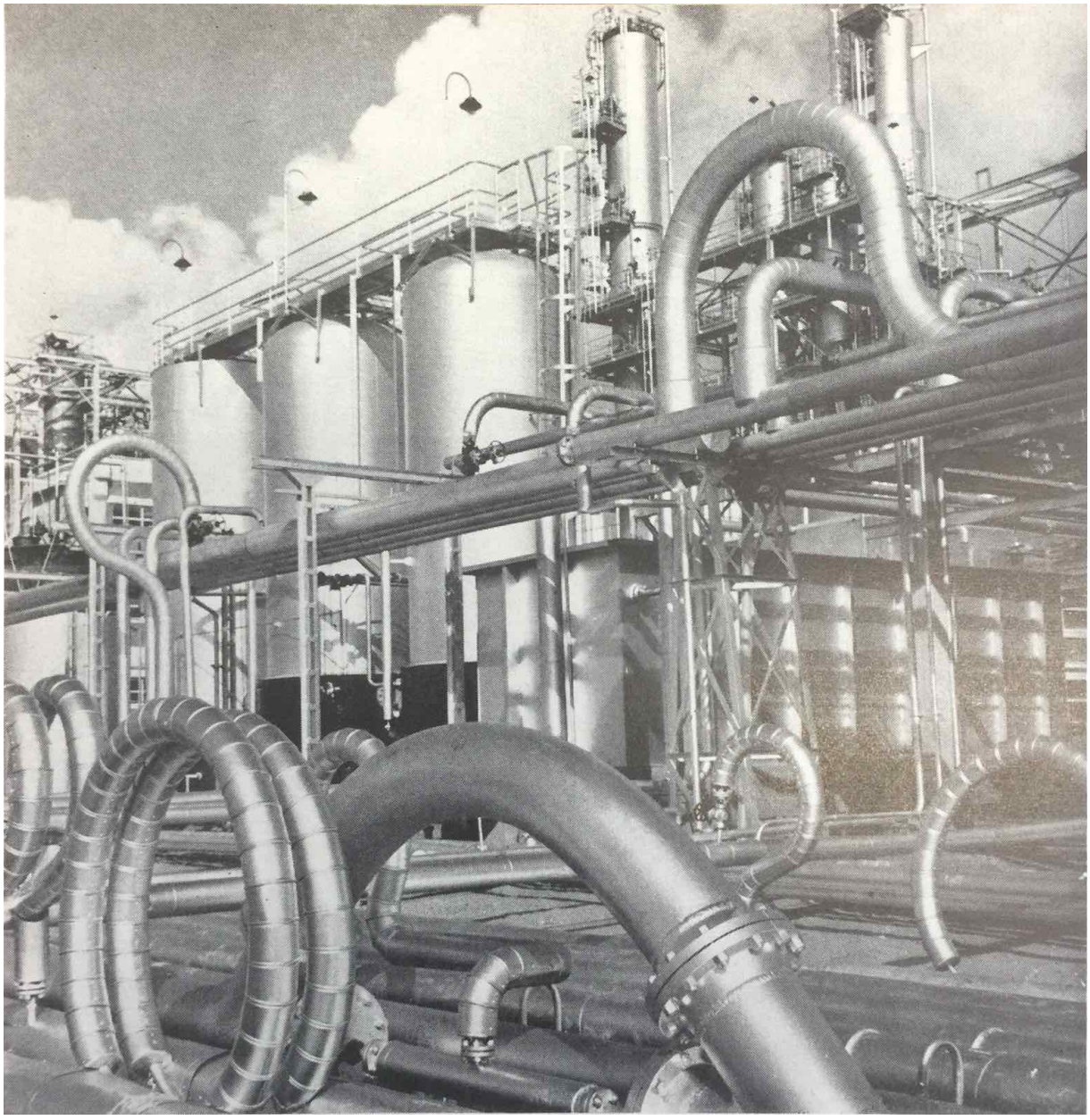
A dissertation submitted to
the Department of Environmental Sciences and Policy of the
Central European University
in part fulfillment of the Degree of Doctor of Philosophy



THE REGIONAL SECURITIZATION OF CYBER-PHYSICAL ENERGY SYSTEMS

Ion A. Iftimie
September 2020

This dissertation is submitted in fulfilment of the Degree of Doctor of Philosophy awarded by the Department of Environmental Sciences and Policy at the Central European University.

Cover photo: Central Europe Pipeline System (CEPS), The Fifteen Nations, 9/10, 1959

Notes on copyright and the ownership of intellectual property rights:

(3) For bibliographic and reference purposes this dissertation should be referred to as:

Iftimie, IA. 2020. The regional securitization of cyber-physical energy systems. Doctoral dissertation, Department of Environmental Sciences and Policy, Central European University, Vienna.

Further information on the conditions under which disclosures and exploitation may take place is available from the Head of the Department of Environmental Sciences and Policy, Central European University.

Author's declaration:

No portion of the work referred to in this dissertation has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning. Furthermore, this dissertation contains no materials previously written and/or published by another person, except where appropriate acknowledgment is made in the form of bibliographical reference, etc.

Ion A. IFTIMIE

Table of Contents

List of Tables

List of Figures

General Abbreviations

€ — Euro (currency of the European Union)
ACER — Agency for the Cooperation of Energy Regulators
AES — Asian Energy Security
AIC — availability, integrity, confidentiality
API — American Petroleum Institute
APT — advanced persistent threats
ASCOPE — area, structures, capabilities, organizations, people, events
ASEAN — Association of Southeast Asian Nations
AU — African Union
BAT — best available technique
BPO — Belgian Pipeline Organization
BREF — BAT reference documents
CARVER — criticality, accessibility, recuperability, vulnerability, effect and recognizability
CCASG — Gulf Cooperation Council
CDMB — NATO Cyber Defence Management Board
CEDC — Central Europe Defence Cooperation
CEE — Central and Eastern Europe
CEI — critical energy infrastructure
CEIP — critical energy infrastructure protection
CEMAC — Central African Economic and Monetary Community
CENSAD — Community of Sahel-Saharan States
CEPGL — Economic Community of Great Lakes countries
CEPS — Central Europe Pipeline System
CERT — cyber emergency response team
CFR — Council on Foreign Relations
CF SEDSS — Consultation Forum for Sustainable Energy in the Defence and Security Sector
CHP — combined heat and power
CIRT — computer incident response team
CIS — Commonwealth of Independent States
CME — coronal mass ejection
CO_2 — Carbon Dioxide
COMESA — Common Market for Eastern and Southern Africa
COTS — commercial off-the-shelf
CPES — cyber physical energy systems
CPS — cyber physical systems
CS2A — collective security (cyber) alliance
CSA — collective security alliance
CSCE — Commission on Security and Cooperation in Europe

CSDP — Collective Security and Defense Policy
CSIRT — computer security incident response team
CSTO — Collective Security Treaty Organization
CTIAP — Critical Thinking Intelligence Analysis Process
DCS — Distributed Control System
DoE — U.S. Department of Energy
DPO — Dutch Pipeline Organization
DPRK — Democratic People's Republic of Korea
EAC — East African Community
EC — European Commission
ECCAS — Economic Community of Central African States
ECE — Eastern and Central Europe
ECOWAS — Economic Community of West African States
EDA — European Defence Agency
EE — energy efficiency
EEA — European Economic Area
EEPR — European Energy Programme for Recovery
EIA — Energy Information Administration
EM — energy management
EMP — electromagnetic pulse
ENISA — European Union Agency for Cybersecurity
ERIA — Economic Research Institute for ASEAN and East Asia
EU — European Union
EU28 — 28 member states of the European Union
EUCOM — United States European Command
EU Med — Alliance of 7 Southern European Union member states
FBG — a German quasi-public corporation
FEMA — United States Federal Emergency Management Agency
GCI — Global Cybersecurity Index
GCU — Global Cybersecurity Unit
FYROM — Former Yugoslavian Republic of Macedonia
FSB — Federal Security Service of the Russian Federation
GEA — Global Energy Assessments
GRPS — Greek Pipeline System
GUI — government, university, industry
HAG — Hungary-Austria pipeline
ICPS — Icelandic Pipeline System
ICS — industrial control systems
IEA — International Energy Agency
IGAD — Inter-Governmental Authority on Development

INGAA — Interstate Natural Gas Association of America
INL — Idaho National Laboratory
IO — international organization
IOC — Indian Ocean Commission
IoE — Internet of Everything
IoT — Internet of Things
IP — intellectual property
IT — information technology
ITU — International Telecommunication Unit
MOSES — Model of Short-Term Energy Security
MMBtu — one million British thermal units
MRU — Mano River Union
MS — member state
NATO — North Atlantic Treaty Organization
NB8 — Nordic-Baltic Eight
NEPS — North European Pipeline System
NIPS — Northern Italy Pipeline System
NIS — Network and Information Security Directive
NIST — National Institute for Standards and Technology
NOPS — Norwegian Pipeline System
NPS — NATO Pipeline System
NSPO — NATO Support and Procurement Organisation
O&G — oil and gas
OECD — Organisation for Economic Co-operation and Development
OEM — Original Equipment Manufacturer
OPEC — Organization of Petroleum Exporting Countries
OMV — the name of an Austrian oil and gas company
OSCE — Organization for Security and Co-operation in Europe
OT — operational technology
PAIN — privacy/confidentiality, authentication, integrity, nonrepudiation
PAP — prevention action plan
PES — primary energy source
PMESII — political, military, economic, social, infrastructure, information
POPS — Portuguese Pipeline System
POTUS — President of the United States
PSC — Peace and Security Council
RAND — Research ANd Development NGO
RePEc — Research Papers in Economics
RES — renewable energy sources
ROK — Republic of Korea

RQ — research question
RSCT — Regional Security Complex Theory
RSS — Regional Security System
RWE — the name of a German utilities company
S2LCET — smart and sustainable low carbon energy transitions
SACU — Southern African Customs Union
SADC — Southern Africa Development Community
SADC — South American Defense Council
SCADA — Supervisory Control and Data Acquisition
SCO — Shanghai Cooperation Organization
SEECP — South-East European Cooperation Process
SICA — Central American Integration System
SPEKD — social, political, economic, knowledge and digital
STEPE — social, technological, economical, political, ecological
SVR — Foreign Intelligence Service of the Russian Federation
TAG — Trans Austria Gasleitung (pipeline)
TEN-E — trans-European energy networks
TpA — third party access
TPES — total primary energy supply
TRAPIL — a French quasi-public corporation
TSO — transmission system operator
TUPS — Turkish Pipeline System
TYNDP — Ten-Year Network Development Plan
UCLA — University of California, Los Angeles
UEMOA — West African Economic and Monetary Union
UKGPSS — United Kingdom Pipeline and Storage System
UMA — Arab Maghreb Union
UN — United Nations
UNASUR — Union of South American Nations
UNSC — United Nations Security Council
U.S. — United States
USAID — United States Agency for International Development
USD — United States dollar
USSR — Soviet Union
V4 — Visegrád Group

Abstract

Energy production, transportation and distribution rely today on smart technologies that are vulnerable to various threats in the cyber domain. This research defines cyber domain as the totality of interconnected systems used for the purpose of enabling communication between physical (hardware), logical (software) and/or social (digital persona) layers by electronic means. Almost all critical energy technologies (even most of the stand-alone systems) are connected to the cyber domain; making every critical energy infrastructure vulnerable to malicious cyber activities.

When critical energy infrastructure fails (due to technical or human factors), environmental disasters happen: oil spills (like the Exxon Valdez Oil Spill in Prince William Sound off the coast of Alaska and British Petroleum Oil Spill in the Gulf of Mexico), black-outs (like the Northeast or Italy blackouts of 2003), and even nuclear meltdowns (like the Three Mile Island in Pennsylvania, Chernobyl in Ukraine, and the Fukushima Daiichi nuclear disaster in Japan). A cyber-attack against an oil tanker's navigation systems could cause the next oil spill; a SCADA attack could cause the next major blackout (this has already happened in Ukraine); and a malicious code against nuclear centrifuges (like we have seen in the case of Stuxnet) could cause the next nuclear meltdown.

The cyber threats to critical energy infrastructure are growing exponentially and nation states can no longer defend themselves without the support of strategic alliances in the cyber domain. In this context, regional collective security alliances, such as the North Atlantic Alliance, emerge as necessary instruments that complement national efforts in protection of domestic cyber-physical systems. For example, NATO Cyber Rapid Reaction teams are already placed at the disposal of NATO member states to assist in protection of domestic critical energy infrastructure, if the need ever arises.

While this is the case, there are currently no studies addressing the cyber threats to regional energy systems and the role of collective security alliances in combating them. To address this gap in literature, this paper looks at the growing energy security role of NATO in the cyber domain to empirically validate the role of collective security alliances in the security of regional energy

systems—geo-energy systems—and their prospects. It also proposes an explanatory framework—that considers the environmental effects of malicious cyber activities—for the role of collective security alliances in protecting critical cyber-physical energy systems.

The main contributions to literature rest in 1) addressing the cyber threats to critical energy infrastructure within the context of regional rather than traditional global and national lens; 2) validating the feasibility of collective security alliances to integrate the protection of national cyber-physical energy systems into their mandate (the ends); and 3) recognizing the link between cyber threats and environmental considerations.

Keywords: Cyber Security, Collective Security Alliances, Geo-Energy Systems, North Atlantic Treaty Organization, Central Europe Pipeline System, Military Mobility.

Acknowledgements

As a senior military officer, pursuing my doctoral studies has not been an easy endeavor. Finding the time for these studies would not have been possible without the support of the fellow senior officers serving under the past two Commanders of the United States Cyber Command: United States Navy Admiral Michael S. Rogers and United States Army General Paul Nakasone.

I am most grateful to four professors in the Department of Environmental Sciences and Policy at the Central European University: 1) my research supervisor, Associate Professor Alexios Antypas, who recognized from the beginning in the importance of my research for national and regional energy and environmental security; 2) Associate Professor Michael LaBelle, who challenged me to further study the links between energy and geography; 3) Professor Aleh Cherp, who was influential in shaping my understanding of energy security's current state of art; and 4) Associate Professor Tamara Steger, for instilling in me a passion for environmental justice. To Gyorgyi Puruczky, the PhD Program Coordinator: thank you for everything that you do!

The interviews conducted for this study would not have been possible without the support of many NATO subject matter experts (both military and civilian) during my Eisenhower Fellowship at the NATO Defense College in Rome, Italy and during my Fellowship at the NATO Energy Security Centre of Excellence in Vilnius, Lithuania. Special thanks are also extended to the members of the Energy Security Panel at the NATO Science and Technology Organization in Paris, France, who found great value in my research and encouraged me to expand on it. Special thanks to Dr. Dumitru Minzarari of the NATO Defense College for always being there to debate difficult questions related to military strategy, modern warfare and conflict technologies. Also, to the United Nations and its International Telecommunications Union for sharing with me the raw data of the Global Cybersecurity Index in order to validate my findings.

Finally, but not lastly, to my beautiful wife Michele and to my two amazing sons, Cezar and Viktor, for their unending love and patience.

Chapter 1

Introduction

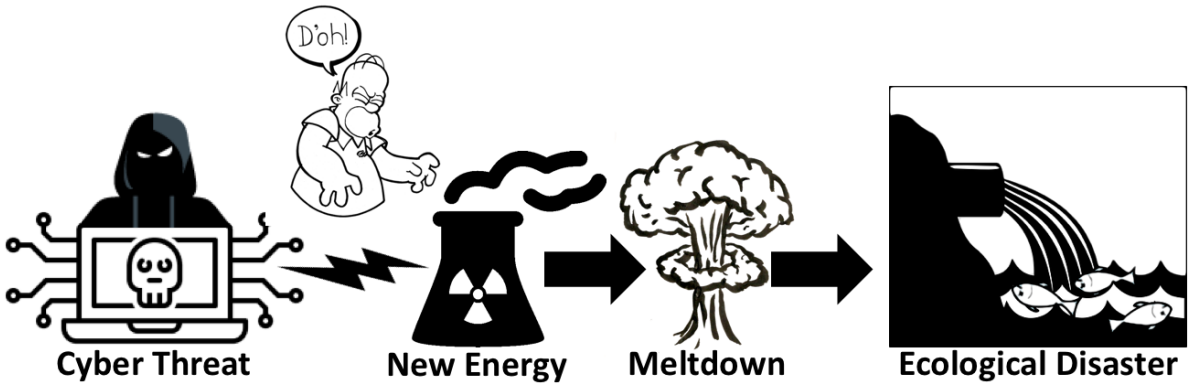
1.1 Statement of the problem

In the year 2000, a cyber-attack against a sewage treatment plant's supervisory control and data acquisition (SCADA) system in Maroochy Shire, Australia, caused 800,000 liters of raw sewage to be spilled into the local rivers and parks (Brown 2011). As a result of this cyber-attack, "marine life died, the creek water turned black and the stench was unbearable for residents" (Abrams and Weiss 2008, 8). While malicious cyber-attacks targeting industrial control systems (ICS) — which monitor and control physical industrial processes (IBM 2015, 3; Nazir and Kaleem 2018) — were isolated incidents in the year 2000, they have grown exponentially, and have become the norm over the past decade. Of these, between 2012 and 2014, reported cyber-attacks against SCADA alone have increased by 636 percent (IBM 2015, 5). When critical energy infrastructure fails (due to technical or human factors), environmental disasters happen: oil spills (like the Exxon Valdez Oil Spill in Prince William Sound off the coast of Alaska and British Petroleum Oil Spill in the Gulf of Mexico), black-outs (like the Northeast or Italy blackouts of 2003), and even nuclear meltdowns (like the Three Mile Island in Pennsylvania, Chernobyl in Ukraine, and the Fukushima Daiichi nuclear disaster in Japan). A cyber-attack against an oil tanker's navigation systems (like the ones that may have already happened against U.S. Navy ships in the Pacific) could cause the next oil spill; a SCADA attack could cause the next major blackout (this has already happened in Ukraine); and a malicious code against nuclear centrifuges (like we have seen in the case of Stuxnet) could cause the next nuclear meltdown. In these contexts (and many others), cyber-attacks against critical energy infrastructure emerge as a threat to both energy and environmental security; and collective security alliances (CSAs) such as the North Atlantic Treaty Organization (NATO) are currently trying to identify their role in addressing this threat during "smart and sustainable" (Elias G.

Carayannis and Rakhmatullin 2014, 212) "low-carbon energy transitions" (Bridge et al. 2013, 331; Geels 2014, 30; Goldthau and Sovacool 2012, 232).

In 2017, several U.S. government agencies responded to a cyber-attack against a U.S. nuclear facility near Burlington, Kansas (Broersma 2017; Riley, Dlouhy, and Gruley 2017). Months later, the Department of Homeland Security and the Federal Bureau of Investigations issued a joint technical alert revealing that Russian Government cyber activities were targeting energy, nuclear and other critical infrastructure sectors (CISA 2018). The report stated that Russian advanced persistent threat activities were specifically targeting critical energy systems operating in English, French, German, Italian and Spanish languages—primary languages of the United States and key European NATO Allies—with the goal of identifying vulnerabilities pertaining to ICS.

The attack against the Burlington nuclear facility highlighted the vulnerabilities to cyber-attacks of critical energy infrastructure of NATO member states. If a meltdown had happened because of a critical system failure, it would not have just put a permanent end to Burlington's annual Catfish Chasers Tournament. The contamination of the Wolf Creek Generating Station 5,090 acres cooling lake (or Coffey County Lake) would also have meant an environmental disaster (see figure 1), with both human and marine life at stake. If things had gone wrong during this state-sponsored offensive cyber-attack, it could also have left local communities and defense facilities in darkness. The attack showed that smart critical energy infrastructures of NATO member states have never been more vulnerable to cyber-attacks than they are today (even when these systems are physically isolated from the Internet). A greater understanding of energy security at the advent of cyber threats as perceived and managed by CSAs is thus needed to understand the former as a driver of smart and sustainable low-carbon energy transitions and of the later as an impediment.



Source: Author's own representation.
Figure 1: How a cyber-attack could cause a nuclear meltdown and an environmental disaster similar to the Fukushima Daiichi nuclear disaster.

1.2 The challenge to the traditional energy security environment

This dissertation examines how NATO perceives the growing cyber threats to the critical energy infrastructures of the Allies and its emerging role as a guarantor of regional energy security in the cyber domain. It is the culmination of 4 practical years spent defending critical energy infrastructures from malicious cyber activities at the national level in the United States. This was followed by an additional 4 theoretical years, studying the cyber threats to vital energy systems at the regional level within NATO: first, as Visiting Fellow at the NATO Energy Security Centre of Excellence in Vilnius, Lithuania; second, as Eisenhower Fellow and Visiting Scholar at the NATO Defense College in Rome, Italy; and third, as cyber-physical infrastructure subject matter expert during the Systems Analysis and Study 163 (Energy Security) at the NATO Science and Technology Organization in Paris, France.

Over the past decade, Allies have identified a steep increase in cyber activities targeting the critical energy infrastructure sector that NATO military operations rely upon. Directly or indirectly, these malicious cyber activities have the capacity to disrupt the Alliance's logistics and forward operations. In response, at the 2016 NATO Summit in Warsaw, cyberspace was recognized as an operational domain in which NATO military forces must be able to maneuver as effectively as they

do on land, at sea and in the air. Since then, however, Allies have been at odds on what role NATO should play in the security of critical energy infrastructures of the Allies. This decision is not taken lightly by policy makers, because it would fundamentally change the very understanding of NATO's mandate of defense and deterrence. To better illustrate this, it ought to be acknowledged that NATO was founded in response to external state military threats (the Soviet Union) without the right to intervene in internal security matters, where member states maintained the monopoly over the use of force. Compared to the air, land and sea domains, however, in the cyber domain, the distinction between internal and external security threats is harder to ascertain, as cyberspace is not constrained by national borders (although certain physical aspects of it might be located within them).

Compared to the geographic domains, in the cyber domain the lack of coordination among Allies on internal security matters undermines both the unity of the Alliance and its mandate of defense and deterrence. On the former, the lack of coordination between Allies during unilateral actions to defend forward critical national infrastructures could lead to friction when resulting effects also infringe on Allied cyber-physical infrastructures. It could also lead to cyber fratricide, when failure to properly attribute Allied digital personas occurs during these defend forward operations in the cyber domain. On the latter, while most Allies are capable of defending their own critical energy infrastructure in the cyber domain, some remain unable to face the growing number of cyber threats unilaterally, despite commitments of the 2016 Cyber Defence Pledge and the 2018 Brussels Summit to increase national-level capabilities. As a result, NATO was recognized by both Allies and the European Union as an important regional stakeholder that can augment the security of national critical infrastructures in the cyber domain (as seen with the 2016 NATO-EU Technical Arrangement on Cyber Defense). NATO has also established Cyber Rapid Reaction teams that are already equipped to conduct defensive cyber operations in support of member states and partner nations if called upon. Even if political consensus among Allies is missing on the evolving security role of NATO in the cyber domain, NATO is already positioning itself to adapt its defense and

deterrence mandate to the new challenges that it poses.

1.3 Aims and objectives

Regional energy/cyber security integration and synchronization strategies are increasingly becoming a widely discussed topic in regional politics (Evans and Horsthemke 2019; Scholl and Westphal 4/2017, 6). This regionalization of smart energy-cyber security complexes and the belief that interdependence is "more intense between the actors inside such complexes than they are between actors inside the complex and those outside it" (Buzan and Wæver 2003, 4) made the energy-cyber security nexus of high importance for CSAs such as NATO. The overarching research problem for this dissertation is three-fold: 1) malicious cyber activities against vital energy systems that CSAs depend on to achieve their operations and missions are increasing; 2) many states traditionally responsible for protecting these systems in the cyber domain are failing to do so and are looking at CSAs for technical, educational and operational support; and 3) CSAs are positioned to complement national critical energy infrastructure protection (CEIP) in the cyber domain, but this support challenges the traditional role of the CSAs.

This problem presumes a number of research questions:

Research Question 1 (RQ1). What is the CEIP role of CSAs in the cyber domain (i.e. through their official documents)?

Research Question 2 (RQ2). How can CSAs prioritize support to regional energy systems—geo-energy systems—and their prospects, considering

i. the general aim of the CSA;
ii. their conventional/mainstream security challenges;
iii. the security challenges and general policy contexts of their key member states; and
iv. the configuration of their cyber physical systems (in relation to energy resources, infrastructures, and geographies)?

Research Question 3 (RQ3). How are the ends (i.e. defense and deterrence mandate) of

these CSAs likely to change in the future to protect these geo-energy systems from emerging cyber-physical threats?

The aim of this research is to empirically validate 1) the means and ways of CSAs in augmenting national CEIP efforts in the cyber domain, and 2) the feasibility of CSAs to integrate the protection of national cyber-physical energy systems (CPES) into their mandate (the ends). This aim is broken into five objectives:

1. Objective 1. Synthesize how energy security, cyber security and CSAs are perceived, defined, and framed in the contemporary security environment;
2. Objective 2. Produce a methodology for prioritizing protection of regional energy systems—geo-energy systems—and their prospects in the cyber domain;
3. Objective 3. Apply the proposed methodology to a CSA that is already invested in protecting CPES in the cyber domain;
4. Objective 4. Empirically validate the means and ways of CSAs in augmenting national CEIP efforts in the cyber domain by
    i. identifying patterns or clusters of cyber security issues, policies, and discourses relevant to CSA defined geo-energy systems; and
    ii. explaining these patterns or clusters in terms of geo-STEPE (Elias G. Carayannis 2011) policy contexts: geo-socio-cultural, geo-technological, geo-economic, geopolitical, and geo-ecological; and
5. Objective 5. Interpret and extrapolate results to validate the feasibility of CSAs to integrate the protection of national cyber-physical energy systems (CPES) into their mandate (the ends).

1.4 Approach/methodology

The theoretical framework of this research builds on the primarily realist and liberal

frameworks used by existing energy and cyber security literature, which focus largely on the state and systemic (global) levels of analysis (Kenneth Neal Waltz 2001) when studying cyber threats to critical energy infrastructure. This will be accomplished by looking at background realist and liberal theories within the context of energy and cyber security assessments, then by introducing the regional security complex theory (Buzan and Wæver 2003, 4), RSCT, and the securitization theory of energy supply chains. A new explanatory framework is then developed for understanding how CSAs will reshape geo-energy systems and their prospects at the advent of new technological risks, such as malicious cyber activities. Interviews with energy and cyber security scholars and practitioners within their geo-energy systems will then be used as methods to refine this new framework and achieve the aims and objectives of this research.

1.5 Structure

A Literature Review of existing energy and cyber security assessments and of regional securitization theories needed to develop a theoretical framework that will answer this study's questions follows this introductory chapter. This theoretical framework for conceptualizing the securitization of cyber-interconnected geo-energy systems during smart and sustainable low-carbon energy transitions is introduced in the third chapter—the methodology of the thesis, which also discusses the limitations of the research. Chapter four will contain the results of the study and is followed by the interpretation and extrapolation of these results in chapter five. Finally, chapter six will contain a summary of findings, conclusions, and recommendations of the research, as well as identify areas that need further research.

Chapter 2

Literature Review

Since the early 20th century, identifying energy security threats and vulnerabilities has slowly emerged as a key priority on the policy agendas of national governments (Chester 2010/2, 887; Sovacool et al. 2011, 5852) and international organizations (IOs) (Elam et al. 2003); and more recently has risen high on the agenda of CSAs (Ciută 2010, 129; Mälksoo 2018; Monaghan 2008; Øverland et al. 2016; Scholl et al. 2016). While the term 'energy security' is currently widely used on the agendas of CSAs, and while there is an extensive body of academic literature that addresses the securitization of energy supply chains at national and sometime regional levels, there is currently no consensus on the precise interpretation of energy security by CSAs (Monaghan 2008). With the rise in malicious cyber activities against cross-border critical energy systems over the past decade, there is also no consensus on if and/or how CSAs should secure these systems in the cyber domain.

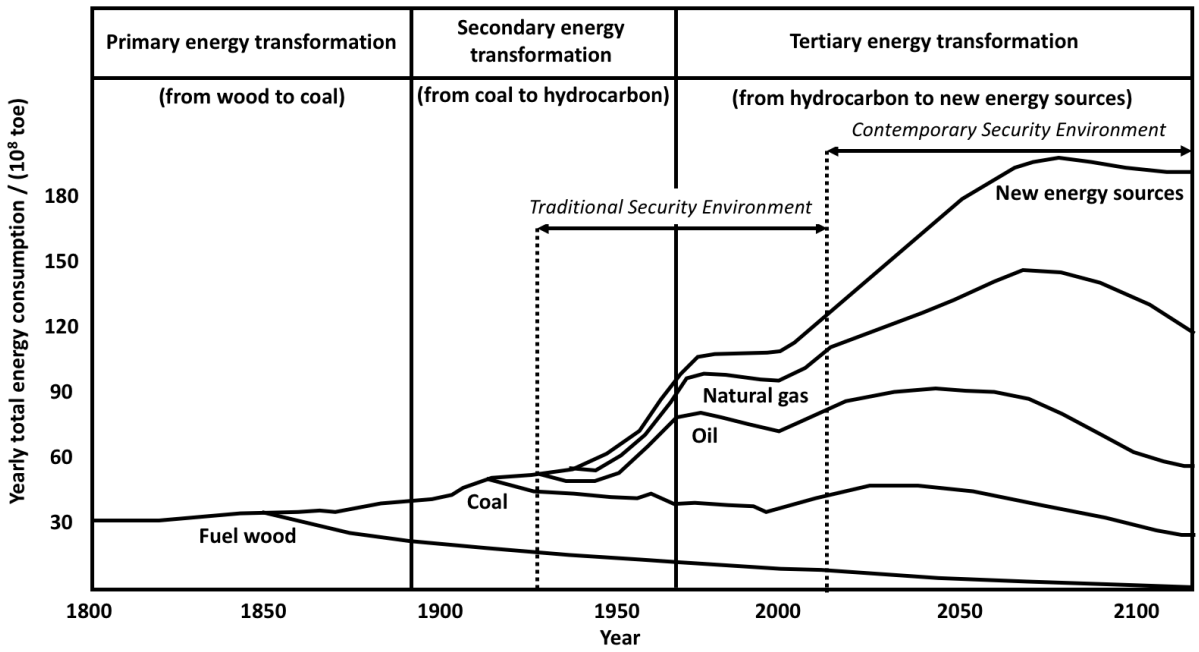
The focus of this chapter is to address the lack of interaction in existing literature between the scientific analysis of cyber vulnerabilities of geo-energy systems and policy narratives of CSAs about cyber risks and response capacities. To accomplish this, the literature review is structured into three parts. The first part focuses on the complexity of energy security assessments both within the traditional and contemporary body of literature, providing an understanding of generic energy security analysis theories. The second part introduces the body of literature concerning the digital transformation for energy transformation theories. Finally, the third part provides a theoretical background on the specific nature of CSAs, and their growing critical energy infrastructure protection (CEIP) role, particularly in cyberspace, during smart and sustainable low-carbon energy transitions. This literature review concludes with a discussion on the challenge of defining and assessing cyber security of energy systems by CSAs in existing security policy studies and literature. This achieves Objective 1: synthesize how energy security, cyber security and CSAs are perceived, defined, and framed in the contemporary security environment.

2.1 Energy security during smart and sustainable low carbon energy transitions

In a century of rapid urbanization (Shahidehpour, Li, and Ganji 2018), modern life and human security are dependent on both the "robustness and resilience of energy systems" (Cherp et al. 2012; Narula 2019). This section discusses the perceptions of energy security threats and vulnerabilities of vital energy systems in both traditional and contemporary scholarly literature, and traces the multidimensional and polysemic nature of energy security from national security/geo-STEPE perspective to an existential field in itself. This historical narrative is needed to provide an understanding of the generic energy security analysis frameworks and the reflexive rationality—where "the ways by which we try to solve our problems [...] become a theme and a problem in itself" (Dunn Cavelty and Mauer 2009, 135)—behind them.

2.1.1 A narrative summary of 'traditional' energy security thought

Unrestricted access to energy supplies has been of little importance to national security strategists of the 19th century, despite the fact that coal fueled the industrial revolution (Cheema 2011), resulting in record economic growth. In 1912, however, Sir Marcus Samuel—founder of Royal Dutch Shell—persuaded the British Royal Navy that transitioning from coal to oil-ran engines would strengthen its maritime power (G. G. Jones 1977). The new diesel-operated British Royal Navy fleet has proven its superiority during World War I, when it defeated the German High Seas Fleet (Vego 2008). Soon, all industrialized countries of the early 20th century replaced their steam vessels—operated by domestic coal—with navies operated by imported oil that often came from subservient colonies. The national security of these states became dependent on the robustness—"the long-term access to" (Deane et al. 2015)—energy supplies (see figure 2); defining the traditional energy security threats in scholarly literature until the end of the Cold War (Yergin 2006).



Source: Adapted from (C. Zou et al. 2016, 8).
Figure 2: Technology transformation to energy transformation outlooks.

Unlike coal, access to oil quickly became a vital component of national security (Crane et al. 2009). Consequently, its proven economic—due to the growth of the affordable automobile industry—and military—with "the life of the Axis" depending on foreign oil (Jewell 2013)—value transformed the oil supplies into strategic targets during World War II. In 1941, for example, an oil embargo against Japan in response to its incursion into China became the first recorded time that oil was successfully used as an instrument of coercion: the United States Navy restricted 80 percent of Japan's oil supply (Anderson 1975). This strategy of denying enemies access to oil supplies also led to significant loss of lives: in 1943 Operation Tidal Wave—a failed bombing mission of Romania's oil fields—resulted in the loss of 53 U.S. aircraft and the death of their 660 crew members (Donnini 2003).

While most of the body of literature on pre-World War II addresses the vulnerabilities of oil solely from a state-level of analysis, the post-war body of literature on traditional energy security threats can be analyzed from both state and systemic-level perspectives (Raven and Verbong 2009). As supra-national alliances between oil suppliers—Organization of Petroleum Exporting

Countries, OPEC—and oil consumers—IEA—are created, Jewell notes that during this period "new concerns do not replace old ones, but rather add to them" (Jewell 2013, 7). Jewell classifies these threats into two categories: threats that affect the robustness of energy system (a concern renewed by the peak of the U.S. oil production in the 1970s), and the emergence of threats (disruptions resulting from attacks or accidents) in the 80s to the resilience of these geo-energy systems.

Despite these rising concerns about secure access to oil supplies, by the mid-20th century oil replaced coal as the energy of choice within the industrialized world (Fletcher 1975). The latter's dependency on oil increased to such an extent, that by 1967 "disruption of oil supplies from Saudi Arabia, Iraq, Kuwait, and Libya for 3 months would have cost the United Kingdom £1.2 billion, almost crippling its economy" (Thorpe 2007, 215). To exacerbate these concerns, the attention of policymakers in the 1970s also shifted to the scarcity of oil and to the possibility that national oil reserves might actually run out at one point in the future (Bentley 2002; Hubbert 1956). As the threats to energy security compounded during the 1970s—threats exacerbated by the Arab oil embargo (1973-1974) and the replacement of oil and coal in electricity generation with nuclear power and natural gas (Olah 2005)—this led to a desperate need for systemic (supra-national) entities that could analyze the robustness of energy systems (Sweeney and Weyant 1979) and enforce the directives of a free market ideology (Keohane 1978).

Other academic literature divides the intellectual history of the post-world-war traditional energy security threats into three phases seen from a state-level perspective (M. Jones, Hope, and Hughes 1990): (1) the 'Good Old Days' (1965-1976) characterized by the post-World War II "transition from a single-fuel (coal) to a multi-fuel (coal, oil, nuclear and gas) energy economies" (M. Jones, Hope, and Hughes 1990, 919), (2) the 'Confusion and Change' (1976-1981) period brought upon by the global fear that interest alignment of OPEC nations would result in higher oil prices, and (3) the 'Apparent Consensus' (post 1981) period dominated by the need for energy diversification, and by increasing coordination among energy importing countries. These

oversimplified classifications fail to address, however, the systemic level (global or regional) implications of energy and human security concerns, and do not take into account the multitude of threats that may affect the resilience of energy systems.

2.1.2 The contemporary thinking on energy security

According to Daniel Yergin—the "father of modern energy security studies" (Jewell 2013, 7)—the intellectual history of global energy security until the end of the Cold War was almost exclusively dominated by the security of oil supplies (Yergin 1988). Access to energy sources in the post-Cold-War market economy "depends on a complex system of global markets, vast cross-border infrastructure networks, a small group of primary energy suppliers, and interdependencies with financial markets and technology" (Chester 2010/2, 887). With the 1980s bringing into the limelight threats to the resilience of energy systems—such as terrorist attacks and blackouts—the contemporary literature on energy security threats witnesses the emergence of three schools of thought to address short-term transitory disruptions of energy supplies (shocks) and enduring long-term pressures to energy systems (stresses): sovereignty (Westphalian), robustness, and resilience.

These three energy security perspectives "have their roots in separate academic disciplines: political science (the sovereignty perspective), natural sciences and engineering (the robustness perspective), and economics (the resilience perspectives)" (Cherp and Jewell 2011/9, 207). They also represent top-down points of view from government, university, and industry (GUI) sectors, which differ in focus and response strategies (Elias G. Carayannis and Rakhmatullin 2014). Understanding these three perspectives is relevant to recognizing the significance of CSAs to enhancing national, regional, and global energy security in the 21st century.

<u>The sovereignty school of thought (defense comes first):</u>

As discussed earlier, the sovereignty school of thought is rooted in international security

and international relations theories, and thus takes a neorealist approach to analyzing the ends, ways, and means of energy security (O'Sullivan 2013). The sovereignty perspective is concerned with intentional actions of external stakeholders such as hostile countries (He and Qin 2006, 101), terrorist organizations (Toft, Duero, and Bieliauskas 2010), or other overly powerful actors with both capacity and willingness to abuse their position of influence at the detriment of the state (Cherp and Jewell 2011/9, 206). Nations remain concerned with the capacity of external stakeholders to generate long term economic stresses—by casting control over geo-energy systems—or short-term physical shocks—realized through deliberate attacks of critical energy infrastructure (CEI) to achieve political ends. Within this defense-centric structure, energy security is "capable of holding multiple dimensions and taking on different specificities depending on the country (or continent)" (Chester 2010/2, 887).

Risk-minimization strategies presented by the sovereignty literature include "switching to more trusted suppliers or weakening a single agent's role through diversification, substituting imported resources with domestic ones, and casting military, political and/or economic control over energy systems" (Cherp and Jewell 2011/9, 206). With the interconnectedness of energy systems, however, casting control over them beyond national borders is not always possible, making regional alliances, and particularly CSAs, very relevant to energy security as viewed from the lenses of the sovereignty perspective.

