefore, it can be concluded that NATO is becoming increasingly involved in energy security through its acquis, its activities and its bodies. This means that its contribution to the field of energy is becoming increasingly meaningful for its member states in order to face common challenges and threats.

REFERENCES

Bahgat, G. (2011). Energy Security: An Interdisciplinary Approach. New York: John Wiley & Son.

Braithwaite, V., Makkai, T., Pittelkow, Y. (1996). Inglehart's Materialism-Postmaterialism Concept: Clarifying the Dimensionality Debate Through Rokeach's Model of Social Values. Journal of Applied Social Psychology. Vol.26(17)

Culshaw, M.G., Osipov, V.I., Booth, S.J., Viktorov, A.S. (eds). (2015). Environmental Security of the European Cross-Border Energy Supply Infrastracture. The NATO Science for Peace and Security Programme. Dordrecht: Springer

Czulda, R., Madej, M. (2015). Newcomers no more? Contemporary NATO and the Future of the Enlargement from the Perspective of the "Post-Cold War" Members. Warsaw: Institute of International Relations

European Commission. (2015). Energy Strategy. Retrieved from https://ec.europa.eu/energy/en/topics/energy-strategy

Flockhart, T. (2011). After the Strategic Concept, Towards a NATO Version 3.0. DIIS Report n.6. Copenhagen: Danish Institute for International Studies

Henry, N. (2015). Editorial. In Energy Security: Operational Highlights, NATO Energy Security Centre of Excellence, n.10

Inglehart, R. (1995). Changing values, economic development and political change. UNESCO. Cambridge: Blackwell Publishers

Inglehart, R. (1997). Modernization and Postmodernization, Cultural, Economic, and Political Change in 43 Societies. Princeton: Princeton University Press

Inglehart, R., Baker, W. (2000). Modernization, Cultural Change, and the Persistence of Traditional Values. American Sociological Review. Vol.65(February)

International Energy Agency. (2015). Retrieved from http://www.iea.org/topics/energysecurity/

Looney, R. (1992). The Gulf War and the Price of Oil: Prospects for the Medium Term. The Journal of Social, Political and Economic Studies.vol.17(3-4)

Mapes, S. (2015). Capable Logistician 2015. Retrieved from http://www.natolibguides.info/ld.php?content_id=14631254

Mastny, V. (1999). NATO at Fifty: Did NATO Win the Cold War? Looking Over the Wall. Foreign Affairs (May/June). Retrieved from https://www.foreignaffairs.com/arti-

cles/1999-05-01/nato-fifty-did-nato-win-cold-war-looking-over-wall

Mearsheimer, J. (2010). Why is Europe peaceful today?. European Consortium for Political Research. Chicago: University of Chicago

Melchiorre, T. (2014). Regional cooperation organizations in a multipolar world. Comparing the Baltic and the Black sea regions. Acta Universitatis Stockholmiensis. Stockholm Studies in Economic History 63

Michaelis, S. (2013). Smart Energy at "Capable Logistician 2013". Energy Security: Operational Highlights. vol.3

Monaghan, A. (2008). Energy Security: NATO's Limited, Complementary Role. Rome: NATO Defense College

NATO. (2010). Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted by Heads of State and Government at the NATO Summit in Lisbon 19-20 November 2010

NATO. (2012). NATO Pipeline System. Rerieved from http://www.nato.int/cps/en/natohq/topics_56600.htm

NATO. (2013). SENT explores energy efficiency for the military in cold climates. Retrieved from http://www.nato.int/cps/en/natohq/news_99173.htm

NATO. (2013a). Smart Energy Camp opens eyes to promising energy-saving solutions. Retrieved from http://www.nato.int/cps/en/natolive/news_101896.htm

NATO. (2014). Strategic Concepts. Retrieved from http://www.nato.int/cps/en/natohq/topics_56626.htm

NATO. (2014a). Active engagement, modern defence. Retrieved from http://www.nato.int/cps/en/natohq/official_texts_68580.htm

NATO. (2015). Member countries. http://nato.int/cps/en/natohq/topics_52044.htm

NATO. (2015a). The Atlantic Treaty, Washington D.C., 4 April 1949. Retrieved from http://www.nato.int/cps/en/natolive/official_texts_17120.htm

NATO. (2015b). NATO and its partners become smarter on energy. Retrieved from http://www.nato.int/cps/en/natohq/news_118657.htm

NATO (2015c). The North Atlantic Council. Retrieved from http://www.nato.int/cps/en/natolive/topics_49763.htm

NATO. (2015d). Connected Forces Initiative. Retrieved from http://www.nato.int/cps/en/natolive/topics_98527.htm

NATO. (2015e). Partnership in Action. Retrieved from http://www.nato.int/events/0110eapc/english/txt-15.htm

NATO. (2015f). Science for Peace and Security. Retrieved from http://www.nato.int/cps/en/natolive/78209.htm

NATO. (2015g). Environment-NATO's Stake. Retrieved from http://www.nato.int/cps/en/natohq/topics_91048.htm

NATO ENSEC COE. (2015). Centre of Excellence. Retrieved from http://www.enseccoe.org/en/about-us/centre-of-excellence.html

North Atlantic Council (2013). NATO's role in energy security. The uprising energy security challenge. Thessaloniki: University of Macedonia.

Stepper, P., Szàlkai. (Winter 2014-2015). NATO's Energy Security Agenda and its Possible Applications in the South Caucasus. Caucasus International. Vol.4(3-4)

Telegraph (November 1, 2011). Russia and Ukraine: History of the Gas Wars. Retrieved from http://www.telegraph.co.uk/sponsored/rbth/politics/8862357/Russia-Ukraine-history-gas-wars.html

Waltz, K. (2000). Structural Realism after the Cold War. International Security. vol. 25(1)

NATO Energy Security Centre of Excellence

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

ISSN 2335-7975