The robustness school of thought (democracy comes first):

The robustness school of thought focuses on the capacity of energy systems to react to stresses of geo-energy security systems as well as long-term changes in the economic or geopolitical environment. The robustness energy strategies—"that is, strategies that would allow policy makers to anticipate a shortfall in supply and to apply appropriate energy risk management instruments" (Van der Linde 2007, 51)—thus accommodate for secular stresses of geo-energy systems. These include "growth in demand, scarcity of resources, aging of infrastructure, technical failures, or

extreme natural events" (Cherp and Jewell 2011/9, 207). It also implies that robust nation states "are allowed to choose from primary energy sources at cost-oriented prices, without being hindered in their choice by economic or geopolitical constraints on energy resources and infrastructures" (Gracceva and Zeniewski 2014, 5).

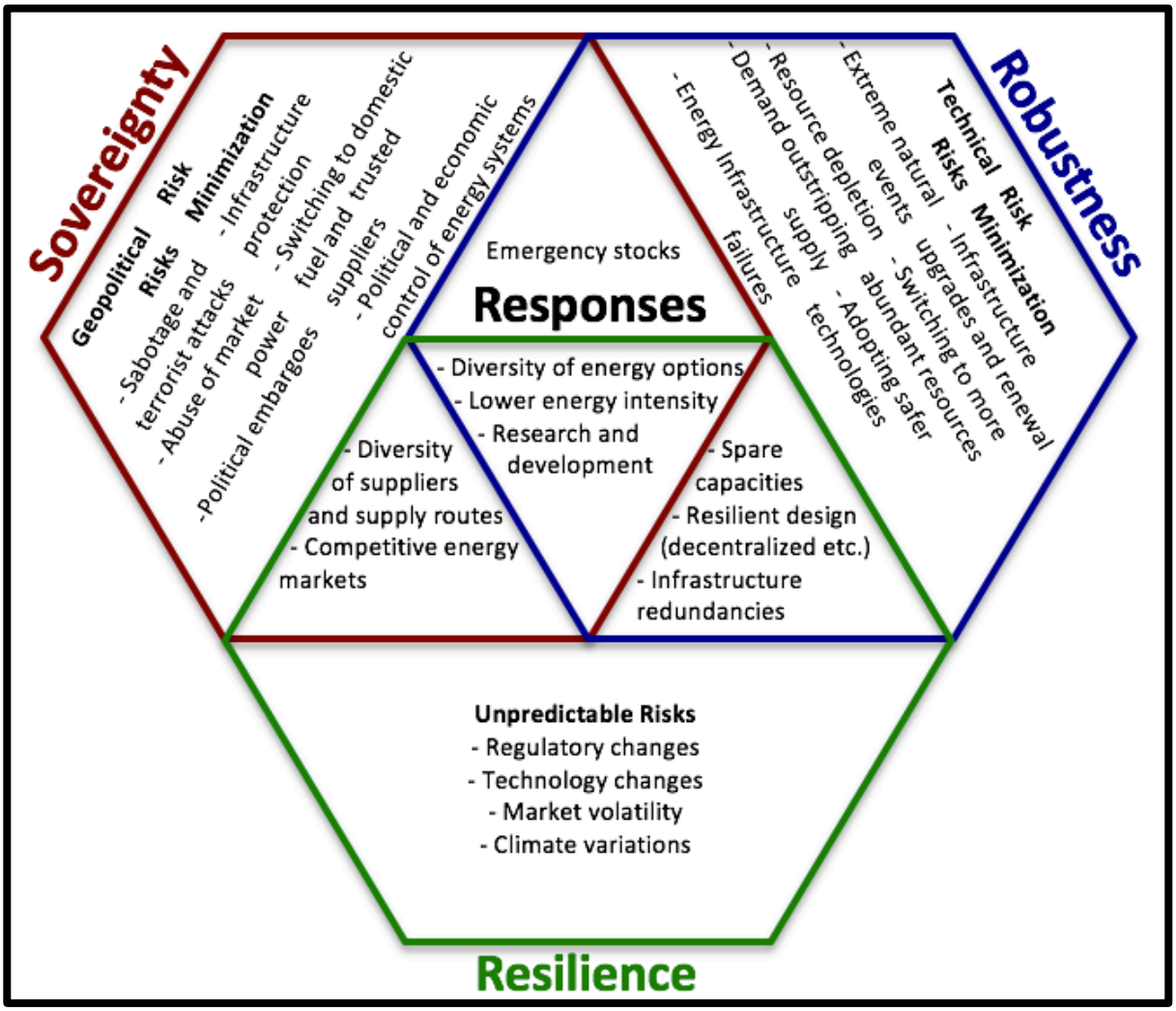
Minimizing the risks of long-term pressures to energy systems—within a robust, democratic construct—encompasses "upgrading infrastructure, switching to more abundant energy sources, adopting safer technologies, and managing demand growth" (Cherp and Jewell 2011/9, 207). Within emerging geo-energy systems, however, switching to more abundant energy sources and adopting safer technologies is hard to realize without the peaceful cooperation between neighbors that are part of the same systems. Collective security—through which the bolstering of regional stability and security is realized—becomes thus a prerequisite to national robustness of energy systems.

The resilience school of thought (development comes first):

The resilience school of thought stresses on the energy systems' response capacity to "sudden and transient shocks, such as the interruption of a major supply source" (Gracceva and Zeniewski 2014, 5). Resilience energy strategies thus accommodate for transitory shocks such as "regulatory changes, unforeseeable economic crises (or booms), change of political regimes, disruptive technologies, and climate fluctuations" (Cherp and Jewell 2011/9). The ability of a geo-energy system to resist to—or bounce back from—shocks is determined by its structural (both physical and abstract) characteristics (Gracceva and Zeniewski 2014, 5). Because of this, minimizing risks of short-term transitory disruptions of energy supplies focuses on development of geo-energy systems that offer flexibility, adaptability, and diversity; ensuring protection through spreading risks and preparing for surprises (Cherp and Jewell 2011/9).

Within this tri-dimensional GUI construct, the value of sharing information across borders is vital to building sovereignty, robustness, and resilience centric energy strategies (see figure 3).

Locally, nationally, regionally, and globally, these strategies rely on building partnership capacity and on equipping and training specialists to address energy security shocks and stresses in a multinational environment. CSAs emerge as vital institutions with the required framework to share this vital intelligence and with the capabilities necessary to insure protection of vital energy systems. Sharing of information could thus be added as a critical response mechanism in Cherp & Jewell's model.



Source: Adapted from (Cherp and Jewell 2011/9)
Figure 3. Cherp & Jewell's three perspectives on energy security.

2.1.3 The emerging climate change risks: framing and conceptualizing energy security during smart and sustainable low-carbon energy transitions

More recently, the climate change threat has influenced nation states, IOs, and regional blocs alike to redefine energy security to also incorporate the environmental (clean) perspective within the definition of energy security. The IEA, for example, added to the energy definition that it's long term prospects must be in line with "environmental needs" (IEA 2019b). As such, energy security can no longer be viewed outside of the construct of smart and sustainable low-carbon energy transitions. In practice, we can also see that regional blocs such as the European Union (EU) are adopting the IEA definition (see the EU's Clean Energy for All Europeans initiative). The regional protection of critical geo-energy systems "on the basis of strategic assessments and contingency planning" (Encke 2015), as well as the robustness and resilience of energy systems is now viewed first and foremost from the lenses of global warming mitigation at all levels of analysis. Given the regional interconnectedness of energy systems, this evolution has the potential to significantly affect the operations and future of CSAs during smart and sustainable low-carbon energy transitions. To date, however, no framework was constructed for the assessment of energy security during smart and sustainable low-carbon energy transitions by CSAs. Furthermore, outside of the EU, regional energy security has only been considered for arbitrarily defined regions, without reference to actual energy policies (i.e. in a positivist fashion).

Before any regional framework for energy security during smart and sustainable low-carbon energy transitions can be built, a generic understanding of existing energy security frameworks is required. According to Cherp and Jewell, an energy security framework has 5 stages (Cherp and Jewell 2013, 150):

1) Defining energy security for the purpose of the assessment;

2) Delineating vital energy systems;

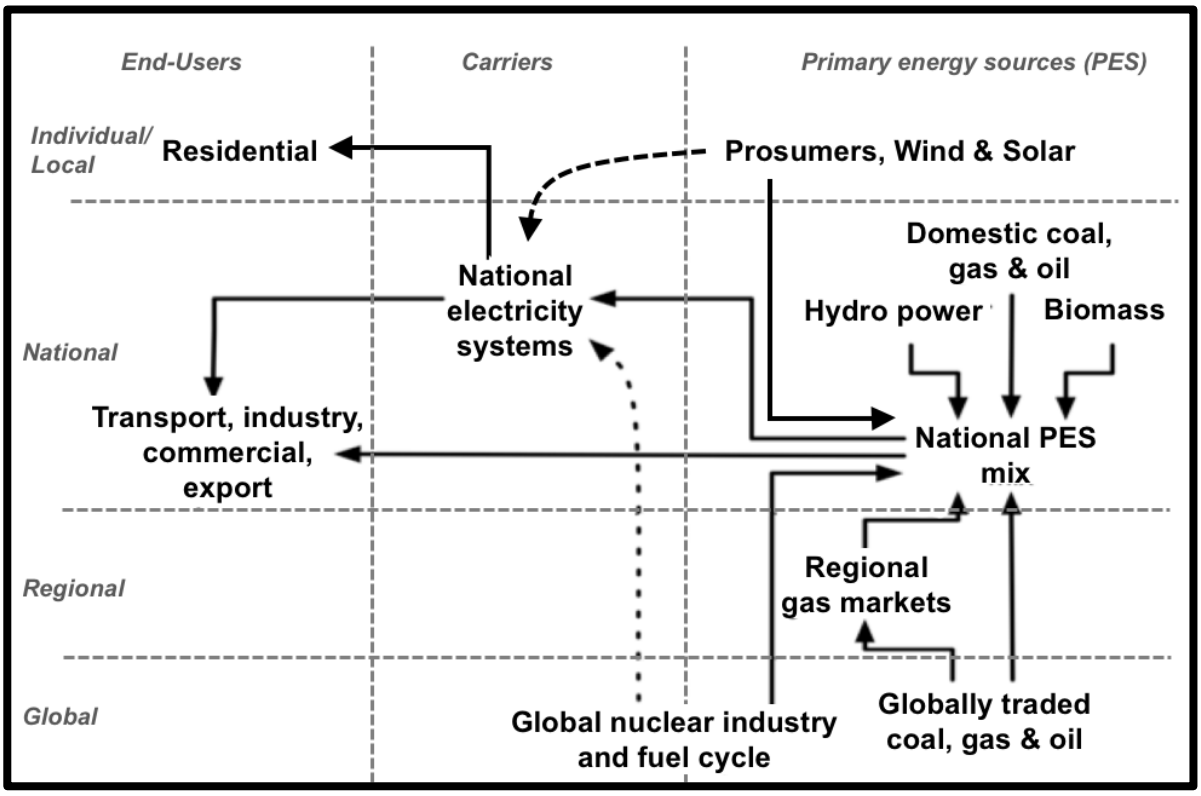
3) Identifying susceptibilities of vital energy systems;

4) Selecting and calculating indicators for these vulnerabilities; and

5) Interpreting the indicators to answer the questions posed by the assessment.

What to protect: delineating vital geo-energy systems

A vital energy system is "a system which is essential for supporting critical societal functions. Serious disruptions of a vital energy system may lead to social, political or economic instability and thus is a matter of [energy] security" (Jewell 2013, 64). Examples are "transport fuels, heat and electricity for residential and commercial sector, energy for industry, and energy export revenues" (Cherp and Jewell 2011/9, 210). Vital energy systems in present energy scenarios (see figure 4) are categorized by geographies (in local, national, regions, global markets and flows), primary fuels (oil, gas, coal, renewables, etc), secondary energy (oil products, liquids, electricity), and end-use sectors (such as transportation, industrial, and buildings sectors) (Jewell 2013, 65). The increase in cross-border infrastructure networks and in energy interdependencies within regional markets caused the emergence of geo-energy spaces where intra-regional energy integration and unique trade relationships and transportation routes between regional producers and consumers strongly influence national energy security strategies (Mañé-Estrada 2006, 3785). Within future energy scenarios of these spaces, CSA energy security strategies will also have to incorporate regional energy models that better explain the links between geo-energy systems. This is particularly the case for CSAs that own CEI crossing national boundaries.



Source: Adapted from GEA (Cherp et al. 2012).
Figure 4. What to protect: vital energy systems.

From what threats to geo-energy systems to protect: a search for regional vulnerabilities

There are two fundamental methodological choices identified by academic literature with regards to vulnerabilities of energy security systems (Cherp and Jewell 2013):

1) specific (physical threats to oil, natural gas, coal, electricity, nuclear power, wind, solar, hydropower, geothermal and biomass resources that typically fall under the responsibility of nation states) vs. generic level of analysis (dealing with both physical and economic risks and lack of resilience of vital energy systems); and

2) perceptions—cultural constructs or "emotional responses that people can have to energy landscapes" (Bridge et al. 2013)—vs. facts.

Back to the three GUI perspectives (sovereignty, robustness, and resilience)

As identified earlier in this chapter, there are two distinct framings of temporalities: short-

term "shocks" and long term "stresses" (Stirling 2014). "Shocks" refer to short-term transitory disruptions of energy supplies in an otherwise stable energy security environment, and "stresses" refer to enduring long-term pressures to energy systems, reflecting underlying shifts in the conditions needed for them to operate most efficiently (this may include enduring trends in the global economy, technological developments, etc.). Identifying the risks and resilience of regional vital geo-energy systems requires a deeper understanding on what causes these shocks and stresses at the regional level.

Scholarly literature associates long term regional risks to vital energy systems with long term potential disruptions of energy supply (or stresses) caused by stakeholders that are part of the region (such as unreliable energy companies or regional alliances that have the power to enforce political embargoes), overly powerful stakeholders that have significant regional influence, or other factors such as "growth in demand, scarcity of resources, aging of infrastructure, technical failures, or extreme natural events" (Cherp and Jewell 2011/9, 207).

The literature on the robustness perspective during smart and sustainable low-carbon energy transitions refers to the ability to respond to enduring long-term pressures to geo-energy systems (or stresses) such as:

a. political embargoes and the abuse of market power: the ability to assert political, military, economic, and/or social control over energy systems; diversification; trusted suppliers; ability to switch from imported energy supplies to domestic supplies;
b. growth in demand: ability to manage demand growth;
c. scarcity of resources: ability to switch to more abundant energy sources;
d. aging infrastructure: ability to upgrade infrastructure;
e. technical failures: adopting safer technologies; and
f. extreme natural events.

Both long-term pressures to energy systems (or stresses) and short and medium term unexpected disruptions of energy supply (or shocks) are of increasing interest within regional geo-

energy spaces. However, while most long-term pressures to energy systems listed above have been typically addressed at national levels, or through economic arrangements, of particular interest to this research is the regional securitization of short and medium term external risks. While these may include "regulatory changes, unforeseeable economic crises (or booms), change of political regimes, disruptive technologies, and climate fluctuations" (Cherp and Jewell 2011/9), at both the national and regional level they are also associated with unexpected disruptions of energy supply (or shocks) temporarily caused by external actors or factors. This includes a deliberate physical attack (explosives, stand-off weapons, and malicious control of equipment) or a cyber-attack against CEI (power grids, pipelines, pump stations, storage facilities, block valve stations, control centers, etc.) from either hostile countries or terrorist organizations and affiliates. "The security of energy infrastructures against deliberate attack has become a growing concern. Therefore, the context within which energy is supplied and used has evolved well past the paradigm that has led to the current physical energy infrastructure and associated institutional arrangements" (Farrell, Zerriffi, and Dowlatabadi 2004, 460). These fears have led to the securitization of energy and the elevation of CEIP on the geo-STEPE agendas of nation states and regional CSAs.

Regional energy resilience implies thus the ability of the region to respond to unexpected temporary disruptions of energy supply (or shocks). Traditionally, responding to attacks to CEI required flexibility, adaptability, and diversity of energy supplies. Today, however, they also require intelligence sharing (to predict and preempt future attacks), strong boundary protection capabilities (penetration resistance, allowing capacity of repelling attack to critical infrastructure originating from outside the defensive perimeter), and agile defense capabilities (resilience of critical infrastructure information systems, allowing operation of critical infrastructure during an attack once defensive perimeter has been breached). In a world where defense cuts are the norm, nations can no longer respond to these threats unilaterally, without cooperation among regional allies connected to the same networks. Building regional cooperative security partnerships, however, "involve sharing intelligence, rapid repair capacity, and technical assistance" (Nye 1980, 149).

By what means to protect: the securitization of energy supply chains

Whereas in the past powerful nation states have been entrusted with the protection of vital regional energy systems (see the U.S. Carter doctrine) in the future this task may be carried out also by regional alliances with the capacity to counterbalance the military and economic power of any one state threatening to destabilize the region. This places energy security at the regional level within a collective energy security construct, that is, "within the social-constructivist framework of securitization. [This construct] necessitates emergency measures through extraordinary means [to protect from existential] threats socially constructed through a reflexive and contextualized process" (Fischhendler and Nathan 2014), and that require regional mobilization of resources for collective action. The spreading of this confrontational view of security has been described in academic literature as 'securitization.'

According to Buzan's securitization theory, "a policy problem becomes a security issue if an agent manages to cast it as an 'existential threat', or a 'supreme priority' which requires treatment and intervention by extraordinary means" (Leung et al. 2014, 2). At the state level, an energy policy problem is an energy security issue "if it is presented and perceived as affecting the stability (and in critical situations, the survival) of a nation, the 'functioning' and 'continuity' of the economy or the realization of 'major national values and objectives'" (Leung et al. 2014, 2), and "requiring emergency measures and justifying actions outside the normal bounds of political procedure" (Trombetta 2008, 589). Securitization rhetoric must thus "identify an energy supply chain that can be portrayed as (a) critically important, (b) highly vulnerable and (c) possible to protect" (Leung et al. 2014, 2). Within this rhetoric, "the logic of compensation breaks down and is replaced by the principle of precaution through prevention" (Beck 2006, 334), thus, allowing the state to alter or silence the existing economic structure within the state and/or its people's way of life in response to energy threats perceived as more urgent by the political establishment.

Because securitization results from failure to deal with threats to energy systems "as normal

politics" (Roe 2012) the securitization process at the regional level must fit within a regional/collective security construct or a series of regional security agreements with the power to protect from regional threats that cannot otherwise be addressed by a single nation (such as mitigating the negative influence of unreliable producers and/or transit regions). Nations are thus increasingly expecting CSAs to devise strategies that address existentialist energy security threats at the regional level. Because energy security can no longer be defined outside smart and sustainable low-carbon energy transitions constructs, this also places the CSAs in the unexplored terrain of addressing change mitigation.

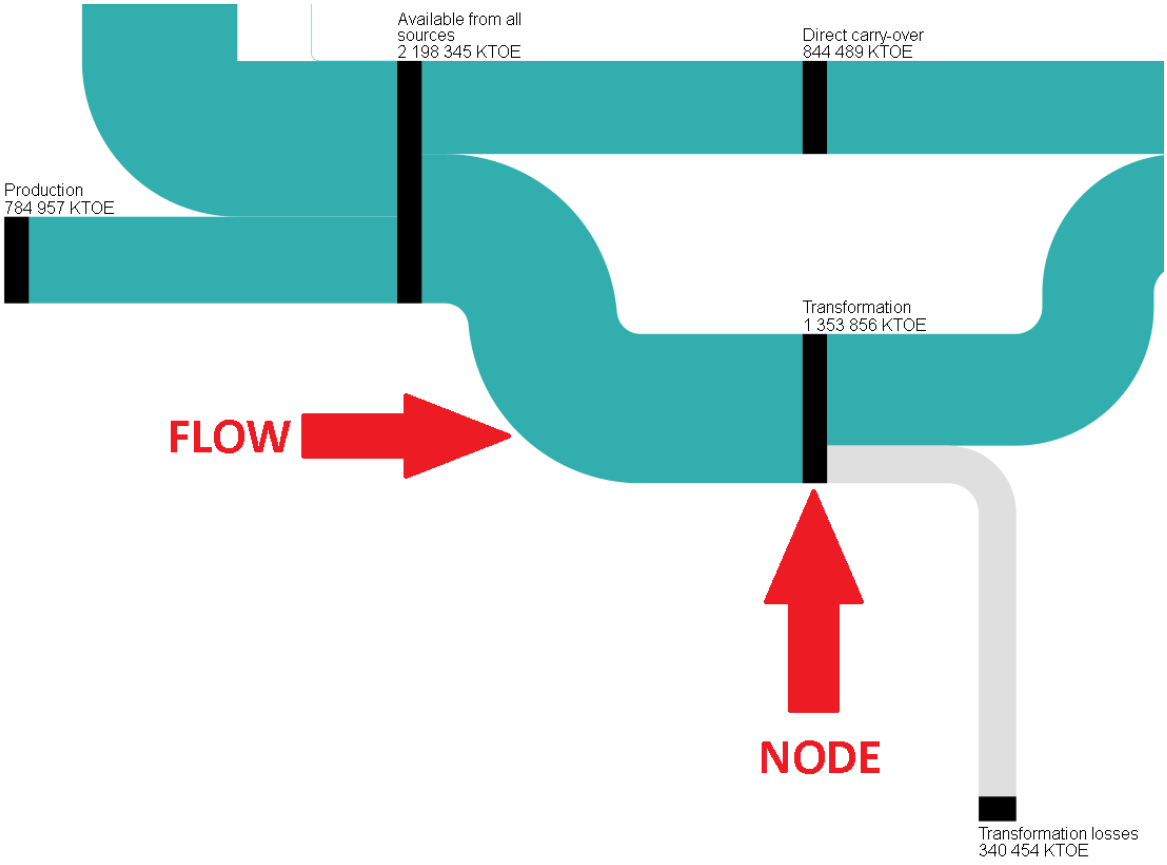
New Frameworks of Analysis: MOSES and GEA

In recent years new frameworks of analysis were developed to support and complement national-level studies with country-specific indicators that allow "for international comparison and interpretation of national energy security challenges" (Jewell 2011, 1). To supplement this effort, the IEA's Model of Short-Term Energy Security (MOSES) tool was developed for "drawing common strategies and responses, as well as for facilitating exchanges of information and policy [dialogues on common energy security priorities] among countries" (Jewell 2011, 1) using an energy systems approach (see figure 5). This approach is significant because it clearly differentiates between the production and consumption of dirty vs clean energy sources; and is in line with the environmental long term outlooks of the IEA.

Similarly, the International Institute for Applied Systems Analysis's Global Energy Assessment (GEA) was developed "to identify, map, and explain the varying conditions of energy insecurity encountered around the world" (Cherp, Jewell, and Goldthau 2011). Yet, while the research acknowledges that "energy security issues have a strong regional dimension because countries located in geographic proximity often experience similar conditions with respect to access to energy resources and the structure of energy use" (Cherp, Jewell, and Goldthau 2011), the study does not go beyond a brief description of major energy security concerns by continent (Africa,

Europe, North America, Asia, Latin America and the Caribbean).

The securitization theory—which was primarily developed for the nation state—continues to favor the state level of analysis within discourses of the new frameworks. Overall, MOSES groups together individual IEA countries based on risks and resilience capacities rather than geographic considerations, while the GEA "uses simplification and aggregation, necessary for mapping [national energy systems security] concerns, rather than producing a single universal energy security index" (Cherp, Jewell, and Goldthau 2011). Neither focus on developing energy security indexes that apply regionally within the context of smart and sustainable low-carbon energy transitions.



Source: EUROSTAT.

Figure 5. Examples of Nodes and Flows in Sankey Diagram using the MOSES energy systems approach (Jewell 2011, 1).

2.2 Digital transformation for energy transformation

In the traditional security environment, critical infrastructures were defined as physical networks and/or systems whose prolonged disruption or destruction could cause "a debilitating impact on the defense or economic security" (Moteff, Copeland, and Fischer 2003, 2). CEI thus referred to the physical vital energy systems whose prolonged disruption or destruction would hurt national security and economic stability. CEI vulnerabilities were exposed primarily to physical (localized) threats, where the perpetrator's physical presence at the place of the attack was a requirement. Climate change and digital transformation have significantly expanded the designation of what is critical in the energy field. As seen in the previous section, with the emergence of climate change threats, the energy security definition expanded to include environmental considerations. Similarly, CEI now includes *interdependent* physical networks and/or systems whose prolonged disruption or destruction could cause environmental disasters. With the digital transformation of the 21st Century, threats to energy systems are also increasingly digital in nature, coming from remote points of origin (in the cyber domain).

A cyber-attack is defined as "an attack on a computer and network system, consisting of computer actions (e.g., remote or local connection, computer file access, program execution, etc.) to compromise the secure operation of the computer and network system" (Chi et al. 2001, 320). These cyber-attacks do not threaten only information technology (IT) systems (data); but also, operational technology (OT) physical nodes. Information technology refers to "automated systems for storing, processing, and distributing information" (van den Hoven et al. 2018). Operational technology refers to "computer-controlled physical processes such as industrial control systems (ICS) or other types of control systems" (Bryant 2016, 7). An ICS "is a computer-based system that monitors and controls physical industrial processes" (IBM 2015, 3). The interconnectedness of the CEI makes the cyber threats against ICS components particularly dangerous, often, as dangerous as the threats that are purely physical in nature. Compared to IT vulnerabilities, attacks against ICS can cause blackouts (Alderson and Di Pietro 2016, 339), explosions (Huang et al. 2009), oil spills

(Wittkop 2016), a nuclear meltdown (Buchan 2012), and other environmental disasters that can even "destroy the marine habitat" (Wadhawan and Neuman 2015).

2.2.1 What to protect? An anatomy of OT vulnerabilities to CEI

OT vulnerabilities are hard to identify. Of those that are identified, not all are shared with the general public before a patch/fix has already been developed. This makes these vulnerabilities particularly hard to research and categorize in an academic setting. In 2015, for example, vulnerabilities were identified in ICS components (including components for supervisory control and data acquisition, SCADA) of 55 different manufacturers; particularly Siemens and Schneider Electric (Andreeva et al. 2016, 4). SCADA "is a system operating with coded signals over communication channels to provide control of remote equipment, typically using one communication channel per remote station" (IBM 2015, 3).

Disruptions of CEI by cyber vulnerabilities

Cyber vulnerabilities of ICS components are not just theoretical, but have already caused disruption of CEI in the past:

- In June of 1982, a state-built Trojan horse "caused a major explosion [with] the power of a three-kiloton nuclear weapon" during a routine pressure test of the Trans-Siberian gas pipeline (Byres and Eng 2009, 58). The ICS used "to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds" (Reed 2005).
- In December of 2002, during a general strike, "hackers were able to penetrate the SCADA system responsible for tanker loading at a marine terminal in eastern Venezuela, [preventing] tanker loading for eight hours" (Byres and Eng 2009, 58).

- In January of 2003, the 'Slammer' worm disabled a safety monitoring system at the Ohio's Davis-Besse nuclear power plant "for nearly five hours" (Poulsen 2003) While the payload was benign, consequences could have been devastating if intent was to cause a nuclear meltdown (Moore et al. 2003).
- In August of 2003, an electric power blackout affected 50 million people for up to 4 days in "most of New York state as well as parts of Pennsylvania, Ohio, Michigan, and Ontario, Canada" (Andersson et al. 2005, 1922). Only one month later, in September, 4 million people lost power in Sweden and Denmark (Andersson et al. 2005, 1922), and another blackout affected more than 56 million people for up to 48 hours between Italy and parts of central Europe. The proximate causes of these blackouts were determined to be "a cascading sequence of events involving line outages, overloading of other lines, malfunctions of protection systems, power oscillations and voltage problems, and system separation and collapse" (Yamashita et al. 2008, 857); but the underlying cause was arguably "an over-reliance on computer-based decision support systems" (C. W. Johnson 2007).
- In March of 2008, the Edwin Irby Hatch Nuclear Power Plant in southeastern United States was "forced into an emergency shutdown for 48 hours, after a software [designed to synchronize data on both the business system computer and the control system computer] was installed on an office computer" (Wong et al. 2010, 18).
- In June of 2010, the 'Stuxnet' worm caused the fast-spinning centrifuges of an Iranian nuclear facility at Natanz (Farwell and Rohozinski 2011, 23) "to tear themselves apart" (Kushner 2013). While the state-sponsored preventive cyber-attack slowed down progress of the Iran's nuclear program, the effects of a nuclear meltdown could have been disastrous also for the environment.
- In December of 2015, a multi-stage, sophisticated cyber-attack against a power plant disabled power generators that served over 700,000 people in Ukraine (Alderson and Di Pietro 2016, 339). Seven 110 kV and twenty-three 35 kV substations "were disconnected

for three hours [while cyber-attacks against] the distribution grid forced operators to switch to manual mode" (R. M. Lee, Assante, and Conway 2016).

- In June of 2017, the NotPetya cryptovirus affected the electronic radiation monitoring systems at the Chernobyl Nuclear Power Plant, "which forced employees to switch to manual radiation monitoring and control systems to prevent irreversible consequences" (Tirranen 2018, 549).
- In May of 2017, a cyber-attack on a U.S. nuclear facility near Burlington, Kansas also occurred; although the nature of the attack is unclear (Broersma 2017; Riley, Dlouhy, and Gruley 2017).
- In August of 2017, a cyber-attack against a petrochemical plant in Saudi Arabia "was meant to sabotage the firm's operations and trigger an explosion" (Perlroth and Krauss 2018).

Cyber vulnerabilities and the interdependency of CEI

During the second industrial revolution, the CEI networks were decentralized, with local energy suppliers connected directly to consumers through local distributors. Disruptions of energy suppliers or distributors resulted in local blackouts. During the third industrial revolution, in order to minimize these local blackouts, CEI networks became interconnected, supporting each other. As seen with the 2003 blackouts in North America and Europe, today, these interconnections cross national borders, and local CEI failures could have disastrous regional implications. These interdependencies made local, national, and regional CEI cyber vulnerabilities of interest not only to local and national governments, but also to regional economic alliances and CSAs.

As seen from the short list of cyber vulnerabilities to CEI, failure of ICS can happen 1) at the primary energy source (PES) level (as seen with most recent failures of—or attacks against—the ICS of nuclear power plants or the 2017 cyber-attack against a petrochemical plant in Saudi Arabia); 2) during transportation of PES to carriers, or Power Generation Systems (see the 1982 cyber-attack against the Trans-Siberian gas pipeline); 3) at the carriers level (as seen with the 2015

cyber-attacks against a power plant in Ukraine); or 4) during transportation from carriers to end-users (as seen with the electric power blackouts of 2003). Given the interconnectedness of CEI across borders, the prioritization of which ICS components must be protected will differ from nation to nation and from national to regional levels. Because of this, to date, there is no agreement as to which CEI should be protected against cyber-attacks and by whom.

There are currently multiple empirical studies available at both national and regional levels tackling the issue of cyber security for energy infrastructure. There are also a plethora of official statements that can be identified; most highlighting the need for collective cyber security in the energy field, particularly in the oil, gas, and electricity sectors, but, with no clear guidance on how to achieve this. At the national levels, the US National Institute of Standards and Technology (NIST) is the US guiding framework for the assessment of resilience of critical infrastructure from cyber threats. The NIST Framework for cyber security is split into 5 functions: identify, protect, detect, respond, and recover. There are no clear guidelines, however, as to how each function must be achieved. Similarly, at the regional level, the EU Network and Information Security (NIS) Directive highlights the importance of "cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc." (EU 2016/1148). But, like the US NIST, the EU NIS does not provide, clear directions to how cyber assessments are to be conducted, particularly in the energy field.

2.2.2 From what threats to protect?

Cyber threats to CEI can come from sabotage and terrorist attacks or political/technology embargoes (the sovereignty perspective), extreme natural events or energy infrastructure failures (the robustness perspective), and unexpected regulatory/technology changes or natural events (the resilience perspective).

The sovereignty perspective

What makes these threats to OT increasingly appealing to perpetrators is 1) the multiple OT system vulnerabilities that remain unprotected from cyber-attacks (Alderson and Di Pietro 2016); 2) the increased availability of cyber tools capable of leveraging these vulnerabilities (Andress and Winterfeld 2013); and 3) the decreased level of risk needed to be taken by the perpetrators, who often remain anonymous in cyberspace after the attack, and never being caught due to lack of attribution (Geers 2010; Hunker, Hutchinson, and Margulies 2008; Mudrinich 2012). As a result, cyber-attacks against SCADA alone increased by 636 percent between 2012 and 2014 (IBM 2015, 5), while the number of vulnerabilities continued to grow faster than the ability to discover and address them. Of 189 ICS vulnerabilities identified in 2015, 49% were critical, and only 85% had new firmware available. Of the critical infrastructure vulnerabilities, 28% were easy targets for cyber-attacks, with exploits available on the internet. 14 out of 19 unpatched vulnerabilities were "of high-level risk" (Andreeva et al. 2016, 4). Today, thousands of cyber-attacks to CEI occur daily, with most remaining unattributed. British Petroleum alone, for example, has to protect itself against 50 thousand cyber-attacks per day, many of which, are attacks against OT (Seebruck 2015).

Cyber threats against CEI OT "are assessed according to two criteria, namely capability and intent" (Paradis et al. 2005). Capabilities vary vastly from perpetrator to perpetrator and depend on whether the cyber-attack is classified as 1) state organized and/or sponsored (through proxies) or 2) a non-state organized and/or sponsored. From a state perspective, 'cyber-power' is defined as "the ability to act and influence through, and by means of, cyberspace" (Czosseck and Ziolkowski 2013, 1). These actors have significant resources and access to restricted ICS know-how that is not typically available to the public. These are skilled and sophisticated adversaries that can conduct hybrid cyber-attacks against CEI OT without ever being clearly identified. Non-state actors stem from terrorism, organised crime, hacktivism, or insider threat. Due to limited resources, these threats are less complex, but can became a real danger with access to the right exploits against ICS.

The intent also differs from nation to nation or from state vs non-state actors. The state-sponsored cyber-attacks against the Trans-siberian gas pipeline in 1982 or against the Natanz nuclear facility in 2010, were not about industrial espionage; they did not "steal, manipulate, or erase information" (Langner 2011, 49). Instead, they attacked the OT infrastructure, causing physical damage with military and economic implications, and potential for an environmental disaster. Non-state actors have also "demonstrated improved malicious skills [and are] taking advantage of the growing arsenal of exploitation tools developed specifically for control systems" (IBM 2015, 10). More recently, a growing nexus between state and non-state cyber actors—where states are "outsourcing cyber-attacks to non-attributable third parties, including criminal organisations" (Farwell and Rohozinski 2011, 23)—has been identified. These relationships in cyberspace "have one common element, namely the willingness of the non-State actors to support their State's goals, be it for monetary or ideological reasons" (Czosseck and Ziolkowski 2013, 25).

The robustness perspective

Digital transformations—in particular, advances in data science, machine learning, and artificial intelligence—have become tremendous assets in the development of smart grids. The Internet of Things (IoT) and the Internet of Everything (IoE) have transformed energy planning, production, transmission, storage, conversion, distribution and consumption processes (Z. Zou, Zheng, and Sha 2018). They have connected the supply chains directly with the consumer, paving the way to the 4th industrial revolution (or Industry 4.0). This interconnectedness, however, has also linked COTS (commercial off-the-shelf), platform-independent ICS components (Ringert, Rumpe, and Wortmann 2015) to new technology platforms operating platform-specific, Original Equipment Manufacturer (OEM) digital ICS components. While platform-independent ICS components can easily coexist with old technologies, on the new platforms, these components can cause problems with severe repercussions. An example of this is the 2008 shutdown of the Edwin Irby Hatch Nuclear Power Plant in southeastern United States after a routine software update

(Wong et al. 2010, 18). Ultimately, while digital transformation has improved operations, the incompatibilities between new and old technologies has also increased the number of CEI OT cyber vulnerabilities.

The Hatch Nuclear Power Plant scenario has also illustrated that the connection of stand-alone OT components to management applications (IT) to improve remote monitoring and operations, has also created new largely unexplored vulnerabilities. Traditionally, IT and OT systems served "different goals, different strategies, and different stakeholders" (Garvin and Others 2015). For this reason, these systems are programmed to behave differently in their respective networks: "IT networks focus primarily on PAIN (Privacy/Confidentiality, Authentication, Integrity and Non-repudiation) OT networks focus primarily on AIC (Availability, Integrity and Confidentiality)" (Garimella 2018). Converging IT/OT networks, and the "conflicting requirements of availability and confidentiality" (Garimella 2018) is a challenge that needs to be addressed before "accelerating the convergence of IT and OT to deliver increased safety, efficiency and productivity" (Kamal et al. 2016).

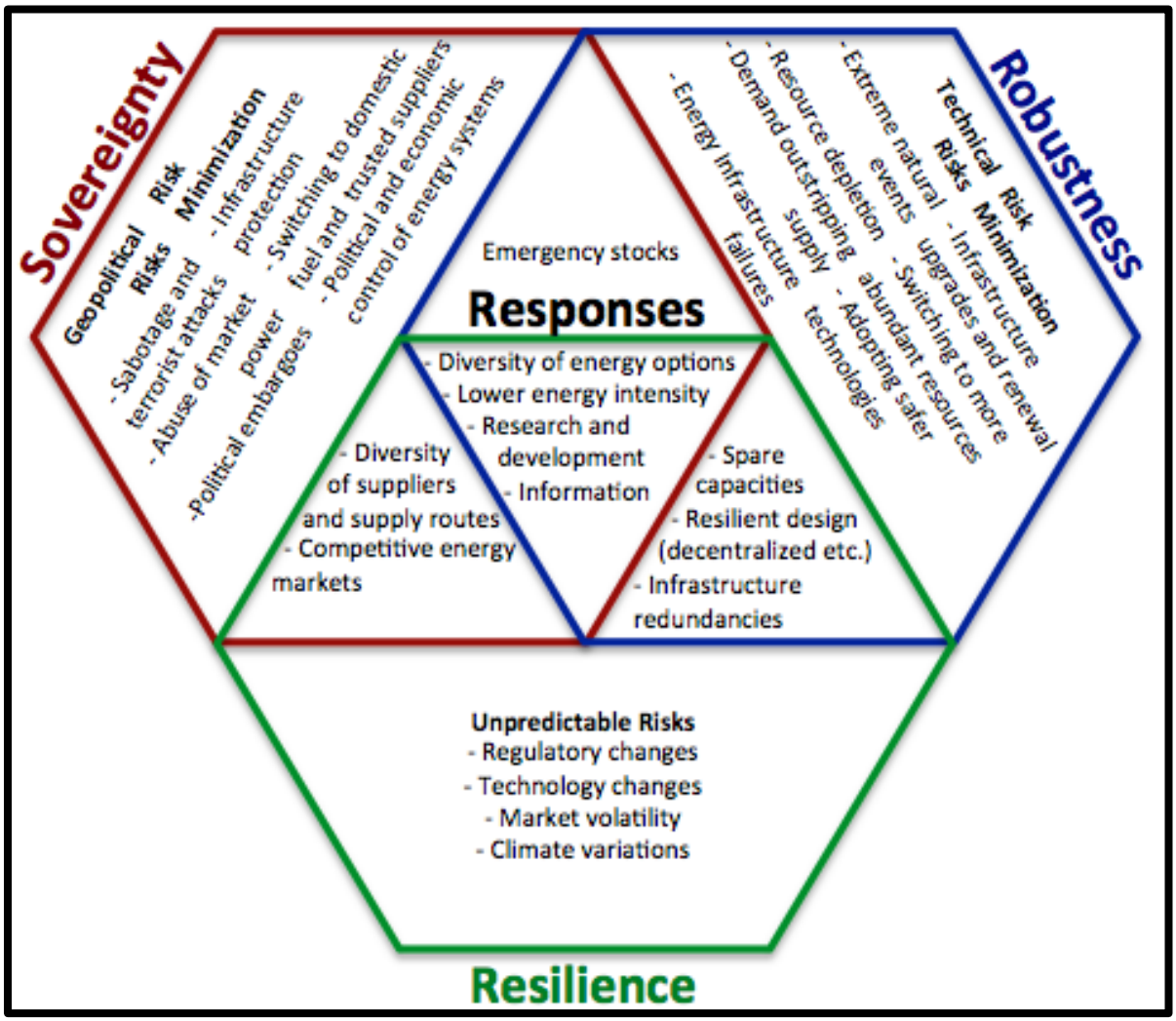
The resilience perspective

Energy infrastructure failures do not occur only due to digitalization of OEM ICS components. They are also caused by unexpected natural events or technological advances and exploits causing OT systems to fail. Natural events do not have to be electromagnetic pulses (EMP) caused by solar flares, known as coronal mass ejection, CME (M. B. Hughes 2017). For example, the chain reaction that led to the Northeast U.S. Blackout of 2003 was initiated by an overgrown tree in Ohio that ended up costing the United States up to $10 billion USD (Andersson et al. 2005, 1922). The hypothetical North American Blackout of 2038 that "left upwards of 300 million people without power, ravaged the world economy, and devastated the global internet" was caused by a cyber adversary with unexpected "technical sophistication", that used OT exploits to take both the primary and fallback systems offline (Anantharaman et al. 2018). Advances by artificial intelligence,

for example do not only help in protection of CEI but also provide new tools for cyber perpetrators to identify and exploit new OT ICS component vulnerabilities.

2.2.3 By what means to protect CEI?

The IT/OT digitization and rapid convergence led to the increase in number of "remote centralized network control centers" (Donde and Tournier 2016) outside national boundaries; placing IT/OT vulnerability assessments and protection against cyber threats outside the control of one country alone. Because of this, without significant assistance from outside regional structures and alliances, nations can no longer respond to cyber threats against CEI independently. Understanding how threat actors exploit ICS components is knowledge that requires collaboration across borders and intelligence sharing. The CSA is slowly emerging as the ideal mechanism to tackle cyber vulnerabilities of CEI with regional implications during the transition from digital transformation to energy transformation. The recent developments in digital transformation for energy transformation (Serrano-Calle and Delarue 2018), particularly, advancements in the fields of data science and artificial intelligence, also "hold tremendous potential" (Kratsios 2018) for CSAs to better protect CEI in cyberspace. While the interconnectedness of technology creates new IT/OT cyber vulnerabilities, CSAs come with the promise of cross-border intelligence sharing (see figure 6) on cyber security, which is needed for surviving the Industry 4.0 digital threats.



Source: Adapted from (Cherp and Jewell 2011/9)
Figure 6. Intelligence sharing added to Cherp's three perspectives on energy security.

2.3 Collective security alliances

From the beginning of warfare—and documented as early as the Battle of the Ten Kings between 4500 and 3500 BC—ancient rulers, often advised by scholars of political affairs, war, and economics, paid particular attention to the study of regional alliances. In the 4th century BCE Chanakya (Kautilya)—one of the earliest pioneers of realism—wrote in his ancient Indian political treatise *Arthasastra* that the planning of alliances is one of the six forms of state-policy that define the study of foreign policy. Chanakya defined alliances (samsraya) as "seeking the protection of another [king who is stronger than one's neighboring enemy or entering] in agreement with any two (friendly) kings, [for the purpose of augmenting one's] resources" (Shamasastry 1915, 374).

Two millennia later, the basic principles of international relations and the fundamental basis of alliances were transformed following the 1648 Peace of Westphalia that ended the Thirty Years' War (1618–1648). The traditional understanding of alliances was best explained by George Liska's theory of alliance formation, where Liska defined alliances as "merely formalized alignments based on interests or coercion" (Liska 1962, 3) and whose purpose—as described by George Modelski's study of alliances—is the "common defense [through] the use of military power" (Modelski 1963, 771). But alliances could not violate the guarantees to the nation-state of the Westphalian system, best explained by Hugo Grotius (1583–1645): "(1) the sovereignty of the state; (2) the sovereign equality of states; (3) the right of non-interference in domestic affairs of the sovereign state; (4) the territorial integrity of the state; (5) the obligation to abide by international agreements; (6) the principle of the peaceful settlement of disputes; and (7) the obligation to engage in international cooperation consistent with national interests" (Gleason and Shaihutdinov 2005, 275). Within this framework, Singer and Small argued that (1) internal threats to a member state's national security do not fall within the jurisdiction of the alliance; (2) the sovereignty of the member state is further guaranteed by non-intervention agreements among member states; (3) hostilities among member states are subject to review by an entente within the alliance; and (4) collective defense agreements obligate member states to assist militarily only if a member is attacked by other non-member states (Singer and Small 1966).

A more contemporary understanding of alliances evolved during the Cold War from a need to better explain the formation of "bilateral or multilateral agreements" of the time (Weitsman 2004, 27). The diminishing of resources brought upon by the East vs. West (Warsaw Pact vs. NATO) security dilemmas forced states to redefine the value of cooperation within an alliance, and the term alliance became more commonly understood as "a formal agreement between two or more nations to collaborate on national security issues" (Holsti, Hopmann, and Sullivan 1973, 4), or "a formal or informal relationship of security cooperation between two or more sovereign states" (Walt 1987, 1). Here, Michael Ward argued that Singer and Small's four characteristics of alliances no longer

make sense within the new post-Westphalian framework, because contemporary alliances rely on (1) a collaborative relationship to combat threats to one's national security; (2) the potential for aggregation of military forces despite the sovereignty principle; (3) the belief that common interests and threats outweigh the desire for conflict among member states; and (4) the primacy of collective action over unilateral responses (Ward 1982, 19:5).

Ward's arguments were renewed in recent years as the focus of international security studies shifted from state to non-state threats. In his writings Glenn Snyder concluded that the study of alliances could no longer be divorced from that of collective alignments. Snyder described alliances through neorealist lenses—focusing primarily on interactions between states—and explained that before entering formal alliances states build first informal alignments dependent on "whether they will be supported or opposed by other states in future interactions" (Snyder 2007, 6). Formal treaties are then agreed upon to strengthen these alignments by adding "elements of specificity, legal and moral obligation, and reciprocity that are usually lacking in informal alignments" (Snyder 2007, 8). The study of how and for what purpose collective security alliances form thus deserves further consideration in order to better understand the evolution of alliances in the 21st century and their role in addressing energy and cyber security threats that impact smart and sustainable low-carbon energy transitions.

2.3.1 Empirical studies on CSAs under the Westphalian system

The earliest theoretical model of collective security is attributed to Cardinal Richelieu, whose genius led to the Peace of Westphalia (1648)—albeit six years after his death. It thereafter took nearly two centuries for Richelieu's geopolitical model—which relied on enforcing the balance of power as "a procedural norm for collective wellbeing [and] through multilateral forums" (Joensson 2010, 15)—to fully materialize in the Concert of Europe (1815-1848). Ultimately, the balance of power model—which stood at the base of the status quo among the Great Powers after Napoleon's defeat—failed to contain the territorial ambitions that led to the start of World War I.

After the Treaty of Versailles (1920), ending World War I, the League of Nations was also "rather ineffective in stopping German and Italian dictators' aggressions in the 1930s" (Yilmaz 2009, 34), serving only to alienate Russia, a major regional power at that time:

> *"Between the two world wars, collective security in Europe was anchored in the Paris Treaties and in the League of Nations. Until her entry into the League in September 1934, Soviet Russia stood apart from this system, because she had concluded her own peace treaties with Germany and Austria-Hungary in March 1918, did not take part in the Paris Conference, and was not invited to membership in the League of Nations. The Soviets viewed the whole Paris settlement as an imperialist enterprise; they especially resented the fact that the Conference confirmed the detachment from Russia of certain territories which had been conquered and annexed by the Tsars during previous two centuries, namely Poland and the Baltic states" (Hochman 1982, 14).*

With the failure of the League of Nations to prevent World War II, the concept of collective security lost its credibility, being replaced by that of collective defense—which aimed at "deterring or defeating aggressors external to the grouping and specified prior to aggression" (Salem 2006, 56) and was a better fit for explaining the Cold War dichotomies. The traditional views of collective security emerged in an effort to understand the failures of the Concert of Europe and the League of Nations, when international relations scholars began reexamining the principles that lie behind the formation of CSAs. In his studies, Inis Claude explained that CSAs form as "a functional response to the complexities of the modern state system, an organic development rooted in the realities of the system rather than an optional experiment fastened upon it" (Claude 1971, 6). This renewal of interest gave rise to competing views on collective security "rooted in the international relations schools of realism, liberalism, institutionalism" (Bennett and Lepgold 1993). Understanding how these schools of thought perceive collective security is necessary to explain why and how sovereign states join or leave CSAs and how these alliances are governed and evolve over time.

Collective security within the realist school of international relations theory

The traditional realism of Machiavelli, Hobbes, and Richelieu perceives the international

system as an anarchic order where the behavior of states is governed by competition for the pursuit of power among nation-states. Within this system, realists like Hans Morgenthau and George Liska perceive alliances as unnatural—by virtue of the nation state's absolute sovereignty. The realist concept of alliance is merely reduced to a temporary means of diminishing "the impact of antagonistic power, perceived as pressure, which threatens one's independence" (Liska 1962, 26). Because alliances have been perceived as both as a threat to and protector of the sovereignty of nation states, the study of how they are formed and governed is also of great interest to the realist school of thought: "the historically most important manifestation of the balance of power […] is to be found not in the equilibrium of two isolated nations but in the relations between one nation or alliance of nations and another alliance" (Morgenthau 1978, 175). In studying these relationships, however, realists focus less on common security interests and threats of potential member-states, and more on the dichotomy between weak and strong states, and their military power (Good 1962, 8–9).

As Arthasastra treatise identified over 2,300 years ago, states enter alliances for their own national interests "when the balance of power is threatened" (Organski 1958, 277), or in order to equalize imbalances that they wouldn't be able to affect in their favor otherwise. This logic implies that member states enter alliances with one another "in order to supplement each other's capability" (Liska 1962, 26) when under threat of diminishing military power. Here proponents of the realist school of thought distinguish clearly between collective security and collective defense agreements—unlike authors like Slater (Slater 1965, 1:47) and Farer (Farer 1993, 178) who fail to make this distinction.

Collective defense agreements differ from collective security ones in both focus and scope. Collective defense "is based on an identified common threat" (Salem 2006, 66), so by deduction, a collective defense alliance "is a collective of states that expresses the will to either deter or respond to a common threat" (Gleason and Shaihutdinov 2005, 277). These types of alliances are the traditional military alliances that existed since the beginning of warfare among competing states

bound together by vulnerabilities to an existing common threat from another state or another collective of states "widely perceived as threatening to actual or prospective alliance members" (Hook and Robyn 1999, 84). According to the realist school of thought,

> *"nations enter into collective defense arrangements to ward off threats to their national security interests, as traditionally conceived, emanating from some specific country or group of countries regarded as the chief national enemy, actual or potential […] the motive behind such arrangements is the conviction that the creation of military strength sufficient to ward off the specific threat would be beyond their national capacity or would prove excessively and unnecessarily costly in view of the opportunities for mutual support and common defense" (Wolfers 1965, 183).*

While states enter collective defense alliances in order to reduce "threats that originate outside the membership" (G. W. Downs 1994, 2), the focus of collective security is not limited to non-member states as the only potential aggressors (Alagappa 1998, 10; Gordenker and Weiss 1993, 6), but concerns itself with both state and non-state threats from both outside the alliance and from among its member states. In this respect, "the scope of collective-security arrangements is inherently broader and more ambitious" (Hook and Robyn 1999, 84), where member states of the CSA could equally become "potential aggressors, victims of aggression, or coalition partners" (Diehl and Lepgold 2003, 43). In other words, within the collective security systems any aggression against one member state is an aggression against all members of the coalition: "collective security is directed against any and every country anywhere that commits an act of aggression, allies and friends included" (Wolfers 1965, 183). Within this framework, "collective security requires that countries combine their military forces in a coalition aimed at punishing acts of armed aggression" (Yilmaz 2009, 34).

According to most scholars of the realist school of thought, the collective security concept is perceived as 'deceptive' (Farer 1993, 155) and 'incompatible' with realism because in order for collective security to work states must trust each other and place the interests of the collective above their own sovereign interests, which realists argue is "virtually impossible" (Mearsheimer 1994, 28–35).

Collective security under the liberalism school of thought

The theories on collective security find most support within the liberal school of thought, which view collective security as a substitute to the traditional Westphalian system (Salem 2006, 60)—where alliances are formed to maintain or disrupt the balance of power (Claude 1971, 247)—and as a conduit towards the "peaceful change of the status quo" (Hogan 2015, 182). Compared to traditional realism, where "states that are heavily influenced by balance-of-power considerations are, by definition, going to be mainly concerned about the balance of power, not about maintaining peace" (Mearsheimer 1995, 88), Adam Smith's liberalism professes that "the interdependence of nations and the reciprocal nature of their needs ensured that peace was in the interest of all states and that only a misperception could lead to" military conflict (HLR 1989, 640). Liberal thinkers view military force as an endemic, irrational force, calling for collective alliances in which "national interests would be subordinated to the interests of the community" (HLR 1989, 641). Sovereignty is regarded here as a privilege rather than a right of the state: "in order to be legitimate, sovereignty must demonstrate responsibility. At the very least that means providing for the basic needs of its people" (Deng et al. 2010, xvii). Because of these key characteristics, theorists of both realism and liberalism schools of thought agree that "the promise of collective security stems from a theoretical perspective that is incompatible with realism" (C. A. Kupchan and Kupchan 1995, 59).

Having its origins in Immanuel Kant's 1795 Perpetual Peace, the traditional liberal view of collective security "has been formed by the growth of practical morality" (Thompson 1953, 754), and by a pressing reality "that has tied all the peoples of the earth together in an unprecedented intimacy of contact, interdependence of welfare, and mutuality of vulnerability" (Claude 1971, 3). Within this liberal framework, the concept of national security is subordinated to that of basic human security, and the primary aim of CSAs became to preserve "the conditions under which most people, most of the time, are able to go about their lives, venture onto the street, work, study, and participate in public life (politics included), without acute fear of being killed or injured—without being terrorized" (Etzioni 2008, 2).

It can be concluded that the liberal focus and scope of CSAs is significantly different from that of the realism school of thought. The primary focus of the CSA under this framework is to act as "a self-stabilizing agreement among members who agree to subordinate the pursuit of their narrow self-interest to the broader goal of system stability" (Gleason and Shaihutdinov 2005, 277) rather than joining forces to protect against national security threats (Thakur 2016). Under this school of thought, member states are bound to collective threat of economic sanctions and/or diminishing economic prospects and the need to share in the cost of defense with the ultimate aim to outlaw war (Joensson 2010, 15) and abolish "all ills and diseases disturbing the body social" (Thompson 1953, 754).

Collective security and new institutionalism

The study of the institutionalization that organizational bureaucracies create within society gave rise to a new theory of constructivist institutionalism, which adopts elements from both Machiavellian realism and Kantian liberalism. According to constructivist institutionalism school of thought, collective security arrangements cannot be understood outside of the rule-oriented bureaucracies they create: "in collective security arrangements, agents identify each other as citizens (rule 1) who are obliged to uphold agreed-upon rules of behavior (rule 2) and act collectively to punish those who do not uphold those rules" (Frederking 2003, 367–369). Within this framework, members enjoy the mutual security benefits of the community only as long as they obey the rules of the community (Salem 2006, 60), and only as long as agents place the institutional bureaucracy agreed upon above or at least on equal footing with the principle of sovereignty. By assenting to a code of behavior in the form of alliances, nation states organize themselves into supra-national security bodies committed to the defense of any member state against any aggression, irrespective of its friendly or hostile origin. Ultimately, nation states surrender the monopoly of the legitimate use of military force in favor of multilateral security obligations towards the collective (Bull 2012; Wolfers 1965).

Theorists of this school of thought argue that because institutionalization "provides more stability than unregulated, self-help balancing predicated on the notion of each for [its] own," (C. A. Kupchan and Kupchan 1995, 52) regional or global peace can only be achieved within formal collective security alliances, where member states are bound together by moral, economic, and military pressures (Salem 2006, 57). But realists argue that collective security alliances still have to pass the critical test where sovereign nations will place the interest of the community before their own, pointing out that "the empirical evidence showing that institutions changed patterns of state behavior was weak, especially in the area of security affairs" (Martin and Simmons 1998, 738). More precisely, the argument is made that the nation-state monopoly over the use of brute force cannot be effectively challenged by multinational organizations because national security is "immune from institutional effects" (Lake 2001, 158), and because the "all-against-one" (C. Kupchan 1994, 43) principle cannot be institutionalized among rational states (Donnelly 2000, 136). In return, non-state-centric constructivists contend that the clash with realists lays mainly in the primacy of sovereignty argument of the international system (Finnemore and Sikkink 1998, 31–33), and claim that the constructivist institutionalism theory already passed this critical test in the governance of peacekeeping operations by CSAs (Barnett and Finnemore 2004).

While "cooperation in security relations has historically been much less visible than that in economic relations" (Gallarotti 1991), in practice they existed since the beginning of warfare. The main challenge CSAs face is thus "to move beyond the self-help world of realism where states fear each other and are motivated by balance-of-power considerations" (Mearsheimer 1994, 28). To overcome this challenge, constructivist institutionalism theorists argue that once a collective security agreement is reached, the resulting bureaucracy is then "institutionalized in organizational structures and procedures, to preserve the common discourse and unite the members in action" (Joensson 2010, 15). These structures and procedures also give the new CSA the legality and legitimacy that states alone may lack in the international system (Tharoor 2003).

Jerome Slater listed two requirements of collective security to insure that theory is applicable in practice: "(1) in cases of violent interstate conflict, collective action must be taken or authorized by the organization to aid the victims of aggression and to restore the peace, and (2) such action must be impartial, ignoring the internal political structures or ideologies of the states involved" (Slater 1965, 1:52). In constructivist institutionalism, the focus of the collective security is thus on "continuously reaffirming states of their mutual commitment" (Joensson 2010, 15) for the purpose of maintaining peace and insuring individual prosperity within the geographical boundaries of the alliance. Whatever their interest in the security threat faced by the community, "the states commit to making available the necessary resources for translating the discourse into practice" (Joensson 2010, 15) rather than limit themselves only to making "educated expectations" that too often lead to inaction (Claude 1971).

2.3.2 Post-Westphalian perspectives on collective security

The emergence of non-state threats of the 21st century challenged the positivist theories on collective security dominant during the traditional security environment, and the scholarship in the field evolved "in the direction of post-positivist theories, namely culturalism, constructivism and normative theories" (Rulska 2010, 24). These new schools of thought marry security and community (Adler, Barnett, and Smith 1998, 5) to construct "mutual aid" societies governed by a system that "lies somewhere between a sovereign state and a regional, centralized, government; that is, it is something of a post-sovereign system, endowed with common supranational, transnational, and national institutions and some form of a collective security system" (Ruggie 1996, 81–82).

The inability of sovereign states to face the new threats unilaterally forced policy makers to revise the conventional, largely realist meaning of security and encouraged academics to incorporate "elements of comparative theories such as theories of regionalism and integration to effectively explain the creation of security organizations and communities" (Rulska 2010, 24). Whereas traditionally security was understood as military security, "now states are identifying 'new' security

issues that revolve around economic, environmental, and social welfare concerns and have ceased to concern themselves with military threats from others within the community"(Adler, Barnett, and Smith 1998, 5).

With the meaning of security changing, so did the theoretical approaches addressing the field of collective security. While during the Cold War positivist theories dominated approach to studying collective security and alliances—with liberalism and constructivist-institutionalism shaping the views on collective security, and realism dominating the debate on alliances—the new security order is largely reliant on the theoretical perspectives of neorealism, globalism, and regionalism (Buzan and Wæver 2003, 6).

Neorealism and the skepticism surrounding the prospects of CSAs

While the field of study on alliances in the bipolar environment of the latter half of the twentieth century has been dominated largely by classical realism, which stressed that states enter alliances in the pursuit of power, the new systemic approach to alliances relies on the school of Waltzian neorealism, which emphasizes that alliances are formed in the pursuit of security (Rulska 2010, 40). In neorealist terms, security means national security and neorealists claim that supra-national cooperation among competing actors is particularly problematic, "especially in areas affecting national security" (Donnelly 2000, 136). Because of the anarchic and competitive nature of the international system, "no state can ever be completely certain about another state's intentions [and] have little choice but to fear each other" (Mearsheimer 1994, 28–31). This implies that inviting outside actors to collaborate on addressing intangible, transnational threats to national security is a matter of last resort (Rulska 2010, 23), and scholars of CSAs largely contend that until recently, "throughout the world, the major inter-state security organizations continue to be essentially Westphalian in nature. They assume the primacy of state actors. While collective security organizations have re-focused their objectives to confront challenges emanating from below the

level of the nation-state, they have not yet reorganized their operational programs to achieve these goals" (Gleason and Shaihutdinov 2005, 275).

Contrary to the traditional security environment, where "politically and economically stable nations [were] more likely to join alliances than are unstable ones" (Teune and Synnestvedt 1965, 189), the complexities of the contemporary security environment made all states dependent on supra-national communities to defend their values and to "convey a sense of national security and material progress" to their citizens (Adler, Barnett, and Smith 1998, 5). Despite this, on the topic of collective security the scholars of neorealism adopted the belief of the realism school that it is typically "the confluence of the objectives of all possible major rivals (who would be adversaries in several other types of system) that makes—and, historically, has made—collective security possible. Thus, such a concert is both the limiting case and the minimum condition of a collective security system" (Ravenal 1975, 704). From a neorealist perspective, CSAs thus continue to be understood as short-lived alliances among threatened states, with multiple aspirations and with the occasional free riders, where more often than not balances fail to form against aggressors, undermining deterrence and leading to an unfair distribution of costs and benefits among member states.

Globalism and the utopian pursuit of international peace and security

With the Cold War precepts of international security collapsing, the United Nations (UN) Secretary-General's 1991 address to the General Assembly positioned the concept of collective security at "a unique juxtaposition of promise and peril," (Bennett and Lepgold 1993, 213). Almost reminiscent of the failures that plagued the existence of the League of Nations between the two world wars, the utopian idea of building a global CSA with the capacity to insure the collective welfare and human security of all people reemerged (Annan 1999; Barnett and Finnemore 2004; Kratochwil and Mansfield 1994; Newman, Thakur, and Tirman 2006; Thakur et al. 2005). This is, however, not a new argument in the study of international relations. If there is one point that classical realists (Claude 1971), and liberal theorists (Haas 1968) agree on with regards to collective

security, it is definitely the argument that CSAs can only function as an international organization with universal membership (like the UN). Within this global community "any illegal threat or use of force by any sovereign member of the international community against any other... should trigger the combined force of all the rest" (Hogan 2015, 179; Miller 1999, 303). Global collective security thus involves "the legal establishment of the prohibition of aggression, the commitment of states to collaborate in the suppression of aggression, and the endowment of an international organization with authority to determine when and against what state sanctions are to be initiated, to decide upon the nature of the inhibitory measures, to evoke the performance of duties to which states have committed themselves, and to plan and direct the joint action which it deems necessary for the implementation of collective security" (Claude 1971, 260).

This thesis agrees with Keohane and Nye argument that "only rarely universal international organizations are likely to provide the world with instruments for collective actions" (Rochester 1995, 202). By limiting the discourse on collective security only within the framework of a global political system, however, policymakers, scholars, and other promoters of global (rather than collective) security "established a set of requirements or definitions so unrealistic that, if met, they would be superfluous (the utopia of benign world government presiding over uniformly co-operative human beings having been attained) while, because they are obviously unmet, they serve to obscure significant organizational behavior containing at least elemental ingredients of practical collective security" (Slater 1965, 1:5).

In order to understand why Wilsonian-style global security alliances fail, it is important to understand the failed assumptions that led to the rise and fall of the League of Nations. First, collective security requires a community of shared values and interests that globally is nearly impossible to achieve. With this in mind, conferring the Soviet Union membership into the League of Nations "was obviously a fallacy in the first place" (Hochman 1982, 397). Second, while states may have "clear interests in protecting an international order that they see as beneficial to their individual security" (C. Kupchan 1994, 45), membership into this global collective security is almost

never a guarantee of deterrence because global peace requires the reinvention of "the system of collective security for the global world" (Joensson 2010, 250). With regards to the League of Nations, Pierre Cot's argument that the integration of France within the League of Nations would guarantee its security "failed to save France" in 1940 (Skidmore 1981, 239). France's belief that other powerful states within the League of Nations "will choose to expend financial resources and put their troops at risk to deter or suppress conflicts that have little or no relevance to their national security interests" (Carpenter 1997, 18) proved to be wrong.

The advent of regional CSAs

The failure of the League of Nations to pass the practicality test in the early twentieth century encouraged collective security theorists like Niou and Ordeshook to search for a more concrete system for maintaining regional—rather than global—peace (G. W. Downs 1994, 8). According to Slater (Slater 1965, 1:5), regional collective security emerged as the "only" system capable of maintaining peace in an area that expands beyond national reach as long as all members are "equally committed" (Miller 1999, 304) to the cause. The existential threat of climate change and the cyber threats to interconnected CEI that cross national borders fits within this category.

The ideal of regionally-based collective security found more support than other global structures in the neorealist and constructivist schools of thought because "such groupings have a greater understanding of the causes and nature of security problems affecting the region; because the incentives for managing conflict are likely to be higher; and because there will be a greater degree of consensus over basic values" (Hurrell 1992, 40). They were found more practical because (1) members were "likelier to act for the group's interest, as they define it" (Kenneth N. Waltz 1979, 198) and (2) "free-riding is more transparent at the regional level" (Diehl and Lepgold 2003, 45), and thus easier to avoid.

The ideal of regional security thrived to an unprecedented level and theorists like Kupchan and Kupchan expressed "a degree of optimism about collective security but only in a regional context," giving birth to the regional security complex theory which states that

> *"most threats travel more easily over short distances than over long ones, security interdependence is normally patterned into regionally based clusters: security complexes. [...] Processes of securitization and thus the degree of security interdependence are more intense between the actors inside such complexes than they are between actors inside the complex and those outside it. Security complexes may well be extensively penetrated by the global powers, but their regional dynamics nonetheless have a substantial degree of autonomy from the patterns set by the global powers. To paint a proper portrait of global security, one needs to understand both of these levels independently, as well as the interaction between them" (Buzan and Wæver 2003, 4).*

The growing support for the regional security complex theory has forced the UN to abandon its aggressive pursuit of collective security at the global level and seek more regional means to foster international peace (Diehl and Lepgold 2003, 159). Because of this, Chapter VIII of the UN Charter now allows the Security council to "use regional arrangements of one sort or another to facilitate the peaceful settlement of disputes or to carry out enforcement measures," and allows "regional organizations acting independently [to] deal with such matters relating to the maintenance of international peace and security as are appropriate for regional actions" (Farer 1993, 161). Since then, the UN often outsourced election observation to the Organization for Security and Co-operation in Europe (OSCE) and military enforcement to the North Atlantic Treaty Organization (NATO) (Joensson 2010, 12).

2.4 Securitization of geo-energy systems: energy security and the challenge of cyber diplomacy within collective security alliances

An 'emerging challenge' for CSAs, energy security at the regional level further exacerbated the energy security policy predicaments encountered at national levels. At both national and regional levels—both within government policies and edicts of CSAs—energy security remains a fluid concept whose definition "has been totally eclipsed by an almost overwhelming focus on

securing supplies of primary energy sources and geopolitics" (Chester 2010/2). But whereas the sovereignty of the state and/or polity over energy threats is rarely challenged, the concept of collective security finds "as many as 12 different definitions" (Buzan 1983), which can vary from one security alliance to another, or even from one state to another within the same security alliance. Because of the polysemic nature of both energy and collective security, while much was written on the security of energy supply chains within independent CSAs (i.e. NATO and the Shanghai Cooperation Organization, SCO), very little was written on the securitization of geo-energy systems of CSAs.

When studying CSAs, most scholars—like Olson and Zeckhauser (Olson and Zeckhauser 1966)—chose to focus on just one important alliance (most commonly NATO) to prove or disprove their theories on collective action and collective security (Oneal 1990, 427). Before making any generalizations on energy security for CSAs, however, one must look at CSAs from distinct regions and ask: "who is threatened, who is threatening, what is the threat, and what can stop that threat" (Rulska 2010, 41)? These questions are also the basis for Cherp and Jewell's three questions that must be answered before building any energy security frameworks—what energy security systems to protect, from what energy security threats to protect, and by what means to protect.

Who is threatened: what energy security systems to protect in cyberspace?

According to Stephen Krasner—Graham H. Stuart Professor of Political Science at Stanford University and former U.S. State Department Director of Policy Planning—collective security arrangements are governed by "rules and norms around which actors' expectations converge" (Krasner 1983, 3). This implies that the process used to determine which energy security system to protect in cyberspace will differ not just from country to country, but also from one CSA to another. NATO, for example, is using the CARVER methodology—based on **C**riticality, **A**ccessibility, **R**ecuperability, **V**ulnerability, **E**ffect, and **R**ecognizability factors—to assess and prioritize cyber security risks to CEI. While this methodology plays a major part in understanding

how NATO states select which energy security system to protect in cyberspace, it is not an indicator on how other CSAs will make their determination.

Who is threatening and what is the threat: from what risks to energy security to protect?

CSAs are set up to defend its member states from both state and non-state threats—or "potentially very harmful conditions created deliberately by human beings" (Keohane 2006, 220)—agreed upon "by regulating, facilitating, maintaining and even enforcing a common discourse on what constitutes threats and 'the security from what' question" (Joensson 2010, 18). State-related threats may include—but are not limited to—the power and/or willingness of a state to impose regional energy embargoes, and could "be either a liability or an asset, depending on where it is located, what it can do, and how it is used" (Walt 1987, vi–viii). In this paper, non-state energy security threats in cyberspace constitute all other actors and/or factors that cause adverse changes to vital energy supply chains of any member state of a CSA. The securitization of geo-energy systems in cyberspace by CSAs is thus a product of member states elevating the "balance of threat theory" over the more traditional "balance of power theory" (Walt 1987, vi–viii).

Contrary to popular belief, the incorporation of non-state threats—to include stresses to energy systems—into policies of CSAs did not originate with NATO, but with the Collective Security Treaty Organization (CSTO). Furthermore, the 1992 CSTO creation "provided that aggression or threat of aggression against one country would be regarded as aggression against all participants in the treaty" (Gleason and Shaihutdinov 2005, 277). Determining who is threatening and what is the threat is thus dependent on the individual built-in bureaucratic mechanisms of CSAs that serve to prevent and discourage both potential aggressors and "potential defectors from violating the rules" (Rulska 2010, 3). Because of this, NATO's Critical Thinking Intelligence Analysis Process (CTIAP) would be insufficient to gain a holistic understanding of threats to energy systems interactions within all geo-energy spaces. Not only because this process is not used by other CSAs, but by linking the physical environment (ASCOPE: Area, Structures, Capabilities,

Organizations, People, and Events) to the geopolitical environment (PMESII: Political, Military, Economic, Social, Infrastructure, Information), the ASCOPE/PMESII Matrix gives a subjective idea of the threat from the researcher's perspective, mirror imaging from the eyes of an outsider, without taking in consideration the governance systems (more exactly the perceptions of the insiders), within which the geo-energy system exists. This picture gets further complicated in cyberspace, where CSAs must also address the problem of attribution of cyber attacks against CEI.

What can stop that threat: by what means to protect geo-energy systems?

Collective security requires "shared willingness to act effectively to enforce the law" (Hurrell 1992, 41), which is pricy in terms of political, military, economic, and social resources and disproportionate in defense expenditures from nation to nation (Olson and Zeckhauser 1966). But the expenditure of these resources is necessary to insure that the system is "flexible enough to adjust to the specific conflict, wide and deep enough to simultaneously grasp processes between, within, and across states, and powerful enough to make the distinction between legitimate and illegitimate claims for self-determination and state sovereignty" (Joensson 2010, 251). Larger states know "that their defense expenditures would significantly affect the outcome of the allied effort. Smaller states, on the other hand, could enjoy the security provided by the ability of their larger partners to deter war without paying a share of the costs proportional to the benefits received" (Oneal 1990, 427).

Collective security relies thus "upon the expectation that, in any given situation, most states—enough to constitute a preponderant force—will remain loyal to the system and will act upon the belief that their interests require them to join in suppressing a challenge to the order of the system" (Claude 1975, 716–717). Because "collective security rests on the notion of all against one" (C. A. Kupchan and Kupchan 1995, 118) despite disproportionality and resources limitations, the means to protect against national and regional threats differs significantly from region to region, sometime rendering collective security actions ineffective (Diehl and Lepgold 2003, 47).

One of the biggest challenges to protecting the regional energy security systems in cyberspace is thus the unwillingness to share in the costs of "collective commitment of a group to hold members accountable for the maintenance of an internal security norm" (G. W. Downs 1994, 2). Theoretically, once an aggressive intent has been identified, a response must be triggered (C. Kupchan 1994, 45). Practically, however, these responses often take a long time to negotiate and are dependent on the resources available, which differ geographically.

2.5 Summary of Literature Review

This literature review identified the lack of interaction in existing literature between the scientific analysis of vulnerabilities of energy systems in cyberspace and policy narratives of CSAs about risks and response capacities. There is almost no scholarly literature to date addressing how each region will ensure the protection of geo-energy systems from cyber vulnerabilities. While this has not been an issue in the traditional Westphalian system, the recent rise in discourses promoting energy integration, the IT/OT agglutination in cyberspace, and intra-regional cooperation with regards to smart and sustainable low-carbon energy transitions without addressing the growing need for security frameworks to protect these geo-energy systems in cyberspace is disconcerting.

The theoretical background on the specific nature of CSAs already identified them as a viable protector of critical and vulnerable regional geo-energy systems in cyberspace. Energy security in cyberspace is contextual in nature not only vis-à-vis a country's energy or cyber policies, resources, infrastructures and geographies, but also vis-à-vis a country's regional security alliances. Because of this, regional CSAs such as NATO, the Common Security and Defense Policy (CSDP), SCO, CSTO, the Peace and Security Council (PSC), the Association of Southeast Asian Nations (ASEAN), or the Union of South American Nations (UNASUR) emerged as possible supra-national bodies with the local trust and legitimacy to build energy and cyber security capabilities regionally within smart and sustainable low-carbon energy transitions (see figure 7).

Source: Author's representation.
Figure 7. The collective security (cyber) alliance (CS2A) as a legitimate defender of CEI from cyber threats and as an enabler of smart and sustainable low-carbon energy transitions (S2LCET).

Over the past decade, CSAs such as NATO (through its multiple documents), SCO, CSDP, and ASEAN have made it a top priority to ensure the security (to include against cyber attacks) of energy supplies needed to meet operational requirements during smart and sustainable low-carbon energy transitions. To date, however, the complexity of energy security assessments (particularly in cyberspace)—both within the traditional and contemporary body of literature and the generic energy security analysis theories (the most important ones being presented in this chapter)—significantly complicated the study of energy and cyber security outside of national boundaries. The securitization of CSAs' geo-energy systems in cyberspace—within the context of smart and sustainable low-carbon energy transitions—requires an analytical framework that is currently not scientifically developed. Further research is thus needed to address the challenge of defining and assessing cyber vulnerabilities of CEI for CSAs in the context of smart and sustainable low-carbon energy transitions.

Chapter 3

Methodology

This chapter will advance the scientific understanding of 'cyber securitization' (Hansen and Nissenbaum 2009, 1152) for regional energy systems during smart and sustainable low-carbon energy transitions by (1) reframing the existing theories of cyber security in the context of regional CEI securitization; (2) developing an array of reliable methods by CSAs for analyzing cyber threats, vulnerabilities, policies and perceptions impacting energy security; and (3) establishing a theoretical framework for cyber security of CEI within a regional CSA.

3.1 Nested cyber security assessments of geo-energy systems

The literature review identified the traditional reliance of energy and cyber security studies on methods rooted in scientific positivism, limiting energy systems interactions and their cyber security threats only to what we can observe and measure. These methods are however incompatible with the polysemic conceptions of energy security within a geographical region during smart and sustainable low-carbon energy transitions because they focus on only one level of analysis (the state), and often discount the importance of key stakeholders in identifying energy security threats and planning or implementing responses during smart and sustainable low-carbon energy transitions. A post-positivist, multitier approach—to better understand what cyber threats can disrupt the interactions between the vital energy systems and the resulting outcomes from the perspective of key national and regional stakeholders—is thus needed to better understand regional energy security complexes and how CSAs can affect the respective cyber security policies during smart and sustainable low-carbon energy transitions.

3.1.1 Cyber security in specific geo-energy contexts

Both national institutions and supra-national organizations promote intra-regional energy security cooperation because "countries located in geographic proximity often experience similar conditions with respect to access to energy resources and the structure of energy use, and may be engaged in more intensive mutual trade and transit of energy carriers" (Cherp et al. 2012). Regional energy networks "have grown to a scale and complexity, and have reached a degree of interconnectedness, that their protection can often only be guaranteed and financed as shared efforts. [This means that] information sharing is a crucial step to acquiring a thorough understanding of large-scale cyber-attack situations, and is therefore seen as one of the key concepts to protect future networks" (Skopik, Settanni, and Fiedler 2016). The protection of geo-energy systems from cyber attacks is thus less dependent on the plate-tectonics theory and more dependent on the securitization of energy access—of key energy supply chains—and interface with intra-regional non-energy arenas—such as intra-regional trade and collective security commitments (especially in the cyber security arena). Understanding the perspectives on energy security across continents—in Europe, Asia, Africa, North America, and Latin America—is however important to understanding and identifying regional cyber-energy security complexes and their impacts across different clusters of states within each continent.

Europe

The future of cyber security of energy systems within Europe lies in the balance between distinct geographical and politico-economic factors that "would be able to promote the common good of all three elements of the energy chain: supplier countries, transit countries and consumer countries" (Roberts 2006, 207). The main CSAs in Europe working towards achieving these objectives are NATO, EU, V4, Baltic Assembly, Northern Council, Nordic Baltic (NB8), EU Med Group, Central Europe Defence Cooperation (CEDC), South-East European Cooperation Process

(SEECP), and the Craiova Group. The securitization of energy supplies within the European continent is the direct result of "the growing importance of gas, the birth of the Euro, the fact of Russia being a 'non- aligned' energy agent and, lastly, the expected scarcity and the greater interest in securing the energy supply" (Mañé-Estrada 2006, 3785). On the latter, according to European Commission energy outlooks, "about 70% of European energy needs in 2030 will be met by primary (and non-renewable) sources originating from foreign areas, some of which are very remote and geopolitically unstable" (Biberacher et al. 2011). With the critical infrastructure of these geo-energy chains being vulnerable to cyber attacks, within the EU, the Network and Information Security (NIS) Directive highlights the importance of "cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc." (EU 2016/1148). The EU has also been tackling the issue of cyber security for energy infrastructure in official statements, highlighting the need for collective cyber security in the energy field, particularly in the oil, gas, and electricity sectors.

Asia

The national energy security standings throughout Asia vary "depending on the country's environment, including resource endowment, and the extent of energy demand increases," and "few countries performed well compared to the OECD average" with respect to the supply and diversity of energy sources or energy utilization efficiency (Koyama, Kutani, and Others 2012) during the current smart and sustainable low-carbon energy transitions. The constant increase in energy imports by consumer countries such as Japan—which "will aim to reduce the dependence on nuclear power" (Suzuki 2014, 76)—China, India, and South Korea, and the dramatic rise of regional competition for these resources force industrialized nations (particularly in South-East Asia) to increase cooperation in ensuring long-term guaranteed access to energy supplies. In pursuit of national energy security—and in an effort to solve South China Sea territorial disputes over the

Spratly Islands between several ASEAN member states, China, and Taiwan—many national governments in South-East Asia will bypass "international energy markets to instead seek longer-term supplies within their immediate regions" instead (Cheng et al. 2013).

To this end, the Economic Research Institute for ASEAN and East Asia (ERIA) recently highlighted the role of "regional energy cooperation in enhancing energy security [and] emphasizing how regional cooperation compliments each country's efforts and best addresses energy security" (Koyama, Kutani, and Others 2012, 5). This message was reinforced by the Asian Development Bank's Asian Development Outlook for 2013, which stressed Asia's need to "progressively integrate regional energy markets and infrastructure [and achieve] the degree of regional cooperation and integration in energy by 2030 that currently prevails in Europe" (Rhee 2013). Despite the fact that ASEAN "envisions the creation of a global ICT hub" (Heinl 2013) that would significantly contribute to regional energy security, however, the competition for energy resources between member states has hindered cooperation in the cyber domain toward the protection of energy infrastructure during smart and sustainable low-carbon energy transitions. Common concerns about access to energy supplies and to technologies that protect CEI is slowly forcing the region to adopt a co-opetition approach.

India and China, "each depend for more than 60 percent of energy consumption on domestic coal" (Manning 2000) on one hand, and potential competitors over energy resources on the other, continue to ramp up investments in energy assets outside their borders (focusing on Sub-Saharan Africa) in an effort to avoid or minimize regional confrontations. Throughout Asia, in fact, "bloated state-owned monopolies" (Manning 2000) share a common concern in securing energy supply chains and price stability, and thus "have every reason to be headed towards greater pragmatic cooperation" (Fengying & Jiejun, 2008) rather than competition. This cooperation is best exemplified through regional efforts like the Asian Energy Security (AES) project, which includes scholars from China, the Republic of Korea (ROK) and the Democratic People's Republic of Korea (DPRK), Japan, Mongolia, and the Russian Federation working together to find "better ways to

summarize and visualize multiple energy security dimensions and attributes […] from different points of view (for example, cultural impacts on different segments of society)" in order to enhance regional energy (and cyber) security cooperation during smart and sustainable low-carbon energy transitions (Von Hippel, Savage, and Hayes 2011).

Africa

The International Institute for Applied Systems Analysis's Global Energy Assessment recognized the need to "address the huge energy gap in the region [through] an enhanced level of intra-regional energy cooperation [because] many African countries are very small and may not be able to finance the huge investment costs needed to develop alternative energy sources" (Cherp et al. 2012); negatively affecting the cyber security of CEI during smart and sustainable low-carbon energy transitions outside of big urban areas. To address this challenge, several regional economic and security alliances emerged throughout Africa over the past two decades: African Union (AU), Common Market for Eastern and Southern Africa (COMESA), East African Community (EAC), Central African Economic and Monetary Community (CEMAC), Community of Sahel-Saharan States (CENSAD), Economic Community of Central African States (ECCAS), Economic Community of Great Lakes countries (CEPGL), Economic Community of West African States (ECOWAS), Indian Ocean Commission (IOC), Inter-Governmental Authority on Development (IGAD), Mano River Union (MRU), Peace and Security Council (PSC), Southern African Customs Union (SACU), Southern Africa Development Community (SADC), Arab Maghreb Union (UMA), West African Economic and Monetary Union (UEMOA), etc.

North America, Latin America and the Caribbean

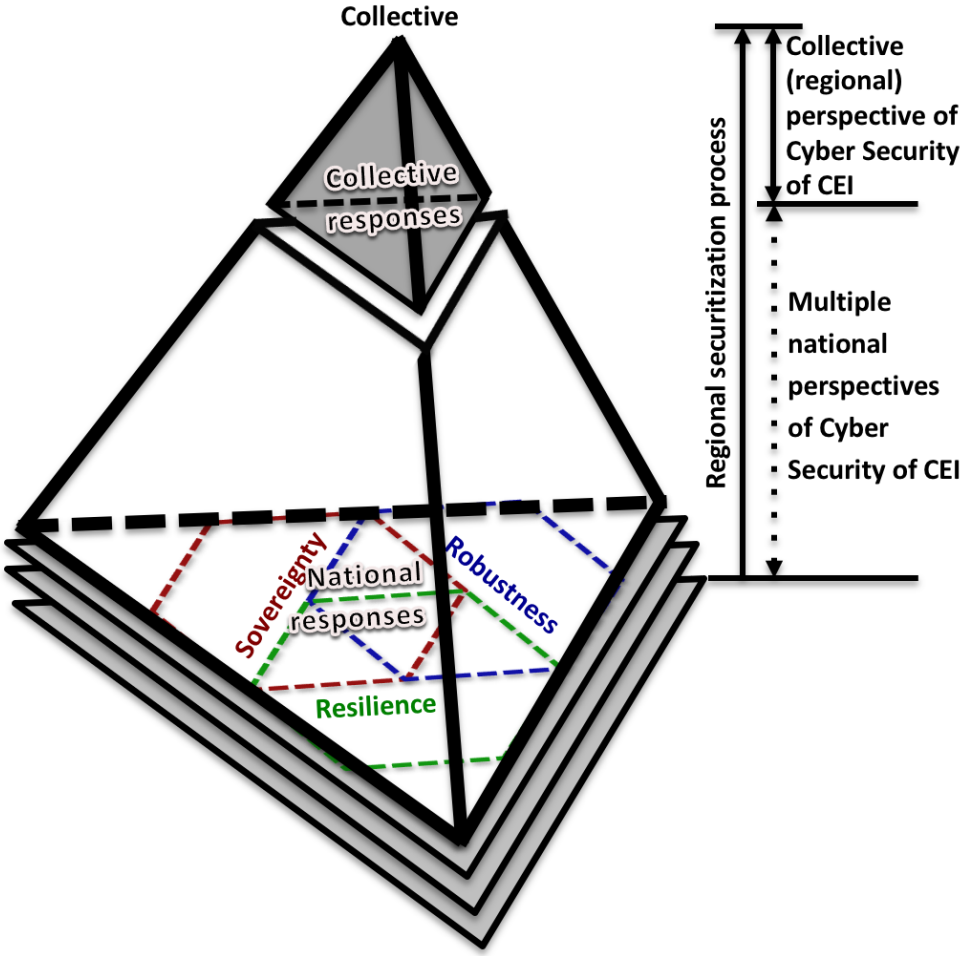
Apart from NATO in North America, several CSAs emerged to represent the interests of South America, Central America, and the Caribbean: the Regional Security System (RSS), the South

American Defense Council (SADC), and the Central American Integration System (SICA). Several other trade organizations that focus solely on trade have been ignored in this paper.

3.2 The proposed CSA cyber security framework during smart and sustainable low-carbon energy transitions

The proposed cyber framework uses "a combination of organizational as well as technological and cultural competences, which rely upon a multifaceted, multimodal, multinodal, and multilevel set of skills and capabilities" (E. G. Carayannis et al. 2019). In the process of analyzing cyber security strategies of CSAs during smart and sustainable low-carbon energy transitions, the proposed multitier framework also considers the existence of national and regional stakeholders—with their respective levels of influence and positive or hostile interests (MacArthur 1997)—in order to "understand behavior, intentions, interrelations, agendas, interests, and the influence or resources [these relevant actors] have brought–or could bring–to bear on decision-making processes" (Brugha and Varvasovszky 2000). It also relies on the premise that the energy and cyber security strategies of CSAs depend (hypothetically) on a mixture of national cyber/energy security perspectives (sovereignty, robustness, and resilience of national cyber awareness and national energy supply chains) and on the structure (bureaucracy) of the alliance—influenced itself not just by a diversity of national interests, but also by unique regional situations and actors such as regional security interests and energy cartels whose influence extends in that specific space. The former explains how individual nation states agree on a joint understanding of cyber security during the smart and sustainable low-carbon energy transitions within the structure of the CSA—while triggering national cyber security responses—and the latter effect collective responses that substantiate how member states collectively agree on (1) which national and regional vital energy systems, primary energy sources, and interactions to protect during smart and sustainable low-carbon energy transitions, (2) from what national and regional cyber security risks to protect, and (3) the national and regional means used to protect from these cyber threats—triggering collective

responses (see figure 8). This achieves objective 2: produce a methodology for prioritizing protection of regional energy systems—geo-energy systems—and their prospects in the cyber domain.



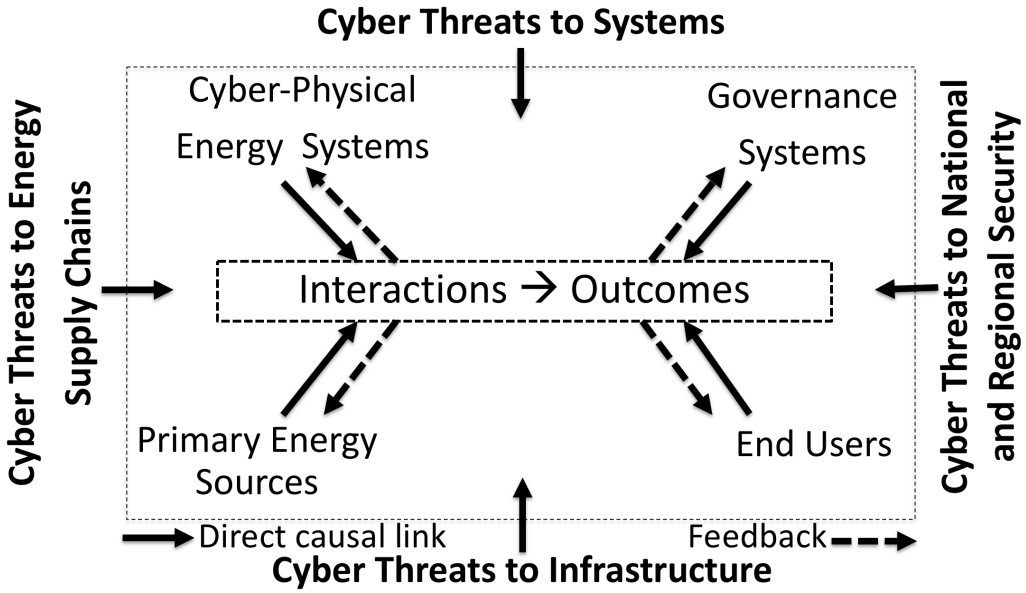
Source: Author's own representation.
Figure 8. National and collective (regional) perspectives of cyber and energy security complexes during smart and sustainable low-carbon energy transitions.

3.2.1 Framing: the national positions on cyber security during smart and sustainable low-carbon energy transitions

By observing how individual nation states (governance system at the first level of analysis) define energy security (and cyber security of CEI) in their official documents, we can identify and prioritize (1) the vital energy systems, primary energy sources, and their interactions (Security for

which values?), (2) the cyber threats to these systems, sources, and interactions during smart and sustainable low-carbon energy transitions (From what cyber threats?), (3) the state and non-state actors threatening these systems (Security for whom?), (4) the means available to protect from these cyber threats (By what means?), (5) the cost of protecting the vital energy systems from cyber threats during smart and sustainable low-carbon energy transitions (How much security and at what cost?), and (6) the timeline to protect these systems by (In what time period?) (Baldwin 1997, 13).

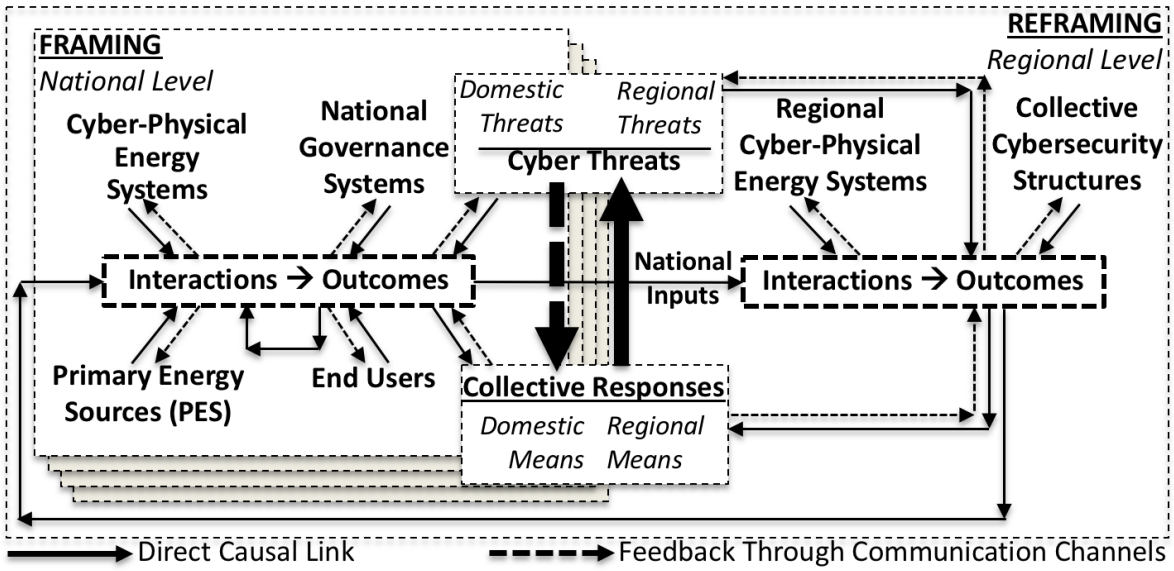
A multitier cyber security framework in the energy field must first begin by determining how attributes of (1) a CPES (particularly, communication networks and associated cyber components of oil and gas, utility, and new/renewable energy companies), (2) the resource units generated by that system (e.g., oil, gas, electricity, wind, solar, nuclear, etc.), (3) the end users of that system (e.g., transportation, industry, residential and commercial sectors, and exports), and (4) the government system (e.g., national government) "jointly affect and are indirectly affected by interactions and resulting outcomes achieved at a particular time and place" (Ostrom 2007, 15182)—figure 9.



Source: Adapted from Ostrom's framework for analyzing complex systems.
Figure 9. A multitier framework for analyzing energy security at the state level.

3.2.2 Reframing: the regional positions on cyber security during smart and sustainable low-carbon energy transitions

The regional energy and cyber security interests are thus linked to both the collective position of states and the position of all other regional actors that can affect smart and sustainable low-carbon energy transitions. It is therefore important to understand how the priorities of cyber and energy security differ from one nation to another within a region (concrete), and the influence of these states to enforce their vision within a CSA when compared to all other states. Each state's priority represents a position that the member state wants to impose on the larger collective position. Reframing these positions will help prioritize these—often-conflicting—positions among states, influencing both regional responses and outcomes (figure 10).



Source: Author's representation (adapted from Ostrom's multitier framework for analyzing complex systems).
Figure 10. The proposed multitier cyber framework for assessment of regional cyber-physical energy systems (CPES) within the purview of collective security alliances.

Within each specific geo-energy system of various CSAs, we first must compare and contrast the national perceptions on (1) vital energy systems, primary energy sources, and their interactions (what to protect?), (2) cyber threats to these national systems, sources, and interactions (from what risks to protect?), and (3) the means available to protect from these cyber threats. Then, cyber security threat clusters (classified by shocks and stresses) within national data sets must be

identified and classified regionally, together with the perceived national (and technological) constraints of addressing cyber threats to the energy systems. One such dataset is the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI), which focuses on five pillars of cyber resiliency: legal, technical, organizational, capacity building, and cooperation. The emerging regional clusters will form cyber-energy security islands—as opposed to sticking to Mackinder's 'World-Island'—that united will have a stronger voice in the strategy making of collective security alliances. To test this hypothesis, their official views must be compared to the official documents of collective security alliances to assess their level of influence within the alliance with respect to cyber security of CEI policies.

The CSA ends (policies) and ways (strategies and processes) for cyber security of CEI will be prioritized by synthesizing the positions of states, and considering their influence and motivations—together with those of supra-national organizations such as the IEA, EU, and OPEC—at the regional level. Here, one of the most ignored—and yet most important—communication channel is the cooperation between intelligence structures (Fägersten 2015), on which Collective Cybersecurity Structures rely on.

Edward Schaumberg Quade—RAND researcher credited for developing the systems analysis problem-solving methodology in public policy—argued that "no public policy question can be answered by analysis alone, divorced from political considerations" (Quade 1972, viii). Because of this the overarching research problem is framed to address cyber security strategies for protection of CEI rather than just national and regional policies. Strategies are more inclusive, and consider more than just the legislative branches. Therefore, within the framework above, national outcomes refer to national strategies (which are inclusive of existing policies), while regional outcomes to regional strategies. Additionally, within the proposed multitier cyber framework there are multiple regional levels of analysis, and within each regional level, multiple national levels (the strategies individual member states of each CSA).

3.3 The proposed framework approach

This proposed framework looks at Baldwin's definition of security as "low probability of damage to acquired values" (Baldwin 1997) and uses Baldwin's three questions—security for whom, for which values, and from what threats?—to refine the statement of problem. In other words, it addresses these questions using a Cherp and Jewell approach, refining them to 1) what critical systems to protect, 2) from which risks, and 3) by which means? (Cherp and Jewell 2014). In the context of cyber threats to critical energy infrastructure, the first question—what critical systems to protect?—will address critical energy systems within the context of energy security and environmental security. The second question—from which risks?—will address the cyber threats to these systems. Finally, the third question—by which means?—will address the means that CSAs have at their disposal to tackle these cyber threats to critical energy systems.

3.3.1 What to protect: critical energy systems in the context of energy security and environmental security

Policy documents of both nation-states and international organizations (IO) agree with the International Energy Agency (IEA) that reliable, stable, and uninterrupted supply of energy sources at an affordable price—energy security—is a requirement for peace (Gnansounou 2008, 3742; Haghighi 2008, 466; Pamir 2007, 262; S. Peters 2004, 190; Stefanova 2006, 91; Verrastro and Ladislaw 2007, 101; Von Hippel, Savage, and Hayes 2011, 6712; Yi-chong 2006, 265) and economic growth (Intharak 2007, 6; Atsumi 2007, 28; Balitskiy, Bilan, and Strielkowski 2014, 123; Bambawale and Sovacool 2011/5, 1949; Climent and Pardo 2007/1, 522; Murad et al. 2019, 22). At the national level, these correlations transformed energy security into "a question of national strategy" (Yergin 2006, 69). In the words of Barack Obama, the 44TH President of the United States during an address given at the White House on January 26, 2009, "no single issue is as fundamental to [a nation's] future as energy" (Raphael and Stokes 2014, 184). Energy security became a key driver of

economic and foreign policies (McCain 2007, 32), and thus an important factor to consider in "smart and sustainable" (Elias G. Carayannis and Rakhmatullin 2014, 212) "low-carbon energy transitions" (Bridge et al. 2013, 331; Geels 2014, 30; Goldthau and Sovacool 2012, 232).

3.3.2 From which risks to protect: cyber threats to critical energy systems

Global economic growth is threatened by a nexus of geo-STEPE risks (Elias G. Carayannis 2011): geo-socio-cultural (water crises and spread of infectious diseases), geo-technological (cyber attacks and critical information infrastructure breakdown), geo-economic (fiscal crises), geopolitical (interstate conflicts and terrorist attacks), and geo-ecological (climate change, extreme weather, natural disasters) threats (World Economic Forum 2019, 4). This dissertation addresses the "rapidly evolving energy systems as cyber-based physical systems" (Ilic et al. 2010, 825) within the energy and environment context (smart and sustainable low-carbon energy transitions). Cyber-physical systems (CPS) are defined as the integration of "computation and physical processes, [where] embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa" (E. A. Lee 2008). As early as 2007, Project AURORA, an Idaho National Laboratory (INL) staged cyberattack against cyber-physical energy systems, "demonstrated how a cyberattack could be used to destroy power generation equipment" (Congressional Research Service 2018, 17). Examples of advanced persistent threats (APTs) that could be used against critical energy systems include variations of Stuxnet, Duqu, or Black Energy. For example, Disakil, an upgraded version of Black energy, "is being linked to the Ukrainian power outages in December, 2015" (Leszczyna 2018, 70). These types of cyber threats to critical energy systems are very little understood, particularly within the context of smart and sustainable low-carbon energy transitions.

3.3.3 By which means to protect—the means that Collective Security Alliances have at their disposal to increase the resilience of critical energy systems to cyber threats

In the traditional security environment (prior to the emergence of new environmental and technological risks), the security studies field considered energy security at either the level of nation-states or at the global level. Within the nation-state context, the study of energy security explores how energy needs shape the strategies of sovereign states and it looks at the energy policies of producer and consumer states as the main drivers behind structural shifts in the global energy supply chains (Bush 2002, 19; E. S. Downs 2004, 21; Kuzemko 2011; Löschel, Moslener, and Rübbelke 2010, 1665). This nexus between energy economics and security at the nation-state level—see the case of China (Chang and Koh 2012, 14; Qinhua 2007, 2)—is considered within a national-level political structure where the "anarchic structures" (Kenneth N. Waltz 1979, 198) of global and regional governance systems are subordinate to the supremacy of state security. The methodology used by the IEA in developing its Model of Short-term Energy Security—MOSES (Jewell 2011, 6)—for example, compared the risks and resilience of energy systems within IEA member states without much regard to specific regional contexts. At the global level, in the contemporary security environment (with the emergence of new environmental and technological risks) there are both analyses of energy security governance arenas (Cherp, Jewell, and Goldthau 2011, 75; Goldthau and Witte 2010)—where energy security focus on most common threats "affecting significant parts of the world's population" (Cherp et al. 2012, 334)—and of proposals for improved global energy regimes—"a variety of different strands of diplomatic, economic and technological activity stitched together as a single (albeit loose) regime" to manage smart and sustainable low-carbon energy transitions (Victor, Joy, and Victor 2006, 42); also argued by (Victor and Yueh 2010; Jewell, Cherp, and Riahi 2014).

While much has been written lately on the impact of economic, environmental, geopolitical, and societal risks to smart and sustainable low-carbon energy transitions at national and global levels (Elias G. Carayannis, Barth, and Campbell 2012; Chuang et al. 2019; Frondel et al. 2010; L.

Hughes 2009; Wang et al. 2018), very few studies address the risks of technology—in particular the threat of cyber-attacks—to smart and sustainable low-carbon energy transitions at the regional levels. The link between cyber attacks and environmental security is also little understood at the regional levels. This is despite the fact that the World Economic Forum Global Risks Report has designated climate change and cyber-attacks the two highest impact and highest likelihood global threats for 2019 (World Economic Forum 2019, 5). This dissertation argues that a cyber attack on new energy technologies could have major negative implications for smart and sustainable low-carbon energy transitions at national levels. Nevertheless, in recent years, more academic scholarship—particularly peer-reviewed articles published in *Energy Policy (Chen, Kim, and Yamaguchi 2014; Jewell, Cherp, and Riahi 2014; Umbach 2010)*—began exploring energy security (traditionally of high importance for the nation states) within the context of renewables and smart and sustainable low-carbon energy transitions (traditionally of high importance for the global energy regimes). These studies analyze smart and sustainable low-carbon energy transitions at the global level and energy security at both the global and the regional level—dealing primarily with artificially constructed regions that sometime make little economic and geographic sense (King and Gulledge 2013, 39). With very few exceptions—one being the EU (Gracceva and Zeniewski 2014), where regional integration "accounts for the functional replacement of sovereignty through [supra-national] institutions" (Stefanova 2006, 91)—these regions do not have clear regional energy security agendas or policies. As a result, the literature addressing energy security in the context of renewables and smart and sustainable low-carbon energy transitions policies only examines energy security as an objective concept limited to the coordinated response of importing countries to unreliable suppliers, to the interest alignment of the OPEC member states, and to the emergence of "various specialized agreements that manage the externalities of producing, transporting and using energy" (Victor, Joy, and Victor 2006, 39). While political, economic, ecological, and socio-cultural risks to smart and sustainable low-carbon energy transitions are addressed in these studies, technological risks are almost entirely ignored.

With the evolution of collective economic alliances of the 21st Century challenging the centrality of states in the anarchical nature of the international system, the former are emerging as polycentric governance systems "with various parts fostering complementary approaches necessary for addressing the highly interlinked energy challenges," (Cherp, Jewell, and Goldthau 2011, 75) and for managing a more complex energy landscape at the advent of technology risks (Herd and Kriendler 2013). Within these economic spaces, national energy security becomes more dependent "on how countries manage their relations with one another, whether bilaterally or within multilateral frameworks" (Yergin 2006, 82) than on domestic energy policy decisions. Since most cyber/technological threats, like energy threats, "travel more easily over short distances than over long ones," (Buzan and Wæver 2003, 4) one can observe the emergence of geo-energy spaces "where a precise set of energy relationships take place, among different agents—producer states, enterprises and consumer governments—who are active within it," (Mañé-Estrada 2006, 3785) and where a nexus of regional (rather than global) energy and cyber security strategies act as a more efficient driver of smart and sustainable low-carbon energy transitions. Currently, there is almost no research on the securitization—that is, "a gradual process wherein political choices are made to frame certain issues in particular ways" (K. Peters 2018, S196)—of the new energy sources supply chains (production, transportation, and distribution) at the regional level as a result of growing technological risks. Furthermore, there is virtually no academic study drawing a parallel between current regional energy securitization efforts and the shift from vertical (state-level) toward horizontal (systemic-level) authority cyber defense structures within these geo-energy spaces.

Collective security alliances (CSA) are becoming increasingly important in shaping the protection policies of regional and global energy systems in the wake of growing technological risks. The uninterrupted supply of vital energy services globally is increasingly dependent on an intricate system of regional energy market interdependencies and "vast cross-border infrastructure networks" (Chester 2010/2, 887) that are vulnerable to cyber attacks (Lacher and Kumetat 2011, 4473; Onyeji, Bazilian, and Bronk 2014; Pearson 2011, 5211; Rinaldi 2004, 2). While global energy

security complexes are extensively penetrated by both powerful states and international organizations (or global regimes)—as was discussed in the previous chapter (this dissertation's literature review)—"their regional dynamics nonetheless have a substantial degree of autonomy from the patterns set by the global powers" (Buzan and Wæver 2003, 4). CEIP (Luiijf et al. 2009), for example, no longer falls under the sole responsibility of states, but also under the responsibility of CSAs that these states belong to (Colesniuc 2013, 125; Pescaroli and Alexander 2016; Pursiainen 2009). Thus, the national definition of energy security needs not only to be expanded "to cope with the challenges of a globalized world," (Yergin 2006, 78) but also to cope with the technological challenges of a regionalized one, where the notion of national energy independence is replaced with that of regional energy sustainability (Hernández et al. 2004/2, 385), resilience (Erker, Stangl, and Stoeglehner 2017), affordability (Walker et al. 2015), social (equity and health) (Vera and Langlois 2007, 878), and cyber security (Gheorghe and Muresan 2011; Nepal and Jamasb 2013, 9).

3.4 Case study selection

While looking at multiple geo-energy spaces (and their respective CSAs) to implement the proposed framework of analysis during smart and sustainable low-carbon energy transitions, this study will focus on NATO, which owns several pipeline systems. The criteria used to select NATO for the purpose of this assessment was limited to the actual ownership of cyber-physical energy systems, the size in terms of membership within the Euro-Atlantic region, as well as maturity and stability of the organization, access to information (available data), and transparency of cyber-physical geo-energy systems and policies of the CSA. NATO also recognizes environmental considerations in its planning and operations. This answers Objective 3: apply the proposed methodology to a CSA that is already invested in protecting CPES in the cyber domain. This also helps answer Research Question 1 (RQ1): What is the CEIP role of CSAs in the cyber domain (i.e. through their official documents)?

This assessment will focus on the cluster of 5 NATO countries—Belgium, France,

Germany, Luxemburg and the Netherlands—that are part of the Central Europe Pipeline System, or CEPS, which is the largest the NATO petroleum pipeline system in Europe, and is used to deliver fuel to both military and non-military clients. The criteria used to select the cluster of states was limited to the sharing of responsibilities for the security of a NATO CPES, concurrent membership within NATO and the EU, as well as membership in other major sub-regional political and economic alliances. All five CEPS 'host nations' belong to the two biggest CSAs within the Euro-Atlantic region: 1) NATO; and 2) the EU within the framework of the CSDP. Within the E.U. framework, each country also has environmental obligations. Furthermore, each host nation belongs to at least one more sub-regional european politico-economic alliance, such as the G6 (EU) after BREXIT, Eu Med and Benelux (table 1).

Sub-Regional Alliances		Nation-States	EU	EURO	Shengen	NATO
BENELUX		Belgium	1958	1999	1995	1949
		Nethrelands	1958	1999	1995	1949
		Luxembourg	1958	1999	1995	1949
G6 (EU) after BREXIT	EU Med	France	1958	1999	1995	1949
		Germany	1958	1999	1995	1955

Source: Author's own representation.
Table 1: List of major political, economic, and collective security alliances that CEPS host nations belong to.

3.5 Applying Baldwin's questions at the national level

Analysis of national-level documents and interviews have been conducted to answer Baldwin's three questions at the national level. In the absence of publicly available data on cyber threats to CEPS at national levels, 30 subject matter experts (both military and civilian mid-level engineers and security professionals) from the five host nations were interviewed. These interviews included six Belgian and six Luxembourg government cyber security subject matter experts with specific knowledge of the Belgian Pipeline Organisation management and operations; three government and three private French cyber security subject matter experts with specific knowledge of TREPIL management and operations; six German government and private industry cyber security subject matter experts with specific knowledge of FBG management and operations; and six government cyber security subject matter experts with specific knowledge of the Netherlands

Defence Pipeline Organisation management and operations. These interviews were conducted during a Fellowship with the NATO Energy Security Centre of Excellence in Vilnius, Lithuania.

The 30 interviews were open ended and were to quantify data for a CARVER Analysis matrix (answering "what to protect" question), an adversary prioritization matrix based on capability and intent (answering "from what threats to protect" question), and to validate GCI data (answering "by what means to protect" question). This data is needed to answer Research Question 2 (RQ2): how can NATO as a CSA prioritize support to CEPS as a regional energy system—geo-energy system—and its prospects, considering 1) the general aim of NATO CEPS Programme; 2) its conventional/mainstream security challenges in the cyber domain; 3) the security challenges and general policy contexts of the CEPS hosts; and 4) the configuration of their cyber physical systems (in relation to energy resources, infrastructures, and geographies)? The experts interviewed had specific knowledge of the CEPS vulnerabilities and careful consideration was given to ensure that no classified information is being disclosed.

3.5.1 What to protect

This methodology will use the CARVER weighting scheme—discussed in the literature review and based on **C**riticality, **A**ccessibility, **R**ecuperability, **V**ulnerability, **E**ffect, and **R**ecognizability factors—to assess and prioritize cyber security risks to CEI. This methodology was selected because it is used by both NATO (Kulawiak et al. 2009) and the EU (Marvin et al. 2009) to "obtain the rankings of the alternatives" (Greaver et al. 2018) in prioritizing what systems to protect first from adversary attacks. It is important to note that "as an asset-level tool, CARVER does not account for the interconnected nature of an infrastructure or how that interconnectedness can lead to cascade failures" (Lewis et al. 2012). Responders were asked to list their alternatives (to identify critical systems) and rate them on a 1 to 5 scale according to the 6 criteria:

Criticality. Criticality is defined as "the potential for, and exposure to, supply disruption" (Roelich et al. 2014). The scale is separated as such:

- 5: Loss would cripple infrastructure

- 4: Loss would affect infrastructure performance considerably
- 3: Loss would reduce infrastructure performance
- 2: Loss may reduce infrastructure performance
- 1: Loss will not affect infrastructure performance

Accessibility. Accessibility is defined as "the level of efforts made [by adversaries to achieve] interruptions of service" (Ben Khelil, Othmani, and Bouslama 2015). The scale is separated as such:

- 5: Easily accessible. Very low security
- 4: Easily accessible. Low security
- 3: Accessible
- 2: Difficult to gain access
- 1: Very difficult to gain access

Recuperability. Recuperability is defined as "the ability to recover" (Taormina 2015) from adversary attacks and/or system failure. The scale is separated as such:

- 5: Extremely difficult to replace. Long down time (>1 month)
- 4: Difficult to replace. Long down time (<1 month)
- 3: Can be replaced in relatively short time (<2 weeks)
- 2: Easily replaced in a short time (<1 week)
- 1: Easily replaced in a short time (hours or days)

Vulnerability. Vulnerability is defined as the risk of the system to adversary means and expertise. The scale is separated as such:

- 5: Adversary has means and expertise to attack
- 4: Adversary probably has the means and expertise to attack
- 3: Adversary may have the means and expertise to attack
- 2: Adversary will probably have no impact
- 1: Adversary does not have much capability to attack

Effect. Effect is defined as "the degree of damage (or loss)" (Kárník, Schenkova, and Schenk 1984) to one or more of the 5 helices: government, business, academia, civilians, and the environment (E. G. Carayannis et al. 2018). The scale is separated as such:

- 5: Would have devastating negative effects on government, business, academia, civilians AND/OR environment
- 4: Would have significant negative effects on government, business, academia, civilians AND/OR environment
- 3: Would have negative effects on government, business, academia, civilians AND/OR environment
- 2: May have negative effects on government, business, academia, civilians AND/OR environment
- 1: Will not have negative effects on government, business, academia, civilians AND/OR environment

Recognizability. Recognizability is defined as "the ability of a system to be recognized" (Yassierli, Vinsensius, and Mohamed 2019) for the purpose of targeting by potential adversaries. The scale is separated as such:

- 5: Easily recognized by all with no confusion
- 4: Easily recognized by most with no confusion
- 3: Recognized with some training
- 2: Hard to recognize. Confusion probable
- 1: Extremely difficult to recognize without extensive orientation

VALUE	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizability
5	Loss would cripple infrastructure	Easily accessible. Very low security	Extremely difficult to replace. Long down time (>1 month)	Adversary has means and expertise to attack	Would have devastating negative effects on government, business, academia, civilians AND/OR environment	Easily recognized by all with no confusion
4	Loss would affect infrastructure performance considerably	Easily accessible. Low security	Difficult to replace. Long down time (<1 month)	Adversary probably has the means and expertise to attack	Would have significant negative effects on government, business, academia, civilians AND/OR environment	Easily recognized by most with no confusion
3	Loss would reduce infrastructure performance	Accessible	Can be replaced in relatively short time (<2 weeks)	Adversary may have the means and expertise to attack	Would have negative effects on government, business, academia, civilians AND/OR environment	Recognized with some training
2	Loss may reduce infrastructure performance	Difficult to gain access	Easily replaced in a short time (<1 week)	Adversary will probably have no impact	May have negative effects on government, business, academia, civilians AND/OR environment	Hard to recognize. Confusion probable
1	Loss will not affect infrastructure performance	Very difficult to gain access	Easily replaced in a short time (hours or days)	Adversary does not have much capability to attack	Will not have negative effects on government, business, academia, civilians AND/OR environment	Extremely difficult to recognize without extensive orientation

Source: Scale adjusted from (Pohl et al. 2013).
Table 2: CARVER weighing scheme of system protection.

The Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors were weighed equally (as it is performed by NATO) and alternative systems to be protected were prioritized based on the sum of these factors from highest to lowest. For the purpose of protecting the responders from revealing any information that may have been deemed as classified, alternatives of vulnerable systems were then split into two categories: 1) OT (ICS, SCADA, pumps, etc.), and 2) IT (intellectual property, information security, etc.). The values reflect the highest valued alternative in the OT category and the highest valued alternative in the IT category.

3.5.2 From what threats to protect?

Respondents were asked to identify the main threats to the OT most vulnerable system. For the purpose of this assessment, adversary threats were classified into 1) Terrorism; 2) Nation states; 3) Corporate espionage; and 4) Criminals. The US National Institute of Standards and Technology (NIST) scale was then used to prioritize adversarial threats. Responders were asked to prioritize these threats based on capabilities and intent (on a scale from 1 to 5).

Capability. Capability is defined as "the capacity and ability" (Daniel, Lauby, and Maillant 1989) of an adversary to attack a system. The scale is separated as such (Bodeau, Fabius-Greene, and Graubart 2010):

- 5 (Advanced): The adversary is very sophisticated and well resourced and can generate its own opportunities to support multiple successful, continuous, and coordinated attacks
- 4 (Significant): The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks
- 3 (Moderate): The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks

- 2 (Limited): The adversary has limited resources, expertise, and opportunities to support a successful attack
- 1 (Unsophisticated): The adversary has very limited resources, expertise, and opportunities to support a successful attack

Intent. Intent is defined as "the expected behaviour" (Sim and Duffy 1994) of the adversary to target a system. The scale is separated as such (Bodeau, Fabius-Greene, and Graubart 2010):

- 5 (Advanced): The adversary seeks with great determination to undermine, impede severely, or destroy, a mission, program, or enterprise, by exploiting a presence in the organization's systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal
- 4 (Significant): The adversary seeks with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's systems or infrastructure. The adversary is very concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly while preparing for future attacks
- 3 (Moderate): The adversary seeks to obtain or modify specific, critical information and/or to usurp or disrupt the organization's cyber resources by establishing a foothold in the organization's systems or infrastructure, but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., exfiltration) over long time periods. The adversary is willing to knowingly impede aspects of the organization's mission to achieve these ends
- 2 (Limited): The adversary actively seeks to obtain critical information and/or to usurp or disrupt the organization's cyber resource, and does so without concern about detection of their attacks or disclosure of tradecraft

- 1 (Unsophisticated): The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about detection of their attacks or disclosure of tradecraft

The threat of a cyber-attack against Industrial Control Systems is then calculated using the formula "Threat=Intent x Capability" (Cook et al. 2016).

VALUE	LEVEL	Capability	Intent
5	**Advanced**	The adversary is very sophisticated and well resourced and can generate its own opportunities to support multiple successful, continuous, and coordinated attacks	The adversary seeks with great determination to undermine, impede severely, or destroy, a mission, program, or enterprise, by exploiting a presence in the organization's systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal
4	**Significant**	The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks	The adversary seeks with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the future, by maintaining a presence in the organization's systems or infrastructure. The adversary is very concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly while preparing for future attacks
3	**Moderate**	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks	The adversary seeks to obtain or modify specific, critical information and/or to usurp or disrupt the organization's cyber resources by establishing a foothold in the organization's systems or infrastructure, but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., exfiltration) over long time periods. The adversary is willing to knowingly impede aspects of the organization's mission to achieve these ends
2	**Limited**	The adversary has limited resources, expertise, and opportunities to support a successful attack	The adversary actively seeks to obtain critical information and/or to usurp or disrupt the organization's cyber resource, and does so without concern about detection of their attacks or disclosure of tradecraf
1	**Unsophisticated**	The adversary has very limited resources, expertise, and opportunities to support a successful attack	The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about detection of their attacks or disclosure of tradecraft

Source: Adapted from (Bodeau, Fabius-Greene, and Graubart 2010).
Table 3: Adversary Prioritization.

3.5.3 By what means to protect

The ITU—composed of over 800 members from industry, government, and academia—uses the GCI to rank preparedness of nation states to tackle cyber threats. This is also an ideal framework (with some omissions) to assess the cyber preparedness of CEPS member states to tackle cyber threats to Operational Technologies. Particularly, the GCI considers legal, technical, organizational, capacity, and cross border cooperation (in a multi-stakeholder environment) pillars that are ideal for our assessment (ITU 2019):

Legal. The legal pillar assesses "the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime" (ITU 2019, 7) based on the following indicators:

1. Cybercriminal Legislation
2. Cybersecurity Regulation
3. ~~Containement or curbing of spam~~ (removed from the methodology's assessment due to our focus on OT)

Technical. The technical pillar assesses "the existence of technical institutions and framework dealing with cybersecurity" (ITU 2019, 8) based on the following indicators:

1. CIRT (computer incident response team), CSIRT (computer security incident response team) or CERT (computer emergency response team)
2. Framework for the implementation of cybersecurity standards
3. Standardization body within the country
4. ~~Technical mechanisms and capabilities to address spam~~ (removed from the methodology's assessment due to our focus on OT)
5. ~~Cloud for cybersecurity purposes in the public sector~~ (removed from the methodology's assessment due to our focus on OT)

6. ~~Child Online Protection~~ (removed from the methodology's assessment due to our focus on OT)

Organizational. The organizational pillar assesses "the existence of policy coordination institutions and strategies for cybersecurity development at the national level" (ITU 2019, 8) based on the following indicators:

1. National strategy for cybersecurity
2. National body/agency responsible for cybersecurity and critical information infrastructure protection
3. Metrics used to measure cybersecurity development at a national level

Capacity Building. The Capacity building pillar assesses "the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity building" (ITU 2019, 8) based on the following indicators:

1. Public awareness campaigns in cybersecurity
2. Framework for the certification and accreditation of cybersecurity professionals
3. Government development or support in professional training /courses in cybersecurity
4. Educational programs or academic curriculums in cybersecurity
5. R&D programs
6. Incentive mechanisms to encourage capacity building in the field of cybersecurity
7. Home grown cybersecurity industry

Cooperation. The cooperation pillar assesses "the existence of partnerships, cooperative frameworks and information sharing networks" (ITU 2019, 8) based on the following indicators:

1. Bilateral agreements on cybersecurity cooperation
2. Multilateral or international agreements on cybersecurity cooperation

3. Participation in international fora/associations dealing with cybersecurity
4. Public-Private Partnerships
5. Inter-agency partnerships
6. Best practice

Because the GCI uses additional indicators that are not relevant for this methodology, the weights had to be adjusted, as seen in table 4.

Indicators	GCI Weight	Adjusted Weight
LEGAL	0.2	0.2
Cybercriminal Legislation	0.079	0.1
Cybersecurity Regulation	0.079	0.1
~~Containement or curbing of spam~~	0.042	NA
TECHNICAL	0.2	0.2
CIRT, CSIRT or CERT	0.065	0.1
Framework for the implementation of cybersecurity standards	0.035	0.054
Standardization body within the country	0.03	0.046
~~Technical mechanisms and capabilities to address spam~~	0.024	NA
~~Cloud for cybersecurity purposes in the public sector~~	0.019	NA
~~Child Online Protection~~	0.027	NA
ORGANIZATIONAL	0.2	0.2
National strategy for cybersecurity	0.092	0.092
National body/agency responsible for cybersecurity and critical information infrastructure protection	0.063	0.063
Metrics used to measure cybersecurity development at a national level	0.045	0.045
CAPACITY	0.2	0.2
Public awareness campaigns in cybersecurity	0.036	0.036
Framework for the certification and accreditation of cybersecurity professionals	0.027	0.027
Government development or support in professional training /courses in cybersecurity	0.032	0.032
Educational programs or academic curriculums in cybersecurity	0.032	0.032
R&D programs	0.026	0.026
Incentive mechanisms to encourage capacity building in the field of cybersecurity	0.024	0.024
Home grown cybersecurity industry	0.023	0.023
COOPERATION	0.2	0.2
Bilateral agreements on cybersecurity cooperation	0.038	0.038
Multilateral or international agreements on cybersecurity cooperation	0.038	0.038
Participation in international fora/associations dealing with cybersecurity	0.036	0.036
Public-Private Partnerships	0.034	0.034
Inter-agency partnerships	0.026	0.026
Best Practices	0.028	0.028
TOTAL	1	1

Source: Adjusted from (ITU 2019, 7).
Table 4: GCI indicators per pillar with original and adjusted weights for CEPS OT.

Because the GCI uses these indicators to compare readiness between nation states (rather than overall preparedness), for each country assessed, the most prepared received a 10, and the other countries were assessed in reference to this value. This is, however, valuable only to compare national-level cyber preparedness among the assessed states. Using the adjusted GCI indicators, the responders were used to make their own assessments of the CEPS infrastructure preparedness,

using a 1 to 10 scale adjusted from the Citizen Corps Public Readiness Index, which the US Federal Emergency Management Agency (FEMA) is using (Council for Excellence in Government 2006):

- 10: Nation state is prepared to defend CEPS OT from cyber threats
- 8 or 9: Nation state is close to being prepared to defend CEPS OT from cyber threats
- 7: Nation state has a good readiness foundation to defend CEPS OT from cyber threats, but there is room for improvement
- 6: Nation state understands the threat and wants to get prepared to defend CEPS OT from cyber threats
- 4 or 5: Nation state taking steps to understand the threat and wants to get prepared to defend CEPS OT from cyber threats
- 3 or below: Nation state does not understand the threat and what needs to be done to get prepared to defend CEPS OT from cyber threats

3.6 Reframing: addressing the research questions for NATO

After addressing Baldwin's questions at the national level, the answers will be conceptualized within the limits of official NATO documents and policies. This step will address objective 4: empirically validate the means and ways of NATO as a CSA in augmenting national CEIP efforts in the cyber domain by i) identifying patterns or clusters of cyber security issues, policies, and discourses relevant to CEPS (as a NATO defined geo-energy system); and ii) explaining these patterns or clusters in terms of geo-STEPE (Elias G. Carayannis 2011) policy contexts: geo-socio-cultural, geo-technological, geo-economic, geopolitical, and geo-ecological. A discussion about how these questions can be conceptualized for collective security alliances in general follows in chapter 5 (Discussions), which addresses objective 5: interpret and extrapolate results to validate the feasibility of CSAs to integrate the protection of national cyber-physical energy systems (CPES) into their mandate (the ends) and answers Research Question 3

(RQ3): how are the ends (i.e. defense and deterrence mandate) of these CSAs likely to change in the future to protect these geo-energy systems from emerging cyber-physical threats?

3.7 Contributions and Limitations

This research is innovative not just because it tackles a problem scarcely researched by the academia—namely the role of CSAs in the security of cyber-physical energy systems. Its methodology is also different from traditional studies of security issues because it offers a multi-tier framework applied at 3 levels of analysis: national, multi-national (sub-regional), and regional. The major limitation here is that only 5 member states (belonging to 2 regional alliances, and to 3 sub-regional alliances) are observed. This limitation, however, made it possible to draw a more comprehensive picture of energy security intricacies throughout each nation covered by the CEPS (at the sub-regional level of analysis). Another major limitation is that questions not answered by official documents and the GCI are addressed in interviews of stakeholders only from government and industry. This is because stakeholders in academia and civil society with specific knowledge of the CEPS systems could not be identified. This is not a matter of competency, but rather one of access to information: where previously published data that covers CEPS vulnerabilities have been classified. One such example is a recent study conducted by the NATO Energy Security Centre of Excellence in Vilnius, Lithuania, which was classified immediately upon completion in the fall of 2019. It is important that these stakeholders are also addressed in future studies, because they have the power to influence public opinion and, thus, future national cyber-security policies that could impact the role of NATO in guaranteeing the security of CEPS from future cyber-attacks.

Chapter 4

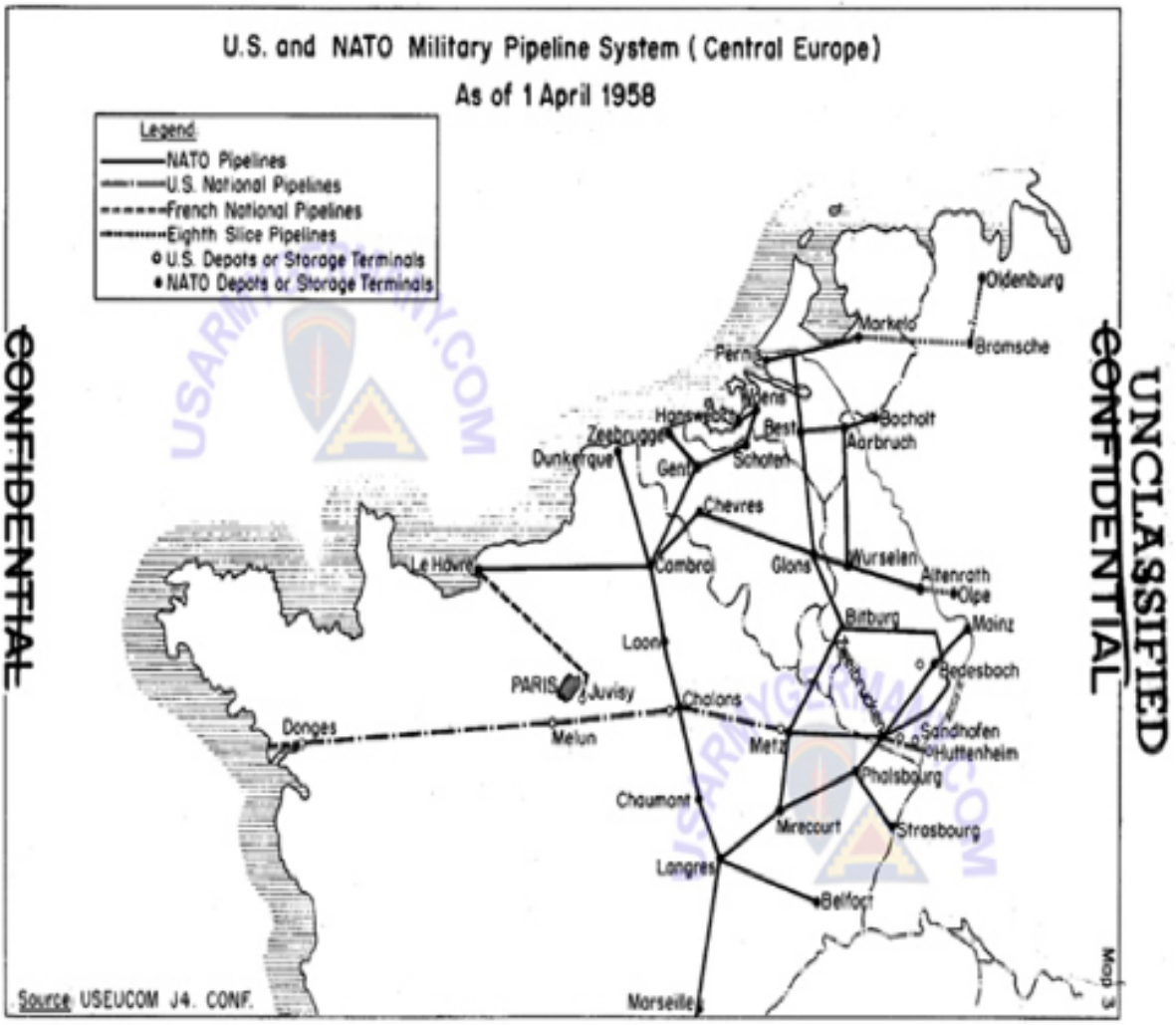
Data Presentation

Military operations in old NATO across Europe rely on eight national and two cross-border military distribution and storage systems that cover over 13,000 km and 13 NATO member states. These extensive pipeline configurations make up the broader NATO Pipeline System (NPS). The 8 national distribution systems (by size) are 1) two Turkish Pipeline Systems (TUPS, 3,204 km); 2) the United Kingdom Government Pipeline and Storage System (UKGPSS, 2,400 km); 3) the Northern Italy Pipeline System (NIPS, 797 km); 4) the Greek Pipeline System (GRPS, 784 km); 5) the Norwegian Pipeline System (NOPS, 99 km); 6) the Portuguese Pipeline System (POPS, 123 km); and 7) the Icelandic Pipeline System (ICPS, 19 km). The two cross-border pipelines are 1) the Central Europe Pipeline System (CEPS, 5,599 km across Belgium, France, Germany, Luxembourg and the Netherlands); and 2) the North European Pipeline System (NEPS, 676 km across Denmark and Germany). With the exception of CEPS, the cyber security and resilience of these NATO pipeline systems are guaranteed entirely by national organizations. NATO Petroleum Committee's responsibility in these cases is limited to managing NATO's fuel requirements (NATO 2017).

This chapter presents the data collected on the NATO Central Europe Pipeline System, with both regional and national cyber-physical threats from theory, policy, politics and practice (TP3) perspectives (Elias G. Carayannis, Samara, and Bakouros 2015). More specifically, this chapter looks at how NATO policies, practices and strategies influence the regional, sub-regional and national cyber-physical protection of geo-energy systems. Particular attention is given to the operation of CEPS (as a sub-region) and its cluster of host nations—Belgium, France, Germany, Luxembourg and the Netherlands—which belong to both NATO and the EU (also a CSA within the framework of the CSDP).

4.1 Cyber security and resilience of the Central Europe Pipeline System

The CEPS is the largest integrated, cross-border tactical NATO pipeline system covering 5,599 km (with the ability to deliver 2.5 million liters of fuel per day) and 33 depots with a storage capacity of over 1,250,000 m^3 throughout Belgium, France, Germany, Luxemburg and the Netherlands (József 2013, 31). Bulk petroleum is brought inland through tanker off-loading facilities at the ports of Marseille, Le Havre and Dunkerque in France, and Rotterdam in the Netherlands (Garrett 1993, 11). It is then pumped into CEPS, which helps supply dozens of military air bases (such as Ramstein and Spangdahlem) and civilian national airports (to include Amsterdam, Brussels, Cologne-Bonn, Frankfurt, Luxembourg, and Zürich) with most—and in some cases, all—of their jet fuel requirements (Rosner 2004, 214). These airports are supplied across three feeder routes: 1) from France to Germany through Marseilles – Lyon – Zweibrücken; 2) from the Netherlands to Belgium, Luxemburg, and Germany through Rotterdam/Amsterdam – Bierset – Luxemburg – Frankfurt – Stuttgart – Munich; and 3) in France through Le Havre/Dunkirk – Rems – Langres – Belfort (see figure 11). Both military and civilian airports are dependent on the CEPS pipeline along these three feeder routes primarily due to the lower price and higher speed of transporting jet fuel via pipeline, versus other regional alternatives (such as via rail and road).



Source: USEUCOM J4 report released on US ARMY GERMANY
Figure 11. Central Europe Pipeline System (CEPS) as of 1 April 1958.

On the military side, the pipeline was built during the Cold War to support NATO's "operational military requirements during peacetime, crisis and conflicts, including expeditionary operations" (József 2013, 31). From these lenses, one of the main advantages of the pipeline system is that pipelines present "extremely poor targets from enemy aircraft [and] pipeline damage can be repaired much faster than damaged railroads or highways" (József 2013, 32). To further increase the resilience of the system from successful potential attacks "separate and distinct military storage and distribution systems were set up, and are an integral part of the NATO pipeline system" (Khamashuridze 2008, 53). Today, these are all at risk not only from nation-state threats

(Khamashuridze 2008, 48), but also from "acts of terrorism, sabotage and organised crime" (NATO Heads of State and Government 1999).

On the civilian side, the pipeline system also plays a critical role during peace-time in assisting host countries protect from disruption of national fuel supplies due to bad weather conditions or internal political crises. A clear example of the latter is the use of CEPS by France (taking advantage of a military priority clause guaranteeing supply) to insure strategic fuel deliveries to Paris during the disruption of operations at civilian refineries and ports by labor unions - like it was the case in June of 2016 (Platts 2016). With energy operations in Europe "increasingly becoming the target of cyber-attacks with potentially catastrophic consequences" (Healey et al. 2016, 1), interest in defending the NATO CEPS from cyber attacks has also increased. All previous studies covering cyber threats to CEPS infrastructure have been classified, making it especially difficult for academia and civil society to contribute to this debate.

4.2 The role of the NATO CEPS Programme in cyber security and resilience

At the regional level, the strategic planning, operation (to include quality control) and maintenance of CEPS is coordinated by the CEPS Programme office, which is part of the NATO Support and Procurement Organisation (NSPO) and is located in Versailles, France. Apart from the Host Nations (Belgium, France, Germany, Luxemburg and the Netherlands), the CEPS Programme membership also includes the United States (József 2013, 31). The CEPS Programme acts as an intermediary between NATO and four national pipeline operators on all aspects pertaining to CEPS, to include management of suppliers and of military or civilian customers. These four pipeline operators are 1) the Belgian Pipeline Organization (BPO); 2) the TRAPIL pipeline operator (a French quasi-public corporation); 3) the Fernleitungs-Betriebs-gesellschaft (FBG) (a German quasi-public corporation); and 4) the Dutch Pipeline Organisation (DPO). Coordination with these pipeline operators is achieved through CEPS Programme's technical, business, and finance departments.

The cyber security and resilience of the pipeline system fall under the responsibility of the CEPS Programme Technical Department; but no guidelines are in place, however, what these responsibilities are. For example, the CEPS Programme Technical Department does not bother itself with securing the cyber-physical networks of CEPS suppliers (which include civilian import depots and refineries). These responsibilities fall under the purview of the NATO member states hosting these suppliers. Additionally, the cyber-physical protection of its 82 pump stations and other critical pipeline nodes fall under the responsibility of the national pipeline operators. The ends and ways driving the NATO CEPS Programme regional interests in protecting cyber-physical systems of critical energy infrastructure are linked to the collective position of the CEPS Host Nations (Belgium, France, Germany, Luxemburg and the Netherlands) and the United States.

4.3 Host Nations' role in the cyber-physical protection of the CEPS infrastructure

Within each the geo-energy system that encompasses the NATO CEPS, this section compares and contrasts the common perceptions of the CEPS host nations on (1) vital energy systems, primary energy sources, and their interactions (what to protect?), (2) the cyber threats to these national systems, sources, and interactions (from what risks to protect?), and (3) the means available to protect from these cyber threats. Then, cyber security threat clusters to CEPS (classified by shocks and stresses) within national data sets are identified and classified regionally, together with the perceived national (and technological) constraints of addressing cyber threats to the energy systems.

The reason behind the establishment of these NATO pipeline systems was to support the host nations "with bulk fuel up to or near front lines" during times of regional conflict (József 2013, 36). The growing dependence of host nations' civilian airports and air bases on jet fuel delivered by CEPS during times of peace, however, redefined the relationship between NATO and these host nations, particularly when it comes to addressing the growing cyber threats to CEPS. Today, the protection of the CEPS critical infrastructure is a joint responsibility of the NATO CEPS

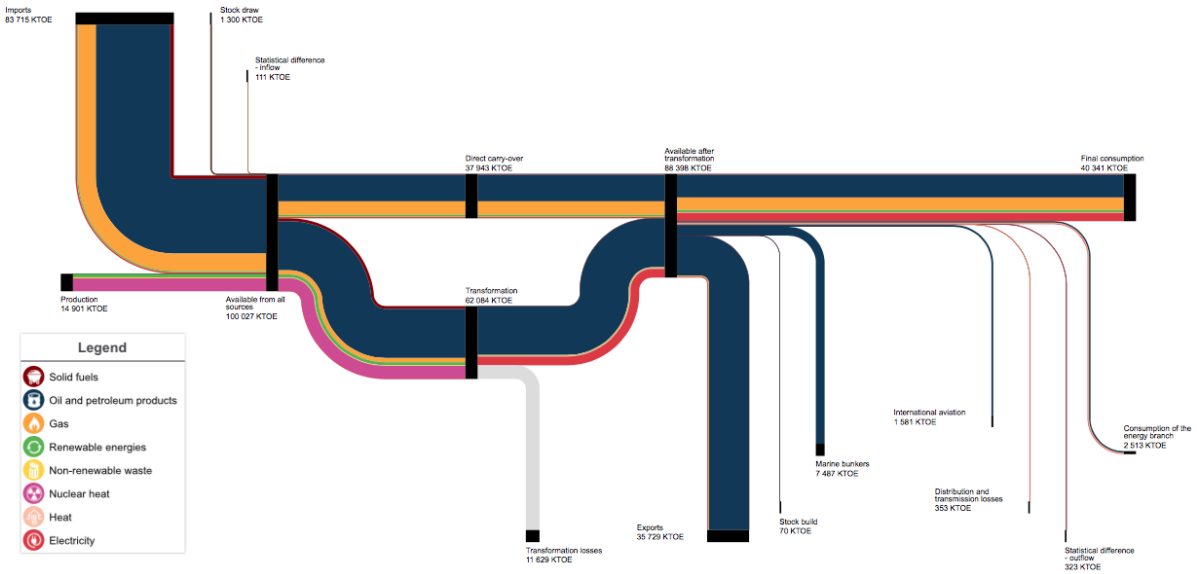
Programme and of the individual CEPS host nations and their respective pipeline operators (Simon 2005, 34). It is important, thus, to understand how the frameworks defining cyber security differ from one CEPS host nation to another within this specific geo-energy region (concrete), and the influence of these states to force their vision within NATO when compared to all other member states. Each NATO CEPS host nation's definition of cyber security within the context of critical energy infrastructure represents a position that the host nation wants to impose on the larger regional definition (or collective position). Reframing these positions will help prioritize the—often-conflicting—positions among these states.

4.3.1 Belgium and Luxembourg

The Belgian Pipeline Organization (BPO) is responsible for the operation and maintenance of CEPS in both Belgium and Luxembourg. This is despite the fact that the energy and cyber security ecosystem differs significantly between the two countries. This is evident, for example, if we compare the readiness of the two nations to react and recover from a major cyber-attack (cyber resilience). The Global Cybersecurity Index ranks Belgium's cybersecurity readiness as 18th in Europe and 30th globally; while Luxembourg's cybersecurity readiness is ranked as 7th in Europe and 11th globally (ITU 2019, 60).

Belgium: Belgium's energy security priorities tend to be focused more on reducing the use of fossil fuels and decarbonizing its economy (see figure 12) in the context of transitioning away from nuclear energy (IEA 2019a). With this important aspect in mind, Belgium views energy security as important because "energy can be used to put pressure on countries" (Flamant and Parrein 2017, 32). As a result of this focus, the protection of energy infrastructure from cyber threats is of lesser importance (strategically and in policies) for Belgium than the protection from irresponsible market players in the energy field. Nevertheless, the official definition of cyber security by the Belgian defence structures, does have implications for the energy field. Belgium defines cyber security as "a situation where the protection of the cyber environment is proportional to the cyber

threat and to the possible consequences of cyber-attacks. Cyber security stands for an absence of dangers or damage caused by the disruption, the breakdown or the abuse of ICT systems" (Flamant and Parrein 2017, 100). This includes the disruption of the energy supply, particularly given the increase in the overall number of cyber-attacks. According to the Belgium Cyber Emergency Response Team (CERT), the average number of reported cyber incidents per day increased to over 100 in 2016, of which 47% emerged from a growing number of IT and/or OT systems vulnerabilities. In the same year, two thirds of all Belgium companies became the victims of a cyber-attack (CERT 2019). Belgium has high "emergency oil stock levels" (IEA 2019a), so in the event of a cyber complex cyber-attack against the CEPS infrastructure, Belgium's airports and air bases would still have temporary access to fuel. Nevertheless, the cyber threat environment has forced the Belgian government to acknowledge that cyber threats (particularly against energy infrastructure) could affect future investments in the country: "The cyber environment can be used to inflict damage on our economy, our industry and the scientific potential of our knowledge society. In case of insufficient protection against cyber-attacks, our economy is exposed to risks that are likely to affect our country's attractiveness in terms of investments. [...] Considering the dangers facing our institutions, our enterprises and our citizens, cyber security will constitute a priority" (Flamant and Parrein 2017, 101). From the Belgian perspective, the protection of the nation's critical energy infrastructure (to include the protection of the NATO CEPS) is focused on three pillars: 1) the improvement of the "surveillance of critical infrastructure and societal sensitive targets" (Flamant and Parrein 2017, 34); 2) the adoption of offensive cyber capabilities, to include "an adequate level of cyber security of the communication and weapon systems of Defence and at the same time be capable to identify, manipulate and disrupt networks and systems of an opponent in order to restrain or destroy its freedom of action" (Flamant and Parrein 2017, 100); and 3) the minimization of impact by becoming "more energy efficient, [by increasing] the use of sustainable energy resources" (Flamant and Parrein 2017, 216).



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 12. 2017 Belgium Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

Results of Interviews:

Six Belgian government cyber security subject matter experts with specific knowledge of BPO management and operations were interviewed. Their responses are presented here.

What to protect: To ensure that no classified information is being disclosed, specific vulnerabilities were afterwards separated into the more generic OT and IT categories. Using the proposed CARVER criteria, we then added the answers on Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors (see table 5). For all responders, the criticality of OT ranged between 4 and 5, indicating the perception that a successful attack against OT infrastructure would either affect performance considerably or cripple infrastructure. IT Criticality averaged a 3 (the perception that a successful attack would reduce performance). The totals for each expert interviewer were then averaged to assess which type of system (OT or IT) should be secured first (see table 6). This indicates that in Belgium, government cyber physical systems experts believe that protection of OT CEPS systems should take priority over IT systems in the near to medium term. On the bright side, experts agreed that OT systems vulnerabilities are very hard to recognize, meaning only certain nation state adversaries currently pose a threat to these systems.

		CARVER	What to protect?	
			OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Belgium				
GOVERNMENT	Respondent 1	Criticality	4	3
		Accessibility	2	1
		Recuperability	1	1
		Vulnerability	3	4
		Effect	2	2
		Recognizability	1	3
		TOTAL	**13**	**14**
	Respondent 2	Criticality	4	4
		Accessibility	2	2
		Recuperability	1	1
		Vulnerability	3	3
		Effect	2	2
		Recognizability	2	4
		TOTAL	**14**	**16**
	Respondent 3	Criticality	4	3
		Accessibility	1	1
		Recuperability	1	1
		Vulnerability	4	5
		Effect	1	2
		Recognizability	2	3
		TOTAL	**13**	**15**
	Respondent 4	Criticality	5	4
		Accessibility	5	3
		Recuperability	2	1
		Vulnerability	5	5
		Effect	3	2
		Recognizability	3	4
		TOTAL	**23**	**19**
	Respondent 5	Criticality	5	2
		Accessibility	5	3
		Recuperability	2	1
		Vulnerability	4	4
		Effect	3	3
		Recognizability	3	2
		TOTAL	**22**	**15**
	Respondent 6	Criticality	4	2
		Accessibility	3	3
		Recuperability	1	1
		Vulnerability	3	4
		Effect	1	1
		Recognizability	3	3
		TOTAL	**15**	**14**

Source: Author's interpretation

Table 5. Results of CARVER cyber analysis for CEPS infrastructure in Belgium.

		1. What to protect?	
		OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Belgium			
GOVERNMENT	Respondent 1	13	14
	Respondent 2	14	16
	Respondent 3	13	15
	Respondent 4	23	19
	Respondent 5	22	15
	Respondent 6	15	14
	Average CEPS Score	**17**	16

Source: Author's interpretation
Table 6. Prioritization of what CEPS systems to protect from cyber-attacks in Belgium.

From what threats to protect: OT threats were then classified into 4 categories: terrorism, nation states, corporate espionage, and criminals. All experts interviewed found the capabilities of nation states to be above all other threats. The intent scored higher, however, on the terrorism category. This is explained by the fact that, while nation states have the capabilities to conduct a successful cyber-attack against CEPS, the fear of NATO retribution deters them from using them. Corollary, while terrorists have the intent to target the CEPS infrastructure, they lack the knowledge to construct the needed capabilities. All cyber experts agreed, however, that this may change in the future, as state capabilities are released into the wild and become accessible to criminals and terrorists. The 6 Belgian government cyber experts prioritized these threats based on their capabilities and intent, and we calculated overall threat as 'capability x intent' (see table 7). Average threat was then assessed in table 8, indicating that nation states represent the highest cyber threat to the CEPS infrastructure from the perspective of Belgian experts.

			2. From what threats to protect			
			Aversary risks			
		Threat	Terrorism	Nation states	Corporate espionage	Criminals
Belgium						
GOVERNMENT	Respondent 1	Capability	2	4	2	1
		Intent	5	3	3	3
		Threat	**10**	**12**	**6**	**3**
	Respondent 2	Capability	1	3	2	2
		Intent	5	3	3	3
		Threat	**5**	**9**	**6**	**6**
	Respondent 3	Capability	1	3	3	2
		Intent	5	2	3	3
		Threat	**5**	**6**	**9**	**6**
	Respondent 4	Capability	2	5	4	4
		Intent	5	4	4	2
		Threat	**10**	**20**	**16**	**8**
	Respondent 5	Capability	3	5	5	3
		Intent	5	4	4	5
		Threat	**15**	**20**	**20**	**15**
	Respondent 6	Capability	2	3	3	3
		Intent	5	3	3	3
		Threat	**10**	**9**	**9**	**9**

Source: Author's interpretation

Table 7. Results of CEPS cyber threat analysis for Belgium.

		2. From what threats to protect			
		Aversary risks			
		Terrorism	Nation states	Corporate espionage	Criminals
Belgium					
GOVERNMENT	Respondent 1	10	12	6	3
	Respondent 2	5	9	6	6
	Respondent 3	5	6	9	6
	Respondent 4	10	20	16	8
	Respondent 5	15	20	20	15
	Respondent 6	10	9	9	9
	Average CEPS Score	9	**13**	11	8

Source: Author's interpretation

Table 8. Prioritization of cyber threats against CEPS in Belgium.

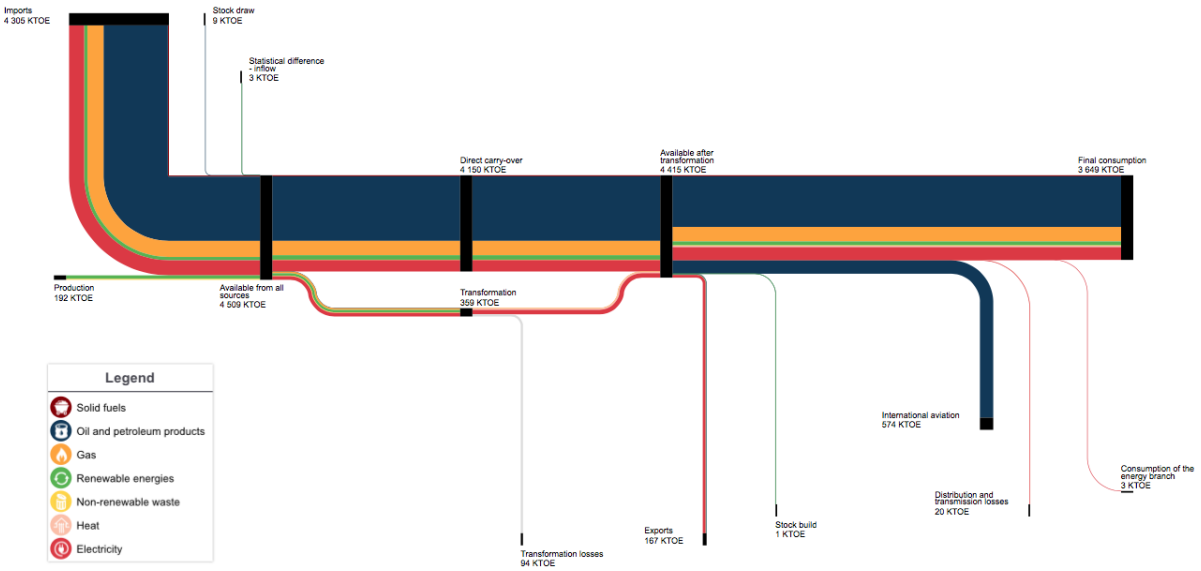
By what means to protect: Most government cyber experts in Belgium were unfamiliar with the GCI methodology, and found it useful in assessing areas of improvement addressed in table 9. The data collected shows that overall, experts agree that Belgium needs to pay particular attention to building capacity (Belgium scored 44 on the GCI ranking), cooperation (Belgium scored 38 on the GCI ranking) and technical measures (Belgium scored 47 on the GCI ranking).

		3. By what means to protect?																				
		Legal Measures		Technical Measures			Organiational Measures			Capacity Building							Cooperation					
		Cybercriminal Legislation	Cybersecurity Regulation	CIRT, CSIRT or CERT	Framework for the implementation of cybersecurity standards	Standardization body within the country	National strategy for cybersecurity	National body/agency responsible for cybersecurity and critical information infrastructure protection	Metrics used to measure cybersecurity development at a national level	Public awareness campaigns in cybersecurity	Framework for the certification and accreditation of cybersecurity professionals	Government development or support in professional training /courses in cybersecurity	Educational programs or academic curriculums in cybersecurity	R&D programs	Incentive mechanisms to encourage capacity building in the field of cybersecurity	Home grown cybersecurity industry	Bilateral agreements on cybersecurity cooperation	Multilateral or international agreements on cybersecurity cooperation	Participation in international fora/assodations dealing with cybersecurity	Public-Private Partnerships	Inter-agency partnerships	Best Practices
	Belgium																					
GOVERNMENT	Respondent 1	9	9	5	4	3	7	6	5	5	4	4	5	3	3	4	4	7	8	8	4	4
	Respondent 2	8	8	6	5	4	6	7	4	6	5	5	3	4	2	6	4	6	7	7	3	3
	Respondent 3	8	7	6	6	4	7	6	6	4	4	4	3	4	3	5	3	6	7	6	3	4
	Respondent 4	8	8	4	5	2	4	5	5	3	3	5	5	3	1	4	2	4	4	5	2	3
	Respondent 5	6	8	5	4	3	5	4	4	2	2	5	4	2	1	3	1	4	5	5	1	3
	Respondent 6	7	7	5	6	4	7	6	5	6	4	6	6	4	3	5	4	5	7	6	4	5
	Average CEPS Score	7.7	7.8	5.2	5.0	3.3	6.0	5.7	4.8	4.3	3.7	4.8	4.3	3.3	2.2	4.5	3.0	5.3	6.3	6.2	2.8	3.7
GCI 2018	Score	7.8	7.9	3.7	3.5	1.7	7.5	6.2	4.5	3.1	1.5	2.8	2.9	1.5	0.0	2.3	0.0	3.8	3.6	3.4	1.5	0.0
	Adjusted Weight	0.1	0.1	0.1	0.054	0.046	0.092	0.063	0.045	0.036	0.027	0.032	0.032	0.026	0.024	0.023	0.038	0.038	0.036	0.034	0.026	0.028
CEPS	Adjusted CEPS score	0.77	0.78	0.52	0.27	0.15	0.55	0.36	0.22	0.16	0.10	0.15	0.14	0.09	0.05	0.10	0.11	0.20	0.23	0.21	0.07	0.10
	By Category	1.55		0.94			1.13			0.79							0.93					

Source: Author's interpretation.

Table 9. Prioritizing by what means to protect CEPS from main cyber threats in Belgium.

Luxembourg: The energy picture in Luxembourg (a much smaller nation) is significantly different than in Belgium. Luxembourg imports all of its energy needs (see figure 13) and is heavily impacted by the increase of oil consumption (particularly in transportation), increasing the importance of energy security on the agenda of policy makers (IEA 2019a). Particularly in the oil and gas field, Luxembourg increased interconnectedness in the oil and gas markets with Belgium, and in the electricity market with France (IEA 2019a); countries that are perceived as trusted partners. As a result, Luxembourg takes a broader approach to energy security, with an increased focus on the protection of critical energy infrastructure from cyber-attacks. Here, Luxembourg's approach is focused more on research and development, and defines cyber security as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies can be used to protect the cyber environment, its organization and its user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment" (Bettel 2018, 10). However, Luxemburg's push on the implementation of new technologies in the energy field (and its focus on the implementation of smart meters) is also directly proportionate with the increase in the number of cyber threats.



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 13. 2017 Luxembourg Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

Results of Interviews:

Six Luxembourg government cyber security subject matter experts with specific knowledge of BPO management and operations were interviewed. Their responses are presented here.

What to protect: To ensure that no classified information is being disclosed, specific vulnerabilities were afterwards separated into the more generic OT and IT categories. Using the proposed CARVER criteria, we then added the answers on Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors (see table 10). Compared to Belgian experts, the criticality of OT systems ranged from 2 to 4, indicating the perception that a successful cyber-attack against CEPS could reduce infrastructure performance. No expert assessed that an attack would cripple the infrastructure. Most experts also perceived that IT systems are harder to recognize. The totals for each expert interviewer were then averaged to assess which type of system (OT or IT) should be secured first (see table 11). This indicates that in Luxembourg, government cyber physical systems experts believe that protection of OT CEPS systems should take priority over IT systems in the near to medium term.

		CARVER	What to protect?	
			OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Luxembourg				
GOVERNMENT	Respondent 7	Criticality	3	2
		Accessibility	5	2
		Recuperability	4	2
		Vulnerability	5	3
		Effect	4	2
		Recognizability	3	1
		TOTAL	**24**	**12**
	Respondent 8	Criticality	4	3
		Accessibility	4	3
		Recuperability	4	3
		Vulnerability	4	3
		Effect	4	3
		Recognizability	3	3
		TOTAL	**23**	**18**
	Respondent 9	Criticality	3	3
		Accessibility	3	2
		Recuperability	2	2
		Vulnerability	4	3
		Effect	4	3
		Recognizability	1	1
		TOTAL	**17**	**14**
	Respondent 10	Criticality	2	2
		Accessibility	3	2
		Recuperability	4	3
		Vulnerability	3	3
		Effect	3	3
		Recognizability	2	1
		TOTAL	**17**	**14**
	Respondent 11	Criticality	3	2
		Accessibility	4	2
		Recuperability	3	2
		Vulnerability	4	3
		Effect	3	3
		Recognizability	3	1
		TOTAL	**20**	**13**
	Respondent 12	Criticality	2	3
		Accessibility	3	3
		Recuperability	2	2
		Vulnerability	3	3
		Effect	2	2
		Recognizability	1	1
		TOTAL	**13**	**14**

Source: Author's interpretation.

Table 10. Results of CARVER cyber analysis for CEPS infrastructure in Luxembourg.

		1. What to protect?	
		OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Luxembourg			
GOVERNMENT	Respondent 7	24	12
	Respondent 8	23	18
	Respondent 9	17	14
	Respondent 10	17	14
	Respondent 11	20	13
	Respondent 12	13	14
	Average CEPS Score	**19**	**14**

Source: Author's interpretation.

Table 11. Prioritization of what CEPS systems to protect from cyber attacks in Luxembourg.

From what threats to protect: OT threats were then classified into 4 categories: terrorism, nation states, corporate espionage, and criminals. The 6 Luxembourg government cyber experts prioritized these threats based on their capabilities and intent, and we calculated overall threat as 'capability x intent' (see table 12). Similarly to Belgium. Luxembourg experts also assessed the capabilities of nation states highest; and the intent of terrorists highest. The concern about corporate espionage was also surprisingly higher than that about criminals (perhaps, because of the involvement of private entities in the management of CEPS). The average threat was then assessed in table 13, indicating that nation states represent the highest cyber threat to the CEPS infrastructure from the perspective of cyber experts from Luxembourg.

			2. From what threats to protect			
			Aversary risks			
		Threat	Terrorism	Nation states	Corporate espionage	Criminals
Luxembourg						
GOVERNMENT	Respondent 7	Capability	1	5	4	2
		Intent	5	3	3	3
		Threat	**5**	**15**	**12**	**6**
	Respondent 8	Capability	3	5	3	3
		Intent	5	5	3	3
		Threat	**15**	**25**	**9**	**9**
	Respondent 9	Capability	2	3	5	3
		Intent	5	4	4	4
		Threat	**10**	**12**	**20**	**12**
	Respondent 10	Capability	2	4	4	2
		Intent	5	3	3	3
		Threat	**10**	**12**	**12**	**6**
	Respondent 11	Capability	1	3	3	1
		Intent	5	3	3	3
		Threat	**5**	**9**	**9**	**3**
	Respondent 12	Capability	1	3	2	2
		Intent	5	3	3	3
		Threat	**5**	**9**	**6**	**6**

Source: Author's interpretation.

Table 12. Results of CEPS cyber threat analysis for Luxembourg.

		2. From what threats to protect			
		Aversary risks			
		Terrorism	Nation states	Corporate espionage	Criminals
Luxembourg					
GOVERNMENT	Respondent 7	5	15	12	6
	Respondent 8	15	25	9	9
	Respondent 9	10	12	20	12
	Respondent 10	10	12	12	6
	Respondent 11	5	9	9	3
	Respondent 12	5	9	6	6
	Average CEPS Score	8	14	11	7

Source: Author's interpretation.

Table 13. Prioritization of cyber threats against CEPS in Luxembourg.

By what means to protect: Most government cyber experts in Luxembourg were unfamiliar with the GCI methodology, and found it useful in assessing areas of improvement addressed in table 14. Overall, experts agreed that more attention needs to be paid to cooperation (Luxembourg ranked 12 on the GCI index) and capacity building (Luxembourg ranked 33 on the GCI index).

		3. By what means to protect?																				
		Legal Measures		Technical Measures			Organiational Measures			Capacity Building							Cooperation					
		Cybercriminal Legislation	Cybersecurity Regulation	CIRT, CSIRT or CERT	Framework for the implementation of cybersecurity standards	Standardization body within the country	National strategy for cybersecurity	National body/agency responsible for cybersecurity and critical information infrastructure protection	Metrics used to measure cybersecurity development at a national level	Public awareness campaigns in cybersecurity	Framework for the certification and accreditation of cybersecurity professionals	Government development or support in professional training /courses in cybersecurity	Educational programs or academic curriculums in cybersecurity	R&D programs	Incentive mechanisms to encourage capacity building in the field of cybersecurity	Home grown cybersecurity industry	Bilateral agreements on cybersecurity cooperation	Multilateral or international agreements on cybersecurity cooperation	Participation in international fora/assodations dealing with cybersecurity	Public-Private Partnerships	Inter-agency partnerships	Best Practices
	Luxembourg																					
GOVERNMENT	Respondent 7	5	5	5	5	3	7	4	5	4	2	2	3	3	3	2	2	4	4	3	2	2
	Respondent 8	5	6	6	6	4	6	6	6	5	4	3	4	5	4	3	3	5	4	4	4	2
	Respondent 9	7	7	7	6	4	7	8	7	7	5	5	5	7	6	6	5	6	6	6	5	5
	Respondent 10	6	6	5	6	3	7	6	6	5	3	3	5	4	4	5	3	5	5	4	4	3
	Respondent 11	5	6	7	5	3	7	5	6	6	5	2	5	4	5	4	3	5	5	5	3	3
	Respondent 12	6	7	8	6	4	8	7	7	7	5	5	6	6	7	6	4	6	6	7	5	5
	Average CEPS Score	5.7	6.2	6.3	5.7	3.5	7.0	6.0	6.2	5.7	4.0	3.3	4.7	4.8	4.8	4.3	3.3	5.2	5.0	4.8	3.8	3.3
GCI 2018	Score	7.8	7.9	4.4	3.5	2.9	9.3	6.2	4.5	3.6	1.2	1.9	2.1	2.4	2.4	2.3	1.3	3.8	3.6	3.4	2.6	0.0
	Adjusted Weight	0.1	0.1	0.1	0.054	0.046	0.092	0.063	0.045	0.036	0.027	0.032	0.032	0.026	0.024	0.023	0.038	0.038	0.036	0.034	0.026	0.028
CEPS	Adjusted CEPS score	0.57	0.62	0.63	0.31	0.16	0.64	0.38	0.28	0.20	0.11	0.11	0.15	0.13	0.12	0.10	0.13	0.20	0.18	0.16	0.10	0.09
	By Category	1.18		1.10			1.30			0.91							0.86					

Source: Author's interpretation.

Table 14. Prioritizing by what means to protect CEPS from cyber-attacks in Luxembourg.

Given the stark differences between the approaches that Belgium and Luxembourg are taking with regards to the protection of critical energy infrastructure from cyber-attacks does not make the work of the Belgian Pipeline Organization (BPO) easier. While both Belgium and Luxembourg acknowledge that "the emergence of more and more cyber-attacks of a very varied nature, often organized on a transnational level" (Bettel 2018, 7) needs to be addressed, their approaches to defending critical infrastructure differ in both understanding of the threat and capabilities to respond. While the focus of Belgium is on terrorism and crime groups (Flamant and Parrein 2017, 25), for example, Luxembourg is more concerned with "cyber threats insofar as they may be related to espionage [or] intrusion" (Bettel 2018, 12). But this can also play to the advantage of BPO, if it increases cooperation with Luxembourg in the cyber arena: between Belgium's focus on offensive capabilities, and the focus of Luxembourg on collection capabilities, BPO has a unique opportunity to significantly increase the resilience of CEPS to cyber-attacks.

Another area of concern that BPO has yet to address is the impact of smart meters on the NATO CEPS infrastructure. Given the increase in interconnectivity between Belgium, Luxembourg, and France, Luxembourg's push on the implementation of smart meters (IEA 2019a), which are ideal cyber targets, can also have unexpected consequences for Belgium and France. This goes beyond the smart meters that are already part of the CEPS infrastructure and expands to the substations that control the flow of electricity. CEPS is still dependent on the local electricity supply, so attacks on the electricity network in France, Belgium or Luxembourg could directly impact CEPS operations in all three countries. While the public and private sectors in France, Belgium, and Luxembourg all conduct "risk analysis according to ISO/IEC 27005 [as] the golden standard for managing information security" (Bettel 2018, 35), each entity has a different valuation criteria. There are also different individual standards for protecting the grid between Belgium and France, and with BPO operating the Luxembourg portion of CEPS, there is not much integration between BPO and French electricity providers, particularly in the field of cyber security. This

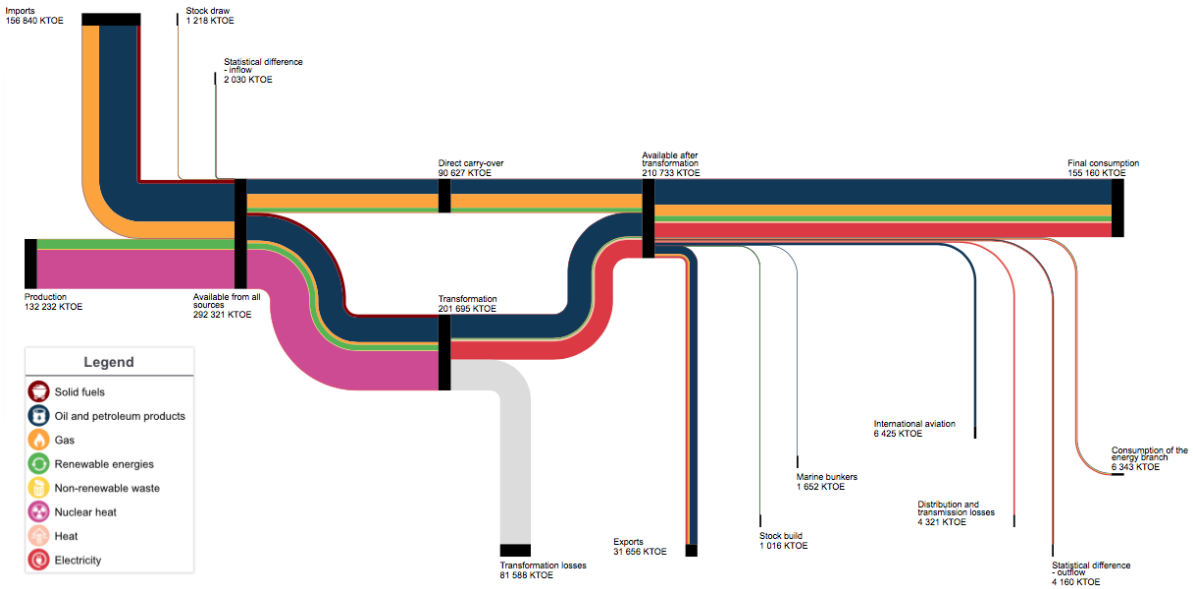
further complicates BPO's task to protect the pipeline in both Belgium and Luxembourg.

There are also disconnects at national levels. In Luxembourg, for example, "the Government will be in charge of identifying critical IT infrastructures, to ensure the implementation of an adequate level of protection" (Bettel 2018, 19). This is accomplished with the help of "four public CERTs and seven private CERTs" (ITU 2019, 46); which have no visibility over CEPS infrastructure. This is because the Luxembourg Defence is "in charge of any cybersecurity elements that fall within national responsibilities and obligations generated within NATO and the EU" (Bettel 2018, 11). These are further amplified by disconnects between public and private cyber security standards. CEPS maintenance (such as intelligence pigging) are in particular vulnerable to such cyber-attacks. Maintenance is typically outsourced by BPO to private contracts (Belgian Pipeline Organisation 2019). Many of these contractors use technologies with limited cyber protection. Both NATO CEPS infrastructure and the contractors that BPO employs to maintain it are dependent on technology "equipped with sensors collecting data and rely on information systems to optimize services that are characterized by their high degree of connectivity. The attacks against these infrastructures are likely to multiply in the presence of authentication systems and cryptographic protocols, which often do not meet the highest security level" (Bettel 2018, 37). The NATO energy and cyber security SMEs interviewed are very much aware of these disconnects, but 1) lack of clear EU legislation for protection of critical energy infrastructure from cyber-attacks and 2) limited budgets to address these growing cyber threats make it unlikely that these will be resolved in the near future. At the national levels, however, there is a consensus that "operating costs for infrastructure" are expected to increase (Flamant and Parrein 2017, 79), which includes costs of protecting the CEPS infrastructure from cyber-attacks.

4.3.2 France

France's energy security "is dependent on reliable supply, i.e. supply free from political contingencies, at an affordable cost for business" (Macron 2017, 30). And cost of business is

expected to increase in a nation where electricity consumption is heavily dependent on nuclear energy, which is quickly reaching "the end of its lifetime" (IEA 2019a)—see figure 14—and civilian and military airports are dependent on fuel delivered by NATO CEPS. These challenges in the energy security outlooks are however balanced by clear, strategic and pragmatic approaches in the cybersecurity field. In fact, the Global Cybersecurity Index ranks France's cybersecurity readiness as 2nd in Europe and 3rd globally (ITU 2019, 60), with France "scoring 100 per cent in legal and organizational pillars" (ITU 2019, 31).



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 14. 2017 France Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

France is "collaborating with institutional partners (ministries, national authorities, private sector and non-profit organizations)" (ITU 2019, 31) to address cyber threats to CEPS. Compared to Belgium and Luxembourg, where NATO CEPS infrastructure is operated and maintained by a Belgian Defence organization (BPO), the French portion of CEPS is operated by TRAPIL, a French quasi-public company created to insure timely delivery of fuel to Paris by pipeline. Apart from civilian infrastructure, TRAPIL also operates the military fuel delivery systems (to include pipeline, storage, and pumping) in close collaboration with the French Ministry of Defence and the Service National des Oléoducs Interalliés (SNOI). As such, TRAPIL operates all CEPS "central

dispatch and control centers, pumping stations, access pits and storage depots" in France (Butrimas 2018). That being said, France has successfully implemented a centralized approach to protecting critical energy infrastructure from cyber-attacks, where responsibility was "assigned to a centralised agency, with authority spanning across multiple sectors" (Healey et al. 2016, 26). This was done in order to "ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack" (Valls 2015, 9).

Results of Interviews:

Three French government and three private cyber security subject matter experts with specific knowledge of TREPIL management and operations were interviewed. Their responses are presented here.

What to protect: To ensure that no classified information is being disclosed, specific vulnerabilities were afterwards separated into the more generic OT and IT categories. Using the proposed CARVER criteria, we then added the answers on Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors (see table 15). In France, criticality of OT systems scored higher among government experts than industry experts (who, on average, scored IT systems as more critical). Private industry also assessed that IT system vulnerabilities of CEPS are harder to recognize. Furthermore, private industry assessed that recuperability of IT and OT systems would take less time to recover than what government experts assessed. The discrepancies could be explained by three important factors: 1) access to classified information about vulnerabilities (where cleared government experts tend to be more concerned about threats in general); 2) budgetary constraints on the private side (where industry experts are forced to prioritize expenses for security, and expenses on IT security outweigh expenses on OT security); and 3) more advanced technical knowledge on the private side (where options for solutions are more abundant; although the cost varies on these options). The totals for each expert interviewer were then averaged to assess which type of system (OT or IT) should be secured first (see table 16). This

indicates that in France, cyber physical systems experts believe that protection of OT CEPS systems should take priority over IT systems in the near to medium term.

		CARVER	What to protect?	
			OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
France				
GOVERNMENT	Respondent 13	Criticality	4	3
		Accessibility	5	2
		Recuperability	3	2
		Vulnerability	4	3
		Effect	3	2
		Recognizability	1	1
		TOTAL	**20**	**13**
	Respondent 14	Criticality	4	2
		Accessibility	5	3
		Recuperability	3	2
		Vulnerability	4	3
		Effect	3	3
		Recognizability	1	2
		TOTAL	**20**	**15**
	Respondent 15	Criticality	4	2
		Accessibility	4	3
		Recuperability	3	3
		Vulnerability	5	4
		Effect	3	2
		Recognizability	2	1
		TOTAL	**21**	**15**
PRIVATE	Respondent 16	Criticality	3	3
		Accessibility	2	2
		Recuperability	2	1
		Vulnerability	3	3
		Effect	2	2
		Recognizability	1	3
		TOTAL	**13**	**14**
	Respondent 17	Criticality	3	4
		Accessibility	2	2
		Recuperability	1	1
		Vulnerability	3	3
		Effect	2	2
		Recognizability	2	3
		TOTAL	**13**	**15**
	Respondent 18	Criticality	3	3
		Accessibility	1	1
		Recuperability	1	2
		Vulnerability	2	3
		Effect	2	3
		Recognizability	2	3
		TOTAL	**11**	**15**

Source: Author's interpretation.

Table 15. Results of CARVER cyber analysis for CEPS infrastructure in France.

		1. What to protect?	
		OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
France			
GOVERNMENT	Respondent 13	20	13
	Respondent 14	20	15
	Respondent 15	21	15
PRIVATE	Respondent 16	13	14
	Respondent 17	13	15
	Respondent 18	11	15
	Average CEPS Score	**16**	15

Source: Author's interpretation.

Table 16. Prioritization of what CEPS systems to protect from cyber attacks in France.

From what threats to protect: OT threats were then classified into 4 categories: terrorism, nation states, corporate espionage, and criminals. The French cyber experts prioritized these threats based on their capabilities and intent, and we calculated overall threat as 'capability x intent' (see table 17). Of note, again, that capabilities of threats score higher among government experts than industry experts because of the three factors previously identified. Average threat was then assessed in table 18, indicating that nation states represent the highest cyber threat to the CEPS infrastructure from the perspective of French experts. The threat of terrorism was, however ranked higher among private experts than government experts, with French industry experts fearing threats against CEPS from terrorists more than threats from criminal groups.

		Threat	2. From what threats to protect			
			Aversary risks			
			Terrorism	Nation states	Corporate espionage	Criminals
France						
GOVERNMENT	Respondent 13	Capability	3	5	5	3
		Intent	5	4	3	5
		Threat	**15**	**20**	**15**	**15**
	Respondent 14	Capability	2	5	3	3
		Intent	5	4	3	3
		Threat	**10**	**20**	**9**	**9**
	Respondent 15	Capability	2	5	2	4
		Intent	5	4	3	2
		Threat	**10**	**20**	**6**	**8**
PRIVATE	Respondent 16	Capability	2	2	2	2
		Intent	5	4	5	5
		Threat	**10**	**8**	**10**	**10**
	Respondent 17	Capability	3	3	2	4
		Intent	5	4	3	3
		Threat	**15**	**12**	**6**	**12**
	Respondent 18	Capability	3	3	2	4
		Intent	5	4	3	2
		Threat	**15**	**12**	**6**	**8**

Source: Author's interpretation.

Table 17. Results of CEPS cyber threat analysis for France.

		2. From what threats to protect			
		Aversary risks			
		Terrorism	Nation states	Corporate espionage	Criminals
France					
GOVERNMENT	Respondent 13	15	20	15	15
	Respondent 14	10	20	9	9
	Respondent 15	10	20	6	8
PRIVATE	Respondent 16	10	8	10	10
	Respondent 17	15	12	6	12
	Respondent 18	15	12	6	8
	Average CEPS Score	13	**15**	9	10

Source: Author's interpretation.

Table 18. Prioritization of cyber threats against CEPS in France.

By what means to protect: Most government cyber experts in France were unfamiliar with the GCI methodology, and found it useful in assessing areas of improvement addressed in table 19. Here, French experts assessed that more attention needs to be paid to cooperation (France ranked 19 on the GCI index) and capacity building (France ranked 10 on the GCI index).

		3. By what means to protect?																				
		Legal Measures		Technical Measures			Organiational Measures			Capacity Building							Cooperation					
		Cybercriminal Legislation	Cybersecurity Regulation	CIRT, CSIRT or CERT	Framework for the implementation of cybersecurity standards	Standardization body within the country	National strategy for cybersecurity	National body/agency responsible for cybersecurity and critical information infrastructure protection	Metrics used to measure cybersecurity development at a national level	Public awareness campaigns in cybersecurity	Framework for the certification and accreditation of cybersecurity professionals	Government development or support in professional training /courses in cybersecurity	Educational programs or academic curriculums in cybersecurity	R&D programs	Incentive mechanisms to encourage capacity building in the field of cybersecurity	Home grown cybersecurity industry	Bilateral agreements on cybersecurity cooperation	Multilateral or international agreements on cybersecurity cooperation	Participation in international fora/associations dealing with cybersecurity	Public-Private Partnerships	Inter-agency partnerships	Best Practices
	France																					
GOVERNMENT	Respondent 13	8	9	8	8	7	9	8	7	6	5	6	5	6	6	5	5	6	6	6	5	4
	Respondent 14	7	7	7	7	6	9	7	6	5	4	4	5	5	6	4	4	5	4	4	3	3
	Respondent 15	6	6	7	6	6	9	6	6	5	3	4	4	6	5	4	3	4	4	4	3	3
PRIVATE	Respondent 16	7	7	7	6	6	9	8	7	6	5	5	5	6	5	4	3	5	6	4	2	2
	Respondent 17	6	8	6	4	5	9	7	6	4	4	4	4	5	4	3	2	3	3	3	2	3
	Respondent 18	7	7	6	5	3	8	6	5	5	4	4	4	5	3	3	2	3	4	4	2	1
	Average CEPS Score	6.8	7.3	6.8	6.0	5.5	8.8	7.0	6.2	5.2	4.2	4.5	4.5	5.5	4.8	3.8	3.2	4.3	4.5	4.2	2.8	2.7
GCI 2018	Score	7.8	7.9	5.8	3.5	2.9	9.3	6.2	4.5	3.1	2.7	2.8	2.9	2.4	2.4	2.3	1.6	3.8	3.6	3.4	1.5	0.0
	Adjusted Weight	0.1	0.1	0.1	0.054	0.046	0.092	0.063	0.045	0.036	0.027	0.032	0.032	0.026	0.024	0.023	0.038	0.038	0.036	0.034	0.026	0.028
CEPS	Adjusted CEPS score	0.68	0.73	0.68	0.32	0.25	0.81	0.44	0.28	0.19	0.11	0.14	0.14	0.14	0.12	0.09	0.12	0.16	0.16	0.14	0.07	0.07
	By Category	1.42		1.26			1.53			0.93							0.74					

Source: Author's interpretation.

Table 19. Prioritizing by what means to protect CEPS from cyber-attacks in France.

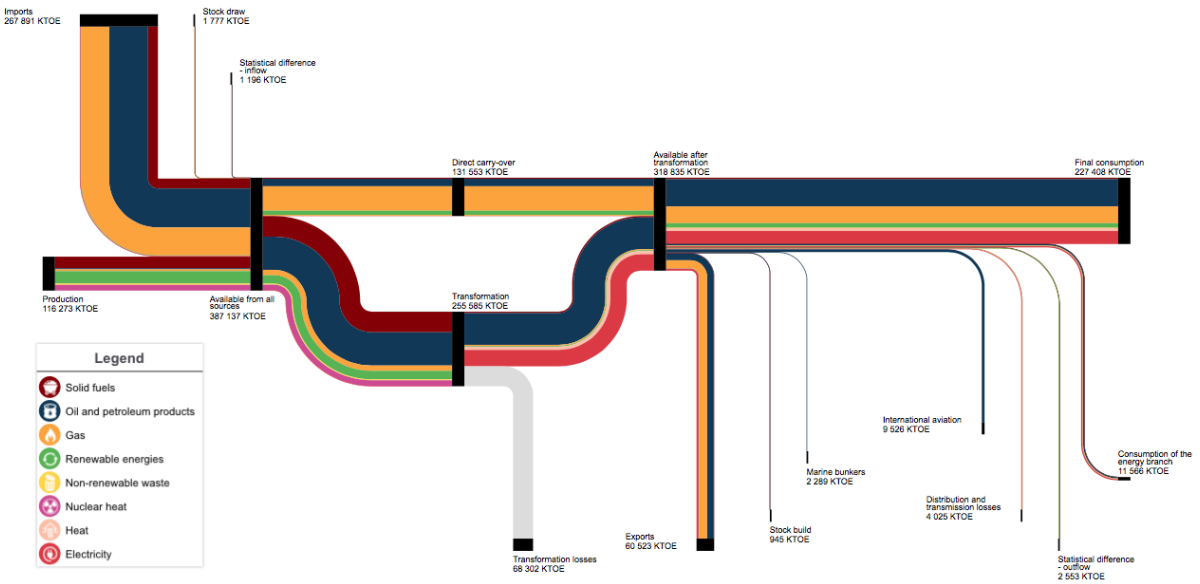
France views cyberspace as "a new domain for unfair competition and espionage, disinformation and propaganda, terrorism and criminality" (Valls 2015, 1). What is unique to France is that it also understands the cyber threat to critical infrastructure in policy documents, which highlight that "cyberattacks have ramped up considerably over the past decade, reflecting the dissemination of increasingly sophisticated means of attack. States have played a direct role in these changes by propagating cyber-weapons that, once known, may be studied, re-engineered and reused, but also indirectly, by allowing such attacks to be developed in or deployed via their territory" (Macron 2017, 33). Using these (now available) cyber weapons, "an attacker could take control of connected objects, remotely interrupt an industrial activity or destroy its target" (Valls 2015, 14). These threat vectors could severely impact CEPS operations, so France's approach to "addressing constantly changing cyber-threats is particularly complex inasmuch as the response must extend beyond the scope of defence, due to the intertwined nature of the challenges faced and of the public and private actors" (Macron 2017, 34).

France also reaffirmed its commitment to guarantee the resilience of critical energy infrastructure to "a major cyber-attack by expanding cooperation with private stakeholders at national and international levels" (Valls 2015, 3). The cooperation between public and private entities in the cybersecurity field "to detect and attribute attacks, based on gathering both human and technical intelligence" (Macron 2017, 72) is also unlike any other country in the world. And, like Belgium, France acknowledges that "the major challenge that cyberthreats represent calls for a substantial increase in France's defensive and offensive capabilities" (Macron 2017, 72). Overall, however, the CEPS infrastructure in France seems to be much more resilient to cyber-attacks than the CEPS infrastructure in both Belgium and Luxembourg.

4.3.3 Germany

Germany's decision to "phase-out of nuclear power by 2022" has made it more difficult to

decrease dependence on solid fuels and Russian gas for electricity generation (IEA 2019a)—see figure 15. This is problematic in a country where its prosperity and "the well-being of [its] citizens will significantly depend on [...] a secure supply of [...] energy [and where] any interruption of access [to energy supplies] involves considerable risks for the ability of [the] state to function and for the prosperity of [its] citizens" (Merkel and von der Leyen 2016, 41). Like France, Germany also understands the cyber threats to critical infrastructure and has implemented a centralized approach to protecting critical energy infrastructure from cyber-attacks, where responsibility was "assigned to a centralised agency, with authority spanning across multiple sectors" (Healey et al. 2016, 26). Despite this, the Global Cybersecurity Index ranks Germany's cybersecurity readiness as 13th in Europe and 22nd globally (ITU 2019, 60). Interviews with both energy and cyber security SMEs indicate that lack of resilience of critical energy infrastructure to cyber-attacks may have to do more with insufficiencies in the public-private cooperation (especially when compared to France) than the lack of understanding by the government of the cyber-physical threats to critical energy infrastructure.



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 15. 2017 Germany Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

Results of Interviews:

The German portions of CEPS and NEPS are operated by the Fernleitungs-Betriebs-gesellschaft (FBG), a German company responsible with supplying fuel for German civil airports. FBG operates a dispatch control center in Idar-Oberstein, close to the border with France, Belgium, and Luxembourg. Six German government and private industry cyber security subject matter experts with specific knowledge of FBG management and operations were interviewed. Their responses are presented here.

What to protect: To ensure that no classified information is being disclosed, specific vulnerabilities were afterwards separated into the more generic OT and IT categories. Using the proposed CARVER criteria, we then added the answers on Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors (see table 20). Compared to France, German industry experts are on average more concerned about IT systems than OT systems. Like in France, however, German experts in industry do seem less concerned about future cyber events, in general, than government experts - for the same three factors illustrated earlier. The totals for each expert interviewer were then averaged to assess which type of system (OT or IT) should be secured first (see table 21). This indicates that in Germany, cyber physical systems experts believe that protection of OT CEPS systems should take priority over IT systems in the near to medium term.

		CARVER	What to protect?	
			OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Germany				
GOVERNMENT	Respondent 19	Criticality	3	2
		Accessibility	4	3
		Recuperability	3	2
		Vulnerability	5	4
		Effect	3	3
		Recognizability	3	1
		TOTAL	**21**	**15**
	Respondent 20	Criticality	5	4
		Accessibility	4	3
		Recuperability	2	1
		Vulnerability	5	5
		Effect	3	3
		Recognizability	3	4
		TOTAL	**22**	**20**
	Respondent 21	Criticality	4	3
		Accessibility	4	3
		Recuperability	4	3
		Vulnerability	5	5
		Effect	4	3
		Recognizability	3	3
		TOTAL	**24**	**20**
PRIVATE	Respondent 22	Criticality	3	3
		Accessibility	1	1
		Recuperability	2	2
		Vulnerability	2	3
		Effect	3	3
		Recognizability	2	3
		TOTAL	**13**	**15**
	Respondent 23	Criticality	3	3
		Accessibility	2	2
		Recuperability	2	2
		Vulnerability	3	3
		Effect	3	3
		Recognizability	1	1
		TOTAL	**14**	**14**
	Respondent 24	Criticality	3	3
		Accessibility	2	3
		Recuperability	1	2
		Vulnerability	2	2
		Effect	2	3
		Recognizability	2	3
		TOTAL	**12**	**16**

Source: Author's interpretation.

Table 20. Results of CARVER cyber analysis for CEPS infrastructure in Germany.

		1. What to protect?	
		OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Germany			
GOVERNMENT	Respondent 19	21	15
	Respondent 20	22	20
	Respondent 21	24	20
PRIVATE	Respondent 22	13	15
	Respondent 23	14	14
	Respondent 24	12	16
	Average CEPS Score	**18**	17

Source: Author's interpretation.

Table 21. Prioritization of what CEPS systems to protect from cyber attacks in Germany.

From what threats to protect: OT threats were then classified into 4 categories: terrorism, nation states, corporate espionage, and criminals. The 6 German cyber experts prioritized these threats based on their capabilities and intent, and we calculated overall threat as 'capability x intent' (see table 22). Average threat was then assessed in table 23, indicating that nation states represent the highest cyber threat to the CEPS infrastructure from the perspective of German experts.

		Threat	2. From what threats to protect			
			Aversary risks			
			Terrorism	Nation states	Corporate espionage	Criminals
Germany						
GOVERNMENT	Respondent 19	Capability	3	4	3	2
		Intent	5	3	3	5
		Threat	**15**	**12**	**9**	**10**
	Respondent 20	Capability	2	3	3	3
		Intent	5	3	3	3
		Threat	**10**	**9**	**9**	**9**
	Respondent 21	Capability	1	3	3	4
		Intent	5	4	3	2
		Threat	**5**	**12**	**9**	**8**
PRIVATE	Respondent 22	Capability	2	2	2	2
		Intent	5	4	5	5
		Threat	**10**	**8**	**10**	**10**
	Respondent 23	Capability	2	2	3	3
		Intent	5	3	3	3
		Threat	**10**	**6**	**9**	**9**
	Respondent 24	Capability	1	3	3	4
		Intent	5	4	3	2
		Threat	**5**	**12**	**9**	**8**

Source: Author's interpretation.

Table 22. Results of CEPS cyber threat analysis for Germany.

		2. From what threats to protect			
		Aversary risks			
		Terrorism	Nation states	Corporate espionage	Criminals
Germany					
GOVERNMENT	Respondent 19	15	12	9	10
	Respondent 20	10	9	9	9
	Respondent 21	5	12	9	8
PRIVATE	Respondent 22	10	8	10	10
	Respondent 23	10	6	9	9
	Respondent 24	5	12	9	8
Average CEPS Score		9	**10**	9	9

Source: Author's interpretation.

Table 23. Prioritization of cyber threats against CEPS in Germany.

By what means to protect: Most cyber experts in Germany were unfamiliar with the GCI methodology, and found it useful in assessing areas of improvement addressed in table 24. German experts (both private and public) generally agree that significant more work needs to be done on cooperation (Germany ranked 8 on the GCI index) and capacity building (Germany ranked 16 on the GCI index).

		3. By what means to protect?																				
		Legal Measures		Technical Measures			Organiational Measures			Capacity Building							Cooperation					
		Cybercriminal Legislation	Cybersecurity Regulation	CIRT, CSIRT or CERT	Framework for the implementation of cybersecurity standards	Standardization body within the country	National strategy for cybersecurity	National body/agency responsible for cybersecurity and critical information infrastructure protection	Metrics used to measure cybersecurity development at a national level	Public awareness campaigns in cybersecurity	Framework for the certification and accreditation of cybersecurity professionals	Government development or support in professional training /courses in cybersecurity	Educational programs or academic curriculums in cybersecurity	R&D programs	Incentive mechanisms to encourage capacity building in the field of cybersecurity	Home grown cybersecurity industry	Bilateral agreements on cybersecurity cooperation	Multilateral or international agreements on cybersecurity cooperation	Participation in international fora/assodations dealing with cybersecurity	Public-Private Partnerships	Inter-agency partnerships	Best Practices
Germany																						
GOVERNMENT	Respondent 19	6	6	8	6	4	7	6	7	5	4	3	4	5	4	3	3	4	4	3	3	2
	Respondent 20	7	6	8	7	4	8	7	6	4	2	2	5	4	4	3	3	5	5	4	2	3
	Respondent 21	8	7	8	8	4	9	8	7	7	5	5	6	6	6	5	4	6	5	5	4	3
PRIVATE	Respondent 22	6	6	7	6	5	7	7	7	6	5	3	5	4	5	5	3	5	5	4	2	2
	Respondent 23	5	4	6	5	4	7	6	6	5	3	2	5	4	4	4	2	4	3	3	2	3
	Respondent 24	7	6	7	6	3	8	7	7	7	5	5	5	6	6	6	2	5	6	5	3	2
	Average CEPS Score	6.5	5.8	7.3	6.3	4.0	7.7	6.8	6.7	5.7	4.0	3.3	5.0	4.8	4.8	4.3	2.8	4.8	4.7	4.0	2.7	2.5
GCI 2018	Score	5.7	7.9	6.5	3.5	1.3	7.5	6.2	4.5	3.1	2.7	1.5	2.9	2.4	2.4	2.3	1.6	3.8	3.6	3.4	2.6	0.0
	Adjusted Weight	0.1	0.1	0.1	0.054	0.046	0.092	0.063	0.045	0.036	0.027	0.032	0.032	0.026	0.024	0.023	0.038	0.038	0.036	0.034	0.026	0.028
CEPS	Adjusted CEPS score	0.65	0.58	0.73	0.34	0.18	0.71	0.43	0.30	0.20	0.11	0.11	0.16	0.13	0.12	0.10	0.11	0.18	0.17	0.14	0.07	0.07
	By Category	1.23		1.26			1.44			0.92							0.73					

Source: Author's interpretation.

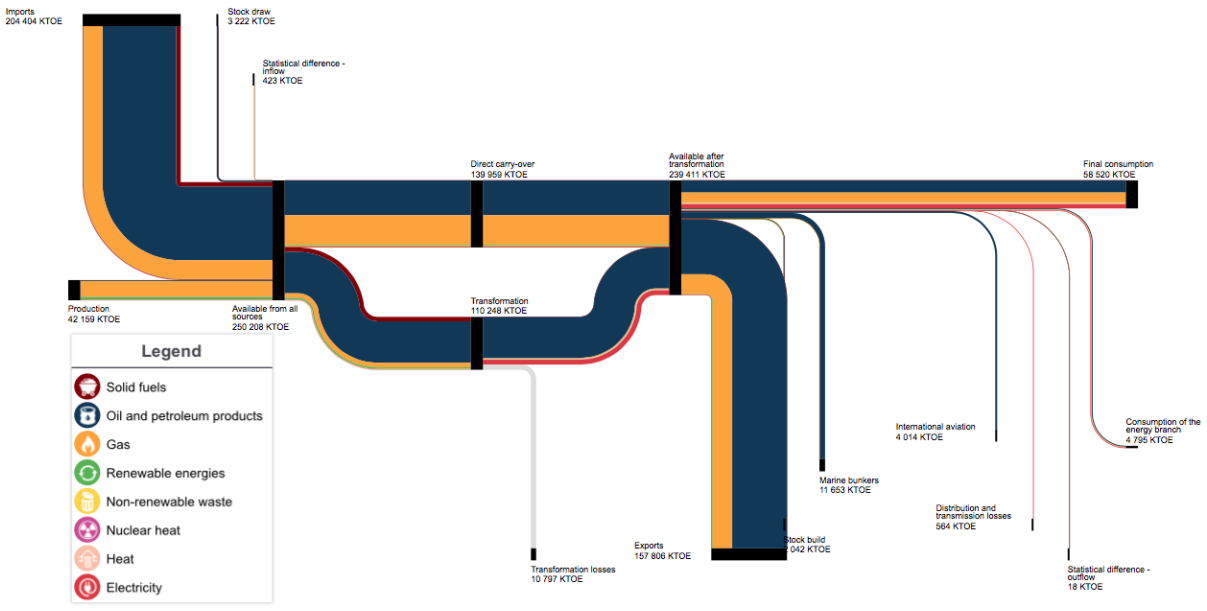
Table 24. Prioritizing by what means to protect CEPS from cyber attacks in Germany.

The collaboration between the FBG and the German intelligence apparatus on cyber-physical threats is not, however, as strong as TRAPIL's in France. Cooperation between FBG and TRAPIL (particularly in the sharing of sensitive information on cyber threats) is also minimal. What is most striking is that FBG strongly believes that the infrastructure that it is charged to protect is resilient to cyber-attack just because physical attacks have had minimal impact in the past. FBG attributes this resiliency on the German ability to develop "extensive scenario building and contingency planning, including redundancy systems for fuel deliveries by pipeline" (Rosner 2004, 214). Officially, however, Germany does fear that future cyber-attacks may lead to "damage of critical infrastructure with severe consequences for the civilian population" (Merkel and von der Leyen 2016, 37). But FBG fails to fully realize how both military and civilian airfields could be severely impacted by such an attack despite the fact that "incidents have occurred which highlight the vulnerabilities in this system" (Rosner 2004, 214).

Despite problems identified at FBG, Germany fully understands the state and non-state cyber threat environment and recognizes that cyber-attacks on critical infrastructure "have been a reality for some time [and that] most modern high-value attacks are specially tailored to fit the targeted system" using both accessible and inexpensive destructive malware (Merkel and von der Leyen 2016, 37). But a comprehensive approach for "better protection of critical infrastructure [and] reduced vulnerabilities in the energy sector" (Merkel and von der Leyen 2016, 39) from these growing cyber threats is not yet here

4.3.4 The Netherlands

The Netherlands is an important energy hub in Europe with integrated supply chains. Despite this, it remains "one of the most fossil-fuel- and CO2-intensive economies among IEA member countries" (IEA 2019a)—see figure 16. In the cyber-physical arena, Netherlands adopted a PPP approach to protecting critical energy infrastructure from cyber-attacks, which "implies that the decision-making process is carried out through cooperation between public and private actors" (Healey et al. 2016, 26). This approach has led the Global Cybersecurity Index to rank The Netherland's cybersecurity readiness as 8th in Europe and 12th globally (ITU 2019, 60). But despite brandishing its public-private approach in the cybersecurity field, the National Cyber Security Strategy (2014) does not mention energy sector at all. This is particularly because of the power of Dutch energy companies continue to exert significant influence over government institutions in The Netherlands (and fear government regulations pertaining to cyber security - which is perceived as an additional cost by energy companies).



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 16. 2017 The Netherlands Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

Results of Interviews:

Compared to Belgium and Luxembourg—where the operations of NATO CEPS infrastructure is managed by BPO, a Belgian Defence body—and Germany and France—where the operations of NATO CEPS infrastructure is managed by quasi-private entities—The Netherland's portion of CEPS is operated and maintained by the Dutch Pipeline Organisation (DPO), a branch of the Dutch military (Oxenaar 2017, 48), in close cooperation with Royal Vopak (a private company). The latter "operates and manages the offloading of fuel from the ships and transfers it to the NATO CEPS" and is also responsible for tank storage of CEPS bulk liquid products (Butrimas 2019b). Six cyber security subject matter experts with specific knowledge of DPO management and operations were interviewed. Their responses are presented here.

What to protect: To insure that no classified information is being disclosed, specific vulnerabilities were afterwards separated into the more generic OT and IT categories. Using the proposed CARVER criteria, we then added the answers on Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability factors (see table 25). In the Netherlands, all respondents found the criticality of OT systems a priority. They also found OT systems easier to recognize (on average) than IT systems. The totals for each expert interviewer were then averaged to assess which type of system (OT or IT) should be secured first (see table 26). This indicates that in the Netherlands cyber physical systems experts believe that protection of OT CEPS systems should take priority over IT systems in the near to medium term.

		CARVER	What to protect?	
			OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Netherlands				
GOVERNMENT	Respondent 25	Criticality	3	3
		Accessibility	5	3
		Recuperability	4	3
		Vulnerability	5	3
		Effect	4	2
		Recognizability	3	2
		TOTAL	**24**	**16**
	Respondent 26	Criticality	4	3
		Accessibility	4	3
		Recuperability	3	3
		Vulnerability	4	3
		Effect	4	3
		Recognizability	3	3
		TOTAL	**22**	**18**
	Respondent 27	Criticality	3	3
		Accessibility	3	2
		Recuperability	2	2
		Vulnerability	3	3
		Effect	4	3
		Recognizability	3	3
		TOTAL	**18**	**16**
	Respondent 28	Criticality	3	3
		Accessibility	3	2
		Recuperability	4	3
		Vulnerability	3	3
		Effect	3	3
		Recognizability	2	1
		TOTAL	**18**	**15**
	Respondent 29	Criticality	3	2
		Accessibility	4	2
		Recuperability	3	2
		Vulnerability	4	3
		Effect	3	3
		Recognizability	3	1
		TOTAL	**20**	**13**
	Respondent 30	Criticality	4	3
		Accessibility	3	3
		Recuperability	3	3
		Vulnerability	3	3
		Effect	2	2
		Recognizability	3	3
		TOTAL	**18**	**17**

Source: Author's interpretation.

Table 25. Results of CARVER cyber analysis for CEPS infrastructure in the Netherlands.

		1. What to protect?	
		OT (ICS, SCADA, pumps, etc.)	IT (IP, information security, etc.)
Netherlands			
GOVERNMENT	Respondent 25	24	16
	Respondent 26	22	18
	Respondent 27	18	16
	Respondent 28	18	15
	Respondent 29	20	13
	Respondent 30	18	17
	Average CEPS Score	**20**	16

Source: Author's interpretation.

Table 26. Prioritization of what CEPS systems to protect from cyber-attacks in the Netherlands.

From what threats to protect: OT threats were then classified into 4 categories: terrorism, nation states, corporate espionage, and criminals. The 6 cyber experts prioritized these threats based on their capabilities and intent, and we calculated overall threat as 'capability x intent' (see table 27). Average threat was then assessed in table 28, indicating that nation states represent the highest cyber threat to the CEPS infrastructure from the perspective of experts from the Netherlands. The Netherlands is very concerned about the capabilities of nations states such as Russia to attack the CEPS infrastructure; but also, by the capabilities of criminals, who are increasingly using new tools to extort money out of governments. As such, the CEPS infrastructure has the potential to become the victim of the next ransomware attack, per one of the respondents.

		Threat	2. From what threats to protect			
			Aversary risks			
			Terrorism	Nation states	Corporate espionage	Criminals
Netherlands						
GOVERNMENT	Respondent 25	Capability	2	5	1	4
		Intent	4	2	3	4
		Threat	**8**	**10**	**3**	**16**
	Respondent 26	Capability	2	4	3	2
		Intent	5	3	3	3
		Threat	**10**	**12**	**9**	**6**
	Respondent 27	Capability	2	4	4	2
		Intent	4	2	3	4
		Threat	**8**	**8**	**12**	**8**
	Respondent 28	Capability	2	5	4	3
		Intent	5	3	3	3
		Threat	**10**	**15**	**12**	**9**
	Respondent 29	Capability	1	3	2	3
		Intent	4	4	3	5
		Threat	**4**	**12**	**6**	**15**
	Respondent 30	Capability	2	3	2	3
		Intent	5	3	3	4
		Threat	**10**	**9**	**6**	**12**

Source: Author's interpretation.

Table 27. Results of CEPS cyber threat analysis for the Netherlands.

		2. From what threats to protect			
		Aversary risks			
		Terrorism	Nation states	Corporate espionage	Criminals
Netherlands					
GOVERNMENT	Respondent 25	8	10	3	16
	Respondent 26	10	12	9	6
	Respondent 27	8	8	12	8
	Respondent 28	10	15	12	9
	Respondent 29	4	12	6	15
	Respondent 30	10	9	6	12
	Average CEPS Score	8	11	8	11

Source: Author's interpretation.

Table 28. Prioritization of cyber threats against CEPS in the Netherlands.

By what means to protect: Most government cyber experts in the Netherlands were unfamiliar with the GCI methodology, and found it useful in assessing areas of improvement addressed in table 29. Experts agreed that more attention needs to be paid to capacity building (the Netherlands ranked 31 on the GCI index) and cooperation (the Netherlands ranked 8 on the GCI index).

		3. By what means to protect?																				
		Legal Measures		Technical Measures			Organiational Measures			Capacity Building							Cooperation					
		Cybercriminal Legislation	Cybersecurity Regulation	CIRT, CSIRT or CERT	Framework for the implementation of cybersecurity standards	Standardization body within the country	National strategy for cybersecurity	National body/agency responsible for cybersecurity and critical information infrastructure protection	Metrics used to measure cybersecurity development at a national level	Public awareness campaigns in cybersecurity	Framework for the certification and accreditation of cybersecurity professionals	Government development or support in professional training /courses in cybersecurity	Educational programs or academic curriculums in cybersecurity	R&D programs	Incentive mechanisms to encourage capacity building in the field of cybersecurity	Home grown cybersecurity industry	Bilateral agreements on cybersecurity cooperation	Multilateral or international agreements on cybersecurity cooperation	Participation in international fora/associations dealing with cybersecurity	Public-Private Partnerships	Inter-agency partnerships	Best Practices
	Netherlands																					
GOVERNMENT	Respondent 25	7	7	7	7	5	9	8	7	5	4	4	5	3	3	4	4	6	6	6	3	3
	Respondent 26	8	8	6	6	4	9	9	8	6	5	5	3	4	2	6	6	7	7	7	4	4
	Respondent 27	6	6	5	5	4	8	7	6	4	4	4	2	4	3	4	3	6	6	6	3	3
	Respondent 28	6	6	5	6	4	9	8	5	2	2	4	3	3	2	3	3	5	5	5	2	3
	Respondent 29	7	7	6	5	4	9	9	7	3	3	4	4	3	2	2	4	6	5	5	3	2
	Respondent 30	7	7	8	7	6	9	8	7	5	4	5	3	4	3	5	4	6	6	5	4	3
	Average CEPS Score	6.8	6.8	6.2	6.0	4.5	8.8	8.2	6.7	4.2	3.7	4.3	3.3	3.5	2.5	4.0	4.0	6.0	5.8	5.7	3.2	3.0
GCI 2018	Score	7.8	7.9	6.1	3.5	2.9	8.5	6.2	3.0	3.1	2.7	2.5	1.4	1.7	2.4	2.3	1.6	3.8	3.6	3.4	2.6	0.0
	Adjusted Weight	0.1	0.1	0.1	0.054	0.046	0.092	0.063	0.045	0.036	0.027	0.032	0.032	0.026	0.024	0.023	0.038	0.038	0.036	0.034	0.026	0.028
CEPS	Adjusted CEPS score	0.68	0.68	0.62	0.32	0.21	0.81	0.51	0.30	0.15	0.10	0.14	0.11	0.09	0.06	0.09	0.15	0.23	0.21	0.19	0.08	0.08
	By Category	1.37		1.15			1.63			0.74							0.95					

Source: Author's interpretation.

Table 29. Prioritizing by what means to protect CEPS from cyber-attacks in the Netherlands.

The systems of DPO and Royal Vopak are, unfortunately, not fully integrated, which means that there is no one standard approach to the protection of "access pits, dispatch centres, fuel depot and Port of Rotterdam facilities" (Butrimas 2019a) against cyber-attacks. Furthermore, the Dutch military is also acting as a for-profit entity. The CEPS infrastructure in The Netherlands "includes a connection between the port of Rotterdam and Schiphol airport", an airport that buys most of its jet fuel needs from the Dutch military through this CEPS connection (Oxenaar 2017, 48). It is difficult to understand how the Dutch military prerogative of CEPS security is balanced by its need to decrease CEPS maintenance costs for the sake of increasing state profits through selling of jet fuel to civilian airports:

> *"The pipeline has a maximum technical capacity of 2.9 mcm annually and the oil companies operating on Schiphol have the obligation to purchase at least 1.8 mcm of kerosene annually to make sure operation remains profitable for the pipeline operator. In 2013 CEPS DPO signed a 25-year contract with the company 'Aircraft Fuel Supply' (AFS) to deliver around 50 percent of the airports annual fuel needs. Most of the oil will come from Rotterdam, but can now be supplemented with oil from the Antwerp or Gent ports. The rest of the required kerosene is provided by the Amsterdam Schiphol Pipeline (ASP), in which the KLM airline is a shareholder. The national government holds a 5.92 percent share in KLM. The government is thus directly involved in transporting kerosene destined for commercial use at Schiphol through its defense ministry, and other (Eindhoven airport is also connected to CEPS) airports, and is indirectly involved through its stake in KLM" (Oxenaar 2017, 48).*

This type of conflicts of interest has led the Ministry of Justice and Security to review the civil military cooperation in the hope "to increase the resilience of society and better protect the vital infrastructure and digital security of the Netherlands" and to "improve the coordination and management of Host Nation Support" (Bijleveld-Schouten 2018, 15). The Dutch military's argument is that "the maintenance costs of the Dutch part of the CEPS pipeline are paid for by the Dutch state. Income from commercial (civil) allows the government to recuperate part of these costs. All other oil pipelines in the Netherlands are owned by privately or publicly traded companies. There is thus a clear dependency of the commercial aviation industry on government

transported fuels and vice versa, since the government needs the commercial activities to reduce CEPS maintenance costs" (Oxenaar 2017, 48). It is important to note that costs of maintenance of the CEPS pipeline do not outweigh income made from the sale of jet fuel, so most of that revenue is directed to support other Dutch military and government efforts.

Despite significant ethical problems in the Duch PPP approach, the DPO has had better success than FBG and BPO at successfully implementing cyber security programs for the CEPS pipeline, which include "pilot projects with two major ports - Rotterdam (FERN) and Schiphol (CYSSIC); coordinated vulnerability disclosure; and continuously improving information sharing agencies" (ITU 2019, 43). Furthermore, despite lack of discourse in policies about cyber-physical threats to critical energy infrastructure, the Kingdom recognizes these vulnerabilities and acknowledges the need for cyber capabilities to ensure that the Netherlands is better protected against digital threats"(Bijleveld-Schouten 2018, 25).

4.4 NATO's role in cyber-physical protection of critical energy systems and the environment

There is no definition of energy security in any NATO official documents. There is, however, a working definition of energy security promoted by the NATO Energy Security Centre of Excellence (headquartered in Vilnius, Lithuania), which states that "energy security refers to the uninterrupted availability and resiliency of energy sources to support alliance security interests" (Bagdonas 2017). This definition was drafted in response to the commitment of the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw "to develop NATO's capacity to support national authorities in protecting critical infrastructure, as well as enhancing their resilience against energy supply disruptions that could affect national and collective defense, including hybrid and cyber threats. In this context, we will include energy security considerations in training, exercises, and advance planning" (NATO 2016, para. 135). It also agrees with the International Energy Agency (IEA) that reliable, stable, and uninterrupted supply of energy

sources at an affordable price—energy security—is a requirement for peace (Gnansounou, 2008, p. 3742; Haghighi, 2008, p. 466; Hippel, Savage, & Hayes, 2011, p. 6712; see Obama et al., 2012; Pamir, 2007, p. 262; Peters, 2004, p. 190; Stefanova, 2006, p. 91; Verrastro & Ladislaw, 2007, p. 101; Yi-chong, 2006, p. 265) and economic growth (APERC, 2007; Atsumi, 2007; Bambawale & Sovacool, 2011; Climent & Pardo, 2007; Jewell, 2011). Nevertheless, a 2017 interview conducted with Michael Rühle—head of Energy Security Section, in the Emerging Security Challenges Division of NATO's International Staff—reveals that NATO energy and environmental security ends (policies) and ways (strategies and processes) have been characterized in practice 1) first and foremost by a synthesis of the positions (to include national security and financial interests) and influence of the member states; and 2) to a lesser extent, by considering the interests of supra-national organizations such as the EU or the IEA.

NATO's role in securing energy supplies and their routes in Europe emerged as a topic of concern in 2008 during the Bucharest Summit (NATO Heads of State and Government 2008) "first and foremost ensuring a steady supply of fuel to its military forces" (Khamashuridze 2008, 53). Later, during the Warsaw Summit (NATO 2016), the energy supplies were identified as one of the seven strategic civil sectors that each NATO member state is responsible to protect, among the ability to effectively 1) provide critical government services (ensure continuity of government), 2) manage the movement migrants on its territories, 3) safeguard its food and water resources, 4) deal with mass casualty incidents (MCIs), 5) secure its telecommunications and cyberspace, and 6) diversify its transportation systems (NATO 2018a). The Industrial Resources and Communications Services Group (IRCSG) is the primary body tasked by the NATO Civil Emergency Planning Committee to "examine and make recommendations to CEPC to assist allies, where appropriate, in taking measures to protect critical energy infrastructure (CEI) from all relevant threats" (NATO 2018a). Since April of 2017, the IRCSG and its working groups have been working to draft baseline requirements that NATO can use to assess the resiliency of energy supplies and associated cross-border interconnections. Among other recommendations, the 2018 State of Civil Preparedness

report included 1) the existence of national sustainability plans, 2) the redundancy of power supplies, and 3) identification and prioritization of national and cross-border critical energy systems' vulnerabilities. Nevertheless, with many of these critical infrastructures owned by private entities, NATO member states are already struggling to get a clear understanding of how energy systems affect each other and what their vulnerabilities are, particularly in the cyber domain.

Threats to the uninterrupted supply of energy sources at an affordable price have been identified by NATO as "nationalistic energy policies of producing countries, declining energy production, and poor infrastructure conditions, [as well as] terrorist attacks on pipelines and refineries" (Khamashuridze 2008, 48) and cyber-attacks:

> *"Energy security plays an important role in our common security. A stable and reliable energy supply, the diversification of routes, suppliers and energy resources, and the interconnectivity of energy networks are of critical importance and increase our resilience against political and economic pressure. While these issues are primarily the responsibility of national authorities, energy developments can have significant political and security implications for Allies and also affect our partners. Consequently, we will continue regular Allied consultations on issues related to energy security. [...] We will refine NATO's role in energy security in accordance with established principles and guidelines, and continue to develop NATO's capacity to support national authorities in protecting critical infrastructure, including against malicious hybrid and cyber activity" (NATO Heads of State and Government 2018).*

With the significant rise in the number of cyber-attacks against critical infrastructures of NATO member states, there is a renewed interest among NATO commanders in the resilience of cyber-physical systems of energy infrastructure critical for military operations. Collaboration between NATO and its member states in securing regional infrastructures from cyber threats is expected to significantly increase, particularly in the area of cyber and environmental "education and training" (Grubliauskas and Rühle 2018). In this process, NATO will remain a strict adherent of the sovereignty school of thought, and will remain concerned primarily with disruptions of supplies that would significantly affect the political and security status quo of the member states (rather than the impact of oil spills on the environment, for example). While the word resilience dominates in official documents, all NATO subject matter experts interviewed linked resilience to Article 3 of the alliance and to the responsibility of each NATO member state to maintain and

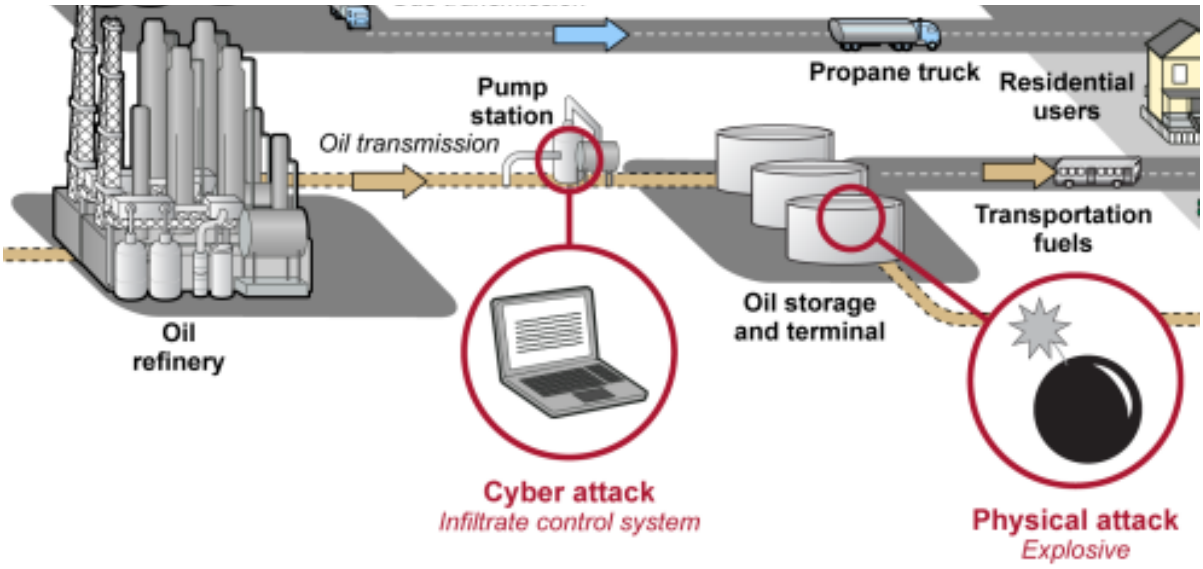
develop their individual and collective capacity to resist armed and/or cyber-attacks. Nevertheless, NATO already puts at the disposal of its member states Cyber Rapid Reaction teams that can be activated to assist in protection of domestic critical energy infrastructure, if the need ever arises.

In the cyber domain, NATO as a CSA is primarily concerned with intentional actions of stakeholders external to the Alliance, such as perceived hostile countries (i.e. Russia), terrorist organizations (i.e. ISIL), or other overly powerful actors with both capacity and willingness to abuse their position of influence at the detriment of the Alliance's member states. Particular attention is paid to external stakeholders capable of generating long term economic stresses—by casting control over geo-energy systems—or short-term physical shocks—realized through a deliberate physical and cyber-attacks of CEI to achieve political ends. Within this classic defense-centric structure, the cyber resilience of critical energy infrastructure is "capable of holding multiple dimensions and taking on different specificities depending on the country" (Chester 2010/2, 887)—explaining the resistance of NATO as a CSA to provide unified definitions of energy security or cyber security in its official documents.

The environmental and resource constraints were highlighted in the NATO 2010 Strategic Concept and are addressed today by several NATO committees and planning units; but rarely within the context of CEPS physical and cyber security. Additionally, the environmental issue is completely absent within high-levels NATO cyber-energy debates; but is reinforced at the operational and tactical levels through national efforts to reduce costs of energy (fuel consumption) without impacting military operations. Here, NATO acknowledges the impact of energy security and resilience can have on the environment, noting that "energy efficiency is important not only for logistics and cost-saving in theatres of operation, but also for the environment" (NATO 2018b). The NATO ENSEC COE was thus established to enhance energy management in the military expeditionary environment (EMMEE); that is, "to improve energy efficiency in the sustainment of military compounds through exploiting non-material aspects of energy use and power generation in operational environment without limiting operational capabilities" (Bagdonas 2016, 2017).

4.5 Conclusions

During the Cold War, traditional threats to NATO CEPS have come primarily from physical vectors. Over the past decade, however, "new threats to the nation's pipeline systems have evolved to include [...] cyber-attack or intrusion by nations" (Government Accountability Office 2018, 1) - see figure 17. Today, leaks in the pipeline could be caused by attacks against critical cyber assets, and could result in significant negative environmental consequences. The CEPS critical cyber assets are separated into critical Operational Technologies (OT) systems (that control the operations of the pipeline) and Information Technologies (IT)/OT systems (that are often used to monitor these operations). "Most pipeline systems are monitored and moderated through automated ICS or Supervisory Control and Data Acquisition (SCADA) systems using remote sensors, signals, and pre-programmed parameters to activate and deactivate valves and pumps to maintain flows within tolerances" (Government Accountability Office 2018, 9). Because of this, both IT and OT systems require "baseline and enhanced security measures" (Transportation Security Administration 2018, 16) that NATO CEPS host nations are responsible to implement. There is also little agreement between these EU member states about how to implement these measures. The EU Cyber Security Strategy for the Energy Sector acknowledges that "wherever a digital technology or an intelligent device has been implemented, even something as simple as control of a valve on a pipeline, there is a risk of it being used as an unauthorised entry point and taken over for malicious intent" (Healey et al. 2016, 15). Developing a detailed inventory of CEPS vulnerable endpoints and of their links to "remote and third party connections," has proven to be, however, a difficult endeavor (Transportation Security Administration 2018, 17), particularly due to "insufficient information sharing and coordination of action" (Healey et al. 2016, 8) among the host nations. This is due to two reasons: 1) diversity and inconsistencies in the data collected; and 2) lack of trust between the CEPS host nations.



Source: GAO analysis of Transportation Security Administration Information (GAO-19-48)
Figure 17. Cyber-physical threats to CEPS.

Interviews conducted show that NATO energy and cyber security SMEs are very much aware of diversity and inconsistency between the NATO CEPS host nations (at the EU member state level), and between the public and private entities supporting the CEPS infrastructure (at the sectoral level), but in the absence of clear EU guidance for the protection of public and private critical energy infrastructure from cyber threats, it is unlikely that they will be resolved any time in the near future. While the EU NIS Directive tasked Member States to "ensure that the competent authorities…require operators of essential services to provide…evidence of the effective implementation of security policies, such as the results of a security audit" (Healey et al. 2016, 27), for example, there is a lack of clear guidance on the valuation of these audits; so methodologies will differ from one CEPS host nation to another, as we have seen in the previous section. This also means that the data collected may also have different meanings, depending on the geographical context, and the entity that recorded it.

The roles of NATO and the EU with regards to the protection of CEPS infrastructure "are thus very much complementary" (Flamant and Parrein 2017, 28), and EU regulations and capabilities have a direct impact on NATO CEPS cyber security. With EU cybersecurity regulations failing to properly address the protection of critical energy infrastructure on the territory of its

member states, to include on the territory of the CEPS host nations, the protection of NATO CEPS becomes more dependent on the EU alliance than NATO. This is an area of concern, particularly as the flow of information between NATO and EU defence agencies concerned with cyber security threats remains minimal (at best). This is despite the fact that both the EU and NATO leaders emphasize the need for increased "international partnerships and cooperation with industry and research institutions" to guarantee Trans-Atlantic cyber resiliency (Merkel and von der Leyen 2016, 93). In fact, lack of comprehensive EU cybersecurity regulation to protect critical energy infrastructure is also attributed to lack of trust between EU member states. Some member states, for example, fear sharing vital intelligence with other European competitors. In the context of the CEPS infrastructure, for example, the CEPS host nations are also competitors in the energy field (like The Netherlands, Germany and France), and cooperation among these states in the field of cyber security has been hampered by fears of "industrial espionage" (Merkel and von der Leyen 2016, 37). Nevertheless, there is a general agreement that "the immediate and potentially catastrophic nature of the cyber threat across the Energy sector, however, demands an urgent and focussed policy response" (Healey et al. 2016, 8) across the European Union. But this lack of trust between allies means that "attempts to establish internationally binding regulations or confidence- and security-building measures may therefore have only a limited effect" (Merkel and von der Leyen 2016, 36).

There is also a lack of trust between NATO member states Russia. Given that locating pipeline leaks is a time-consuming endeavor, "pipelines [and] pump stations [...] are attractive targets for enemy air and missile attacks" (József 2013, 32). This makes the NATO CEPS a target during future military conflicts in Europe. 80 percent of the CEPS host nations and energy and cyber security SMEs interviewed for this paper (and 60 percent of pipeline operators interviewed by the GAO) "said cyber-attacks from nation-state actors were a primary threat to their industry" (Government Accountability Office 2018, 72). CEPS host nations are particularly concerned by the "modernisation and strengthening of the Russian armed forces. Increasing military activity and

hybrid threat", which includes offensive cyber capabilities (Bijleveld-Schouten 2018, 8). Russia has been particularly accused for trying to divide the European Union and undermine its relationship with NATO by pursuing "a policy of all-out assertion (Eastern flank, the Mediterranean Sea, Syria, the Balkans) and across all domains" (Macron 2017, 41), to include the cyber domain. It is thus a priority for both NATO and the EU to have "an adequate response to the use of all available (including military) Russian means of power, a way of acting that is defined today as hybrid warfare" (Flamant and Parrein 2017, 28). Because of this, an attack by Russia against the CEPS infrastructure "might be regarded as armed aggression, due to [...] scale and severity. A major cyberattack may, given the damage it could cause, justify invoking legitimate defence under Article 51 of the UN Charter" (Macron 2017, 33) or even under the NATO Article 5. The Wales NATO Summit, in particular, "added the cyber dimension to the dimensions in which NATO exercises collective defence, as it has been noticed that cyber-attacks can have the same effect on the territorial integrity of NATO countries as conventional attacks" (Flamant and Parrein 2017, 53). One of the realizations of most CEPS host nations in response to cyber threats from nation states is the need to build offensive cyber capabilities. At the alliance level, this is the case of the new "cyber-security center in Mons Belgium" (Efthymiopoulos 2019), which is expected to showcase offensive cyber capabilities capable of defending NATO critical infrastructures (such as CEPS) in Europe.

Russia is, however, not the only concern for the NATO CEPS host nations. An attack against the NATO CEPS infrastructure by "terrorist groups, criminal organisations, and skilled individuals can potentially cause serious damage with minimal effort" (Merkel and von der Leyen 2016, 36); so increasing investments "in capabilities that deny third countries access to specific areas (anti-access/area denial) are particularly significant in this context" (Merkel and von der Leyen 2016, 41). While there is "no imminent threat" (Congressional Research Service 2019, 2), these "military cyber capability also needs to be reinforced to meet the needs of collective defence. NATO considers this a national responsibility, but expects the countries that have important NATO facilities on their territory to take the lead in the matter of cyber protection" (Flamant and

Parrein 2017, 53). Because of this, the Cyber Defence Management Board (CDMB), which is the "body of NATO in charge of cyber defence affairs of the alliance" (Bettel 2018, 40), needs to take a more proactive role in working with the host nations and guarantee the protection of the NATO Pipeline System (especially as the protection of these systems is achieved with very limited national financial resources). Furthermore, the rise in variety and number of cyber threats are expected to increase the opportunities for collaboration between NATO CEPS Programme and the CEPS Host Nations (Grubliauskas and Rühle 2018).

During congressional testimony in January of 2019, the U.S. Director of National Intelligence "singled out [...] pipelines as critical infrastructure vulnerable to cyberattacks which could cause disruption for days to weeks" (Congressional Research Service 2019, 2). Therefore, the protection of CEPS "central dispatch and control centers, pumping stations, access pits and storage depots" (Butrimas 2018) from cyber security threats also needs to be urgently addressed. This is particularly relevant given the conflicting IT and OT approaches to cyber resilience, "many of which are based fundamentally on intrinsic technology design" (Healey et al. 2016, 12). Operational technologies "are the systems that detect or cause a change through the direct monitoring and/or control of physical devices, processes and events in the pipelines. OT systems include control systems (SCADA, process control systems (PCS), distributed control systems (DCS)), measurement systems and telemetry systems, which are collectively referred to as pipeline cyber assets" (Transportation Security Administration 2018, 16). The modernisation of OT infrastructure was built on existing systems that were not constructed with cyber security in mind. Because of this, the OT systems "used to operate much of the pipeline system are vulnerable to outside manipulation. An attacker can exploit a pipeline control system in a number of ways to disrupt or damage pipelines (Congressional Research Service 2019, 2). The use of smart metering by the CEPS infrastructure and the dependency on national electricity supplies that are also vulnerable to cyber-attacks. These linkages to the electric power sector have further "heightened concerns about the security risks to these pipelines" (Congressional Research Service 2019, 1); especially because many of these cyber

assets are still connected to the internet. Segregating them by "using physical separation, firewalls and other protections" (Transportation Security Administration 2018, 18) is likely to become a priority for NATO CEPS host nations over the next few years. Finally, pipelines, valves, pumps and compressors also need preventive maintenance to increase their life and avoid breaches/leaks. The inspection of these NATO CEPS infrastructures also use technologies such as smart pigs to perform various evaluations of the pipeline; and other technologies that are also vulnerable to cyber-attacks.

Chapter 5

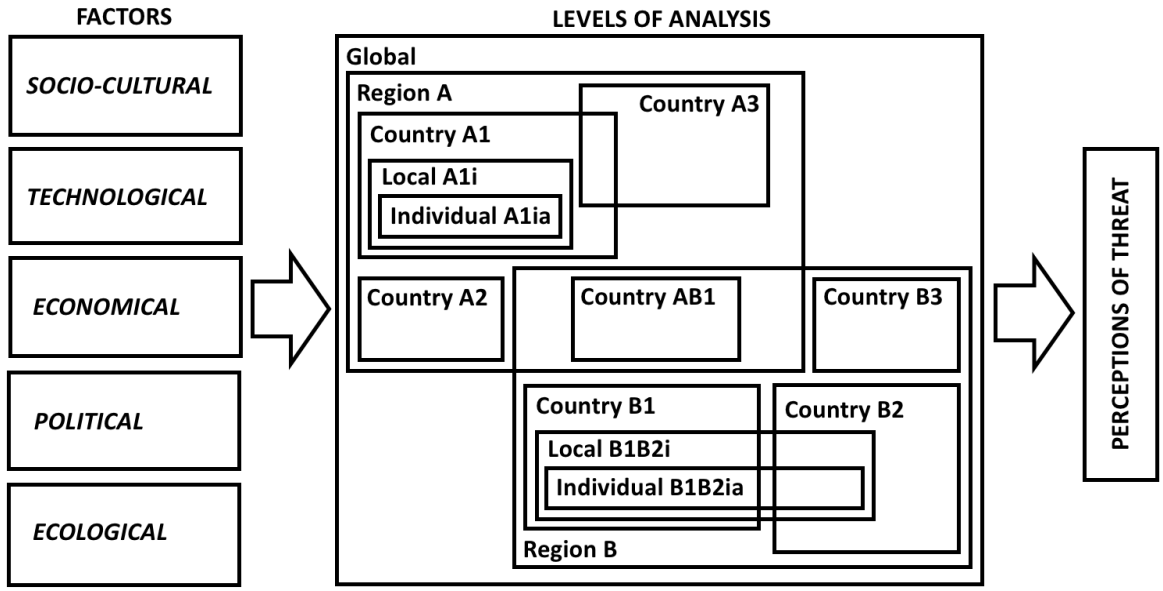
Discussions

Collective security alliances, as owners and protectors of trans-national energy infrastructures, are becoming increasingly important in shaping the security policies of regional and global energy systems in the wake of growing cyber-physical risks. As we have seen with the dependency of national airports on the NATO CEPS, the uninterrupted supply of vital energy services globally is increasingly dependent on an intricate system of regional energy market interdependencies and "vast cross-border infrastructure networks" (Chester 2010/2, 887), to include CSA-owned and operated networks. These cross-national energy networks are vulnerable to cyber-attacks (Lacher and Kumetat 2011, 4473; Onyeji, Bazilian, and Bronk 2014; Pearson 2011, 5211; Rinaldi 2004, 2); especially as infrastructure host nations diverge on appropriate responses to these cyber threats. These CSAs have also started to develop "a substantial degree of autonomy from the patterns set by the global powers" (Buzan and Wæver 2003, 4). The CEPS case analysis shows that critical energy infrastructure (Luiijf et al. 2009) protection from cyber threats, for example, no longer falls under the sole responsibility of states, but also under the responsibility of CSAs that these states belong to (Colesniuc 2013, 125; Pescaroli and Alexander 2016; Pursiainen 2009). In the case of the NATO CEPS, this has been illustrated by increased cooperation by the NATO CEPS Programme and the host nations in the area of cyber security. Thus, the CSA definitions of energy security need not only to be expanded "to cope with the challenges of a globalized world," (Yergin 2006, 78) but also to cope with the technological challenges of a regionalized one, where the notion of national energy independence is replaced with that of regional energy sustainability (Hernández et al. 2004/2, 385), resilience (Erker, Stangl, and Stoeglehner 2017), affordability (Walker et al. 2015), social (equity and health) (Vera and Langlois 2007, 878), and cyber security (Gheorghe and Muresan 2011; Nepal and Jamasb 2013, 9)—as the backbone of smart and sustainable low-carbon energy transitions.

Regional energy/cyber security integration and synchronization strategies are increasingly becoming a matter of regional security policies (Evans and Horsthemke 2019; Scholl and Westphal 4/2017, 6). This regionalization of energy-cyber security complexes and the belief that interdependence is "more intense between the actors inside such complexes than they are between actors inside the complex and those outside it" (Buzan and Wæver 2003, 4) made the energy-cyber security nexus of high importance for CSAs. But, as we have seen with the case of NATO CEPS, many factors and converging/diverging stakeholder interests can impact the implementation of regional cyber-physical securitization of energy systems.

5.1 How CSAs perceive, define, frame and manage cyber threats to vital energy systems (objective 1)

Whereas the literature review identified the constantly evolving nature of cyber threats to CEI (Chester 2010/2) and of the role of CSAs (Buzan 1983), data collected in chapter 4 highlighted the polysemic nature of the ways to protect this infrastructure considering multiple STEPE (socio-cultural, technological, economical, political, and ecological) factors and stakeholder perspectives at national and regional levels of analysis - figure 18. This shows that in order to determine Objective 1 (how CSAs perceive, define, frame and manage cyber threats to vital energy systems) and to answer Research Question 2 (how CSAs prioritize said defense), more attention needs to be given to the geo-STEPE considerations and stakeholders that can influence 1) the general aim of the CSAs; 2) their conventional/mainstream security challenges; 3) the security challenges and general policy contexts of their key member states; and 4) the configuration of their cyber-physical systems. This refocusing is needed to determine how CSA strategies are likely to change in the future to protect CEI from cyber threats during smart and sustainable low-carbon energy transitions.



Source: Author's own representation.
Figure 18: Multi-level and multi-lateral perceptions of cyber-physical threats.

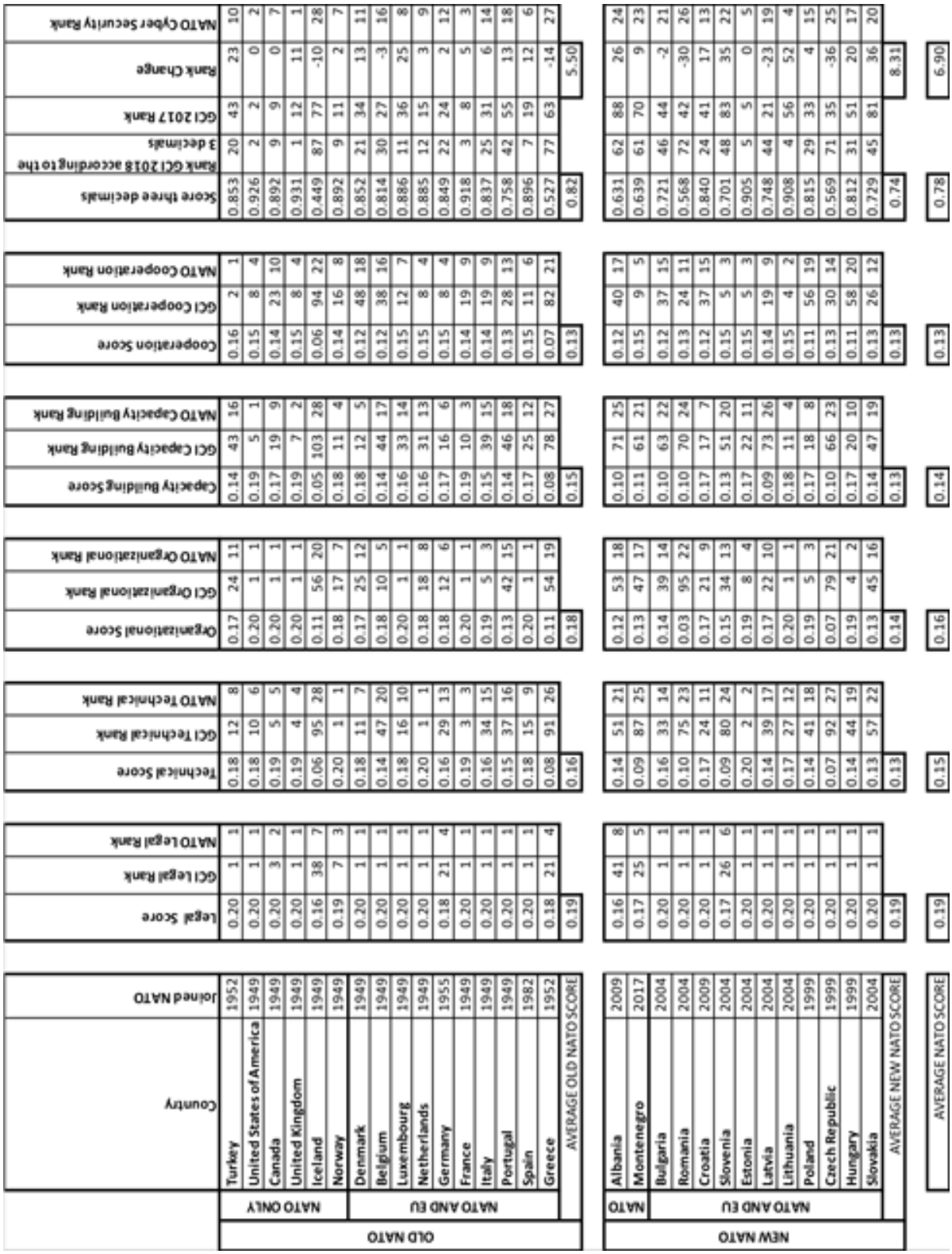
5.1.1 The Geo-STEPE divide

In order to protect the cyber-physical energy supply chains and their geo-energy systems, regional security arrangements "should command long-term commitment, determination, focus and resources with a high level of integration of energy policies across scales of governance, supply and demand sides of energy systems, and energy technologies" (Cherp, Jewell, and Goldthau 2011, 75). These obligations require crossing the social, political, economic, cultural, knowledge, and digital (SPECKD) divides (Elias G. Carayannis, Kaloudis, and Mariussen 2008) in negotiations among actors of different backgrounds, which is harder to achieve within regional than national settings. Citing Huntington, Tana Johnson—Assistant Professor of public policy at Duke University—described the socio-cultural divide as the main challenge in finding common energy security solutions for the Global Governance 2022 Scenarios—an independent initiative comprised of 24 fellows from the U.S., China, and Germany (Cheng et al. 2013). Although the expectation is that geographical neighbors share many values and beliefs, this is not always the case, and mistrust among states often complicates negotiations in the fields of energy and cyber security (as we have

seen with the fear of cyber espionage among the NATO CEPS host nations). These socio-cultural divides are further exacerbated by economic factors (democracy vs. profit considerations, competition among cyber security firms, etc.), technology transfer complications (and growing roadblocks to free trade), and lack of coherent legislation (with conflicting security vs. privacy implications). For these reasons, while regional cyber security cooperation (particularly in the energy field) is heavily promoted at all levels of international relations, regional dialogue on cyber security (particularly within the context of CEIP and the smart and sustainable low-carbon energy transitions) remains limited.

In chapter 4, we observed how the ITU—composed of over 800 members from industry, government, and academia—GCI used, however, the geo-STEPE considerations as a strength rather than a weakness in cyber security assessments. The GCI also highlighted that some countries (such as Singapore, the US, UK, Russia, France, Estonia, Canada and Israel) managed to overcome geo-STEPE challenges by balancing competitive factors without sacrificing the positive competitive requirements of innovation (Firdous 2018). The GCI considers legal, technical, organizational, capacity, and cross border cooperation (in a multi-stakeholder environment) indicators worth further consideration when assessing the cyber preparedness of CSAs to tackle cyber threats to CEI during smart and sustainable low-carbon energy transitions. For NATO, for example, it also shows that cyber security resilience is not dependent only on financial resources, where nations of old NATO ought to be better prepared than nations of new NATO. Instead, some new NATO member states (such as Estonia and Lithuania) with big financial resource limitations seem to be better prepared for the growing cyber threats within NATO (see table 30). This means that achieving the technical means to defend from cyber threats is more dependent on ways (strategies) and ends (political goals) than means (financial resources). These ways and means are dependent on stakeholders that rarely all agree on what CEI needs to be protected, from what cyber threats and by what means. One such challenge is the implementation of environmental considerations in the ways (as seen with the proposed CARVER methodology), which the GCI is

found missing.



		Country	Joined NATO	Legal Score	GCI Legal Rank	NATO Legal Rank	Technical Score	GCI Technical Rank	NATO Technical Rank	Organizational Score	GCI Organizational Rank	NATO Organizational Rank	Capacity Building Score	GCI Capacity Building Rank	NATO Capacity Building Rank	Cooperation Score	GCI Cooperation Rank	NATO Cooperation Rank	Score three decimals	Rank GCI 2018 according to the 3 decimals	GCI 2017 Rank	Rank Change	NATO Cyber Security Rank
OLD NATO	NATO ONLY	Turkey	1952	0.20	1	1	0.18	12	8	0.17	24	11	0.14	43	16	0.16	2	1	0.853	20	43	23	10
		United States of America	1949	0.20	1	1	0.18	10	6	0.20	1	1	0.19	5	1	0.15	8	4	0.926	2	2	0	2
		Canada	1949	0.20	3	2	0.19	5	5	0.20	1	1	0.17	19	9	0.14	23	10	0.892	9	9	0	7
		United Kingdom	1949	0.20	1	1	0.19	4	4	0.20	1	1	0.19	7	2	0.15	8	4	0.931	1	12	11	1
		Iceland	1949	0.16	38	7	0.06	95	28	0.11	56	20	0.05	103	28	0.06	94	22	0.449	87	77	-10	28
		Norway	1949	0.19	7	3	0.20	1	1	0.18	17	7	0.18	11	4	0.14	16	8	0.892	9	11	2	7
	NATO AND EU	Denmark	1949	0.20	1	1	0.18	11	7	0.17	25	12	0.18	12	5	0.12	48	18	0.852	21	34	13	11
		Belgium	1949	0.20	1	1	0.14	47	20	0.18	10	5	0.14	44	17	0.12	38	16	0.814	30	27	-3	16
		Luxembourg	1949	0.20	1	1	0.18	16	10	0.20	1	1	0.16	33	14	0.15	12	7	0.886	11	36	25	8
		Netherlands	1949	0.20	1	1	0.20	1	1	0.18	18	8	0.16	31	13	0.15	8	4	0.885	12	15	3	9
		Germany	1955	0.18	21	4	0.16	29	13	0.18	12	6	0.17	16	6	0.15	8	4	0.849	22	24	2	12
		France	1949	0.20	1	1	0.19	3	3	0.20	1	1	0.19	10	3	0.14	19	9	0.918	3	8	5	3
		Italy	1949	0.20	1	1	0.16	34	15	0.19	5	3	0.15	39	15	0.14	19	9	0.837	25	31	6	14
		Portugal	1949	0.20	1	1	0.15	37	16	0.13	42	15	0.14	46	18	0.13	28	13	0.758	42	55	13	18
		Spain	1982	0.20	1	1	0.18	15	9	0.20	1	1	0.17	25	12	0.15	11	6	0.896	7	19	12	6
		Greece	1952	0.18	21	4	0.08	91	26	0.11	54	19	0.08	78	27	0.07	82	21	0.527	77	63	-14	27
		AVERAGE OLD NATO SCORE		0.19			0.16			0.18			0.15			0.13			0.82			5.50	
NEW NATO	NATO	Albania	2009	0.16	41	8	0.14	51	21	0.12	53	18	0.10	71	25	0.12	40	17	0.631	62	88	26	24
		Montenegro	2017	0.17	25	5	0.09	87	25	0.13	47	17	0.11	61	21	0.15	9	5	0.639	61	70	9	23
	NATO AND EU	Bulgaria	2004	0.20	1	1	0.16	33	14	0.14	39	14	0.10	63	22	0.12	37	15	0.721	46	44	-2	21
		Romania	2004	0.20	1	1	0.10	75	23	0.03	95	22	0.10	70	24	0.13	24	11	0.568	72	42	-30	26
		Croatia	2009	0.20	1	1	0.17	24	11	0.17	21	9	0.17	17	7	0.12	37	15	0.840	24	41	17	13
		Slovenia	2004	0.17	26	6	0.09	80	24	0.15	34	13	0.13	51	20	0.15	5	3	0.701	48	83	35	22
		Estonia	2004	0.20	1	1	0.20	2	2	0.19	8	4	0.17	22	11	0.15	5	3	0.905	5	5	0	5
		Latvia	2004	0.20	1	1	0.14	39	17	0.17	22	10	0.09	73	26	0.14	19	9	0.748	44	21	-23	19
		Lithuania	2004	0.20	1	1	0.17	27	12	0.20	1	1	0.18	11	4	0.15	4	2	0.908	4	56	52	4
		Poland	1999	0.20	1	1	0.14	41	18	0.19	5	3	0.17	18	8	0.11	56	19	0.815	29	33	4	15
		Czech Republic	1999	0.20	1	1	0.07	92	27	0.07	79	21	0.10	66	23	0.13	30	14	0.569	71	35	-36	25
		Hungary	1999	0.20	1	1	0.14	44	19	0.19	4	2	0.17	20	10	0.11	58	20	0.812	31	51	20	17
		Slovakia	2004	0.20	1	1	0.13	57	22	0.13	45	16	0.14	47	19	0.13	26	12	0.729	45	81	36	20
		AVERAGE NEW NATO SCORE		0.19			0.13			0.14			0.13			0.13			0.74			8.31	
		AVERAGE NATO SCORE		0.19			0.15			0.16			0.14			0.13			0.78			6.90	

Source: Built with 2018 data from the International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI)

Table 30. New NATO and Old NATO legal, technical, organizational, capacity, and cross border cooperation considerations for cyber security of critical infrastructure

5.1.2 The stakeholder divide

The key energy security actors in government and/or international organizations (producing and consuming nations, OPEC and/or Gas OPEC member states, IEA/G8 members, etc.), industry (energy companies, carriers, PES transportation companies, etc.), academia, and civil society (NGOs, consumers, prosumers, etc.) not only differ from one region to another, so do their priorities and stakes in each region. These stakeholders also have diverging views on the implication of technology transformations (AI and cyber centric) for smart and sustainable low-carbon energy transitions. The challenge to deduce simple, universal solutions (panaceas) in multi-stakeholder, "highly context dependent" (Kruyt et al. 2009/6) environments (see Ostrom) is thus multiplied in regional fractal, multi-level, multi-modal, multi-nodal, and multi-lateral (Elias G. Carayannis 2008) settings when compared to national settings. This effort "calls for wide involvement of different actors as well as flexibility, innovation, openness and diversity. Nations, energy industries, and communities will need to find unique, [innovative] solutions that work for them. No panaceas, either technological or institutional, are likely to succeed" (Cherp, Jewell, and Goldthau 2011, 75) without proper calibration of measures (Ragin 2009) during smart and sustainable low-carbon energy transitions. Additionally, supranational institutions (such as CSAs) currently struggle with the difficulty to account for all actors with a stake in cyber security for sustainable energy transformations at both national and regional levels. This is caused primarily by a lack of transparency about CEI vulnerabilities at national levels. While the International Energy Forum (IEF), for example, "has emerged as an organization in which consumer and producer countries join a dialogue about stabilizing energy markets and improving transparency in energy markets," its reach has been limited (Cheng et al. 2013). Chester argued that this is because

> *"twenty-first century access to energy sources depends on a complex system of global markets, vast cross-border infrastructure networks, a small group of primary energy suppliers, and interdependencies with financial markets and technology. […] An examination of explicit and inferred definitions finds that the concept of energy security is*

> *inherently slippery because it is polysemic in nature, capable of holding multiple dimensions and taking on different specificities depending on the country (or continent), timeframe or energy source to which it is applied. This 'slipperiness' poses analytical, prediction and policy difficulties" (Chester 2010/2).*

In the process of identifying regional cyber threats to sustainable energy security or planning and implementing responses, it is important to understand the decision-making mechanisms—which "must involve multiple stakeholders" (Cheng et al. 2013)—with the influence and determination to affect cyber security for smart and sustainable low-carbon energy transitions. The Stakeholder Analysis (SA) is a methodology that can be used to prioritize both threats and cyber risk mitigation strategies or responses by accounting for—and often incorporating—the needs of those who have a 'stake' or an interest in the outcomes. Mitchell, Agle and Wood proposed that classes of stakeholders can be identified by their possession or attributed possession of one, two, or all three of the following attributes: 1) the legitimacy of the outcome's impact on the stakeholder (what legitimizes their position); 2) "the urgency of the stakeholder's claim" concerning the outcome (an indicator of their outcome's salience); and 3) "the stakeholder's power to influence" the outcome (their influence) (Mitchell, Agle, and Wood 1997, 854).

5.2 Back to NATO CEPS: the need for a stakeholder analysis

Identifying CEI cyber-physical threats to all the potential stakeholders during smart and sustainable low-carbon energy transitions is important in predicting the success of CSA cybersecurity objectives because stakeholders have the power to "prevent our accomplishments" (R. E. Freeman 2010, 52), and thus determine the outcomes. Lack of trust between French and German intelligence agencies, for example, severely impacts the effectiveness of NATO CEPS cyber security efforts during smart and sustainable low-carbon energy transitions. Managing the relationship with key stakeholders—despite the conflict of interest between them—is not only important to the understanding of regional mechanisms and interactions, but also to facilitating the

regional dialogue between them on cyber security during the entire process of smart and sustainable low-carbon energy transitions, which is currently missing.

5.2.1 Stakeholders of NATO CEPS cyber-energy security during smart and sustainable low-carbon energy transitions

A stakeholder analysis of geo-energy systems has identified the following key, primary, and secondary stakeholders (Miron and Preda 2009) that would also need to be considered when developing NATO CEPS cyber security strategies in the context of smart and sustainable low-carbon energy transitions:

- Key Stakeholders, "who can significantly influence or are important to the success of a project or a programme (according to the major policy objectives and to the purpose of the respective programme)" (Miron and Preda 2009, 878) include:
    - *Regional integration structures*. Regional integration is the "voluntary linking in the economic and political domains of two or more formerly independent states to the extent that authority over key areas of national policy is shifted towards the supranational level" (Mattli 1999, 1). The European Union cyber security regulations, for example, can be critical in guiding the priorities for the protection of NATO CEPS from cyber-attacks;
    - *Other CSAs and international organizations (IOs)*. CSAs and IOs have an increasing interest in cyber security, and are directly impacted by attacks against energy infrastructures of their member states. In fact, "most global, transatlantic and regional international organisations (UN, NATO, the EU, G8, OSCD, OECD, ITU, ICANN, AU, ASEAN, OAS, etc.) have developed policies and instruments to address the growing sophistication of cyber-attacks against critical infrastructures and services" (Pernik 2014, 1). Examples of other CSA actions with an impact on NATO CEPS include NATO's "Smart Defence" policy (E. G. Carayannis,

Campbell, and Efthymiopoulos 2014; Efthymiopoulos 2014), and the creation of a NATO Cyber Command in Belgium by 2022, the establishment of the European Defense Agency (EDA) in 2004 (Mix 2011), and even the growing focus of the Shanghai Cooperation Organization on cyber (Boland 2011), etc;

- *Public authorities*. These may include energy regulatory bodies of CSA member states, ministry of economic affairs or department of commerce, national competition regulator bodies, etc.;
- *Defense agencies*. These have had a major influence on the development of national cyber security strategies (NCSS) in Australia, Canada, China, Czech Republic, Estonia, France, Germany, India, Israel, Japan, Lithuania, Luxembourg, Romania, Russia, the Netherlands, New Zealand, South Africa, Spain, Uganda, the United States, the UK, etc. (Luiijf, Besseling, and De Graaf 2013). As we have seen with the case of NATO CEPS, host nations cyber security strategies impacted the security of NATO CEI from cyber-physical vulnerabilities;
- *Utility companies (generation and transmission)*. Utility companies are "increasingly using information and communication technology (ICT) to increase the efficiency and reliability of the grid" (Pearson 2011). NATO CEPS is often dependent on access to electricity provided by these companies-which transcends national borders;
- *Actors in the energy sector*. Often, within CSAs, energy actors of member states are in competition with each other, so sharing of information to combat cyber threats against CEI can be slow - and this is also the case with sharing on collaboration among NATO CEPS partners;
- *International financial bodies*. As we have seen with NATO CEPS, host nation support depends on limited access to resources, so international financial bodies can have a direct impact on cyber security;
- *Political parties*. Politics can also impact the implementation of cyber security

strategies by CSAs, particularly when cyber security is perceived as too high of a cost, and resources are diverted toward other endeavors (ro promote other government successes). In the Netherlands, for example, much of the profits made by the government through the selling of NATO CEPS delivered jet fuels is redirected toward other priorities rather than cyber security of the pipeline;

- *Other influential lobby groups*. In France, for example, we have seen that the NATO CEPS pipeline is used to deliver fuels to Paris during political and social turmoil (particular during strikes); this also increases the cyber threats to the pipeline during these social movements.

- Primary Stakeholders, "individuals, groups of individuals or institutions who are affected either positively (beneficiaries) or negatively by a project or a programme who has impact on them; in most projects primary stakeholders will be categorised according to project objectives and social analysis" (Miron and Preda 2009, 878):
  - *Energy production and distribution companies*. Cyber-attacks against Germany's FBG or France's TRAPIL, could cripple much of the NATO CEPS operations;
  - *Cyber security vendors*. The author has identified some 1962 vendors and 5932 cyber security products (at different levels of development) that could impact the cyber security of CSA CEI;
  - *Strategic investors*. Cyber security is dependent on CEI investments; and
  - *Energy consumers and prosumers*. Some civilian airports, for example, are fully dependent on NATO CEPS jet fuels supply.
- Secondary Stakeholders, "different intermediary entities in the process of delivering the activities comprising the project or programme, who can or cannot take part in the decision-making process and who can be influenced positively or negatively" (Miron and Preda 2009, 878):
  - *Potential investors*. Investment in cyber security companies by VCs, for example, have

doubled between 2016 and 2018;

- *Energy suppliers*. Much of the fuels transported through the CEPS pipeline comes from ships that are also vulnerable to cyber-attacks;
- *Energy transportation companies*. Once fuels reach key points, they are loaded onto trucks and delivered to clients. If the pipeline goes down, this also impacts these companies' ability to deliver fuel to their clients;
- *Equipment suppliers*. Pumps, valves, and other smart equipment used by the CEPS pipeline need to have cyber security firewalls, and their failure to operate will also impact future business with the suppliers;
- *Research institutes in the energy sector*. This is done within most nations, but lack of resources also lead to lack of comprehensive cyber security solutions;
- *Regional centres of excellence*. These include the Estonian-based Cooperative Cyber Defence Centre of Excellence (CCD CoE) (R. Hughes 2009), the Lithuania-based Energy Security Centre of Excellence (ENSEC CoE) (Molis and Vaišnoras 2010), the Finland-based European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (Møller and Petersson 2019);
- *Banks financing projects in energy sector*. These banks are critical in financing CEPS operations in Germany, France, and The Netherlands, where projects of CEPS private partners are regularly funded by private banks;
- *Consultancy firms*. These are often brought in by CEPS private partners in Germany, France, and The Netherlands to consult on cyber security threats;
- *Employees of the companies in the sector*. During a strike in France, a disgruntled oil and gas employee could be compelled to attack the NATO CEPS infrastructure with cyber malware (insider threat) disabling it for days or even weeks;
- *Trading unions of the companies in the sector*. Delivery of jet fuels through the NATO CEPS is rarely affected by the actions of trade unions, but the operation of the

pipeline could have a direct effect on trading unions (as discussed before).

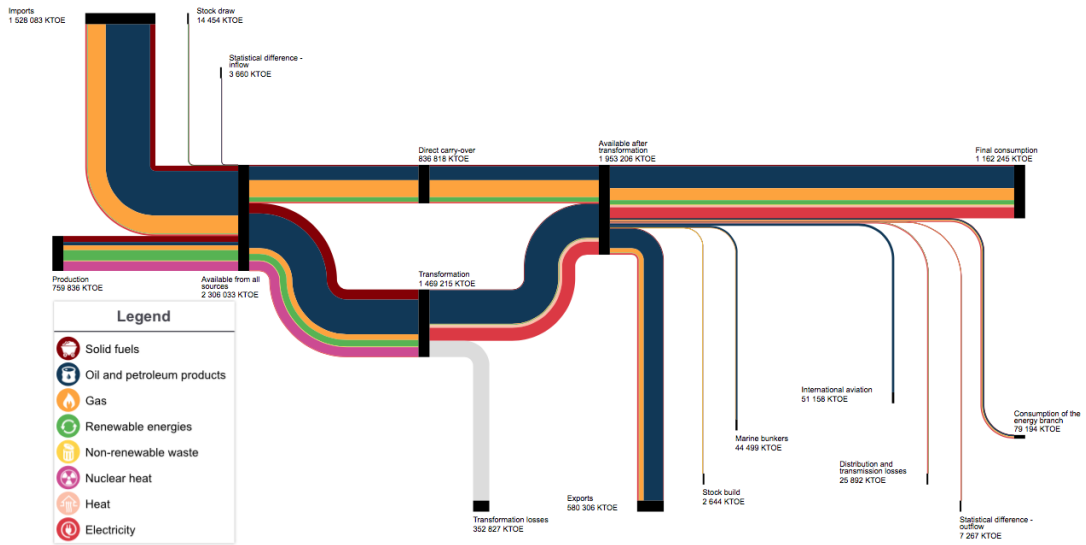
- *NGOs*. The NATO CEPS pipeline does not assist in decreasing the consumption of fuels, and host nations tend to be less sustainable than their neighbors. NGOs can have a direct impact on increasing resiliency of the pipeline by pushing for more diversified and sustainable sources; and
- *Other employers and professional associations in the sector*. This includes regular forums where these cyber threats to CSA CEI are discussed and solutions proposed.

5.2.2 The EU as a stakeholder of NATO CEPS cyber security

At the advent of regional cyber-physical threats, we are also witnessing a shift from vertical (state-level) toward horizontal (systemic-level) authority cyber defense structures within geo-energy spaces. Additionally, collective economic alliances (such as the EU) have also been forced to behave more like collective security alliances, and sometimes even used their economic and political tools to influence regional security policies that were traditionally shaped by nation states. The EU, for example, has largely influenced the regional securitization of the new energy sources supply chains (production, transportation, and distribution) and of the cyber-physical approaches to protect them at the regional level. This explains, for example, why the EU (with the additional political and economic instruments) has had more success in shaping regional energy and cyber security policy of its member states than NATO. EU's legitimacy to address cyber-physical threats rests in its policy and economic instruments that NATO does not have access to. While NATO, like the European Union Agency for Cybersecurity (ENISA), does not have the authority or legitimacy to impose the regional implementation of cyber security policies and standards, the EU has other ways to coerce nations to place common interests/security above local/national politics. The EU's economy is also more at risk of being directly impacted by a cyber-attack against its critical energy infrastructure. Even a cyber-attack on the NATO CEPS infrastructure would impact the civilian airports and European economy more than the military airfields and European security. As a result,

EU securitization efforts have also directly affected the way that NATO infrastructure (such as CEPS) is protected; meaning that a discussion on EU as a stakeholder is warranted.

The 2014 European Energy Security Strategy starts with a simple, but very clear message: that "the European Union's prosperity and security hinges on a stable and abundant supply of energy" (COM(2014)330). In contrast to NATO—a strict adherent of the neorealist sovereignty school of thought, promoting energy security for its member states—the EU Energy Security Strategy places the Resilience and Robustness of the union above the energy security of the state. On the robustness side, the EU recognizes its domestic scarcity of resources; and that predicted growth in domestic oil and gas demand will increase its dependency on imports from the Gulf states and the Former Soviet Union (FSU). With energy representing over 20% of total EU imports and these energy imports representing more than half of all the energy it consumes (see figure 19), the EU is currently struggling to move "from a fossil fuels-based energy system to a low-carbon and fully digital and consumer centric one" (COM(2017)688).



Source: EU Sankey Diagram (EUROSTAT 2017)
Figure 19. 2017 EU Sankey Diagram using the MOSES (Jewell 2011) energy systems approach.

On the resilience side, the Energy Union, the EU energy security strategy, and the third package accommodate for transitory shocks such as "regulatory changes, unforeseeable economic crises (or booms), change of political regimes, disruptive technologies, and climate fluctuations"

(Cherp & Jewell, 2011). As such, the Energy Union became one of the ten priorities of the European Commission; the Third Package promoted the independence of regulatory authorities from both government regulation and industry; and smart and sustainable low-carbon energy transitions became inseparable from the concept of energy security in Europe (COM(2014)330). Here, the smart and sustainable low-carbon energy transitions is defined by the 20/20/20 targets set by the Union to be attained by 2020: 1) 20% reduction in greenhouse gas emissions [24% reduction expected by 2020 and 32% by 2030], 2) increase to 20% share of renewable energy as a proportion of final energy consumed [expected to reach 21% by 2020 and 24% by 2030] (see table 30), and 3) 20% improvements in energy efficiency; all compared to 1990 levels (COM(2014)15). Of note is that all CEPS member states are failing to meet their 2020 RES commitments.

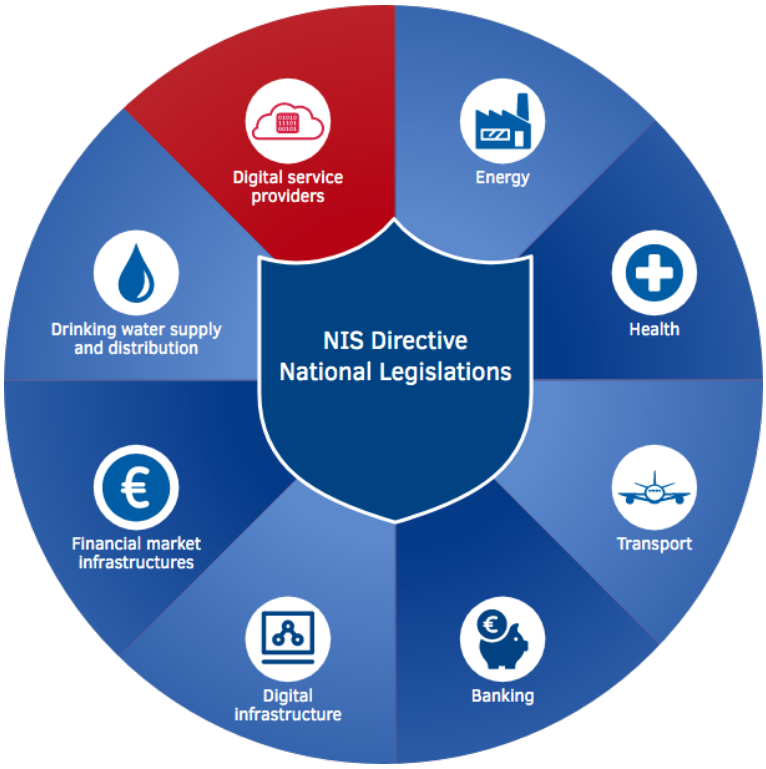
Nation-States	EU	2015 RES	2020 target	Complete
Austria	1995	33	34	97%
Belgium	1958	7.9	13	61%
Bulgaria	*2007*	*18.2*	*16*	100%
Croatia	*2013*	*29*	*20*	100%
Cyprus	2004	9.4	13	72%
Czech Republic	2004	15.1	13	100%
Denmark	1973	30.8	30	100%
Estonia	2004	28.6	25	100%
Finland	1995	39.3	38	100%
France	1958	15.2	23	66%
Germany	1958	14.6	18	81%
Greece	*1981*	*15.4*	*18*	86%
Hungary	2004	14.5	13	100%
Ireland	1973	9.2	16	58%
Italy	1958	17.5	17	100%
Latvia	2004	37.6	40	94%
Lithuania	2004	25.8	23	100%
Luxembourg	1958	5	11	45%
Malta	2004	5	10	50%
Nethrelands	1958	5.8	14	41%
Poland	2004	11.8	15	79%
Portugal	1986	28	31	90%
Romania	*2007*	*24.8*	*24*	100%
Slovakia	2004	12.9	14	92%
Slovenia	*2004*	*22*	*25*	88%
Spain	1986	16.2	20	81%
Sweden	1995	53.9	49	100%
UK	1973	8.2	15	55%
			Average	**83%**

Table 31: EU with shares of gross final consumption of RES in 2015 and 2020 target

Within the CSDP framework, the EU also relies on building partnership capacity and on equipping and training specialists to proactively predict, prevent, and pre-empt (4P) energy security shocks and stresses in a multi-national environment. The CSDP emerged recently as a vital institution with the EU for sharing vital intelligence and with the capabilities necessary to insure CEIP during smart and sustainable low-carbon energy transitions. From 2015 until 2019, the European Defence Agency (EDA, which supports CSDP operations) was tasked with organizing the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS) and "continue to examine how technological and regulatory progress made in energy efficiency,

renewable energy and protection of critical energy infrastructures could also be successfully applied to the defence and security sector" (EDA, 2018). Its three working groups focus on 1) Energy Management (EM) and Energy Efficiency (EE), 2) Renewable Energy Sources and Technologies (RES), and 3) Critical Energy Infrastructure Protection (CEIP). This effort is critical for the development of Euro-centric energy systems that offer flexibility, adaptability, and diversity; ensuring protection through spreading risks and preparing for surprises (Cherp & Jewell, 2011).

Protection of the EU's critical energy infrastructure—to include CEPS—from cyber-attacks falls under the responsibilities of the third working group, the Critical Energy Infrastructure Protection (CEIP). With the EU energy infrastructure "transitioning into a decentralised, digitalised smart energy system" (Healey et al. 2016, 1), both the EU and NATO critical geo-energy chains are becoming more vulnerable to cyber-attacks. Because of this challenge, the EU Network and Information Security (NIS) Directive highlights the importance of "cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc." (EU 2016/1148). The EU has also been tackling the issue of cyber security for energy infrastructure in official statements, highlighting the need for collective cyber security in the energy field, particularly in the oil, gas, and electricity sectors (figure 20).



Source: ENISA.
Figure 20: Sectors under the European NIS Directive.

The EU NIS did not provide, however, clear direction to how cyber assessments are to be conducted, particularly in the energy field. This issue is, however, not sui generis for the EU, but also an issue within every NATO member state. This is particularly because of resistance from energy lobby groups. For example, within the U.S., the "Implementing Recommendations of the 9/11 Commission Act of 2007" (P.L. 110-53) directed TSA to "promulgate pipeline security regulations and carry out necessary inspection and enforcement if the agency determines that regulations are appropriate" (§1557(d)). In over one decade since this requirement was passed, no such regulation has been drafted; compliance of industry with pipeline cyber security guidelines being completely voluntary, with industry arguing that "regulations are unnecessary because pipeline operators have voluntarily implemented effective physical and cybersecurity programs" (Congressional Research Service 2019, 2). This is despite the fact that in 2018 the GAO study identified a number of weaknesses in the industry's voluntary compliance with the TSA program, to include "inadequate staffing, outdated risk assessments, and uncertainty about the content and

effectiveness of its security standards" (Congressional Research Service 2019, 2). Interviews reveal that ALL of these issues also apply in Europe, and particularly in the case of the CEPS pipeline.

Despite the fact that the energy and cyber security strategies of NATO and the E.U. (through the CSDP) are at different stages of development, these two CSAs complement each other and will both play an important role in shaping the security of the NATO CEPS. By understanding the E.U. energy security strategies and NATO cyber security capabilities, the similarities and differences between the two would be useful to understand how other CSAs, like Benelux, or Eu Med will deal with threats to cyber-physical energy systems in the future. It is worth nothing here, that while there is cooperation and complementation between NATO and the EU in the field of cyber security, there is also competition. As such, any commitment of national resources to NATO capabilities is often seen by EU defense experts interviewed as a threat to European defense. With the EU increasingly perceiving NATO as a competitor, it is expected that collaboration in the cybersecurity field will also be affected.

5.3 CSAs and the future of CEIP in the cyber domain

As seen above, the CEPS stakeholders are not limited only to nation state governments; but include actors from government, industry, academia, and media or civil society. While the case study paid attention to some of the key stakeholders of NATO CEPS that can influence cyber security policies, more attention needs to be paid to primary and secondary stakeholders in future studies. For example, more attention needs to be paid to how the media and civil society can influence policies of CEPS member states. Furthermore, with the focus of CEPS being primarily to transport fuels, more attention needs to be paid to how renewable energy policies (both national and european) will impact the future of CEPS operations.

Potential stakeholders (discussed in section 5.2.2) within each CSA, their interests, and their influence are major stages in stakeholder analysis (Wolfe and Putler 2002, 65) that directly affect

the implementation and effectiveness of regional cyber-physical policies. This stakeholder analysis (PRMPS 2009, 1) of regional cyber-energy policies must thus consider four major attributes: 1) the CSA stakeholders' position on the regional cyber-energy policies; 2) the level of influence that CSA stakeholders hold in drafting and enforcing regional cyber-energy policies; 3) the level of interest that cyber threats to critical energy infrastructure instills in the CSA stakeholder, or salience; and 4) any additional group/coalition/alliance to which CSA stakeholders belong to or can reasonably be associated with. This last element is also important to consider because, as we have seen in the previous section, EU cyber security policies have a direct impact on how NATO CEPS infrastructure is protected from cyber threats.

Each CSA stakeholder's position can be ascertained by analyzing both the information reported directly by the stakeholder (eq, in official CSA documents) and through secondary information (eq, news interviews). To clearly define this position, knowledge of cyber security supporters and opponents must be correlated with advantages and disadvantages of the outcome to each CSA stakeholders. A position map must thus illustrate more than just which CSA stakeholders support or oppose an outcome, but must also answer the question why they support or oppose the outcome (in our case, cyber-physical security of critical energy infrastructure). With regards to the NATO CEPS, we see for example resistance to better integration between NATO CEPS host nations because of lack of perceived trust and competitive nature of some of these relations between them.

Salience is defined as "the ability of a particular form of information presentation to grab a person's attention, regardless of the importance of the task or goal in which the person was previously engaged" (Endsley 2016, 255). While it is safe to agree that under normal circumstances all stakeholders are rational entities, outside pressure (and the perceived idea of necessity) cuts down the time allocated to planning, and forces the stakeholders on autopilot, where they rely on limited information and instinct (past experiences) in their decision making process. In fact, researchers believe that "most of the decisions we make are made mindlessly, with little thought at all. Our

minds are programmed with persuasion triggers when we receive an appropriate cue" (Mills 2000, 218). In a collective security environment, CSA stakeholders need to be able to weigh the salience of cyber security objectively, rather than in contrast to other competing public-private interests (like the cost of cyber security on major energy companies, for example).

Influence refers to how persuasive a CSA stakeholder is in converting other CSA stakeholders into true believers that are willing and eager to effect change and to bring out desired outcomes. Assessing the influence of each CSA stakeholder of shape and enforce regional cybersecurity regulations is perhaps the most important step of a CSA-level stakeholder analysis. The more influential a group is, the closer the attention paid to it should be (hence, the classification into key, primary, and secondary stakeholders). In the case of NATO CEPS, we notice, for example, that host nations had more influence over how the pipeline is protected from cyber threats than the NATO CEPS Programme.

5.3.1 The impact of group politics on cyber threat prioritization

The regional group/alliance association is also important to consider because they can further complicate how CSAs perceive, define, frame and manage emerging cyber threats to vital energy systems. It also determines how environmental considerations are imbedded into CSA cyber defense strategies. Fortunately, much of these assessments can be done using predictive analytics tools. To quote physicist and author Barabási, "driven mainly by commercial interests, predictive tools will continue to improve, particularly those that quantify individual behavior. And to further enhance their accuracy, these tools will move from focusing on individuals, to focusing on the groups they belong to" (Barabasi 2010, 252). These tools can also be used to further refine the stakeholder lists that we have addressed above. For example, Karabaich's taxonomy of 14 questions can be used to develop a rough idea of "who" the CSA stakeholders really are: 1. Why have the individuals formed the group? 2. How are events and other groups external to the group perceived?

3. What has the group been trying to achieve recently, as indicated by their propaganda and activities? 4. What is perceived to be the most effective means of pursuing these goals? 5. What are the perceived utility and role of different means for advancing the group's interests? 6. What is the role of chance/fate in the group's philosophy? 7. What is the best approach for selecting the goals for action? 8. What are the perceived chances of achieving the goals? 9. What are the perceived acceptable means of achieving the goals? 10. What is the best approach to calculation, control, and acceptance of risks? 11. What is the best timing of action? 12. What are the perceived constraints on achieving the goals? 13. What is their level of commitment? and 14. How is the group perceived by the larger group? (Karabaich 2004). For the purpose of future cyber assessments during smart and sustainable low-carbon energy transitions (that embrace environmental considerations for new energy technologies), these questions can be reframed in the following way:

1. Identify the key, primary, and secondary groups of CSA stakeholders invested in cyber security for critical energy infrastructure during smart and sustainable low-carbon energy transitions;
2. What is the CSA stakeholders' position on cyber and environmental security for critical energy infrastructure during smart and sustainable low-carbon energy transitions? (What do they SAY they want?)
    a. Larger Goal: Why did the individuals form the group?
    b. Short Term Goals: as indicated by public statements and activities.
    c. Long Term Strategy: How do short term goals fit into the larger goal?
3. How focused are they on cyber and environmental security for critical energy infrastructure during smart and sustainable low-carbon energy transitions when compared to other organizational goals?
    a. Level of Commitment: What is the level of commitment of both leaders and members to short term and larger goals?
        i. What choices do they have? Identify the perceived constraints (look at

situational factors and beliefs that affect the outcome).

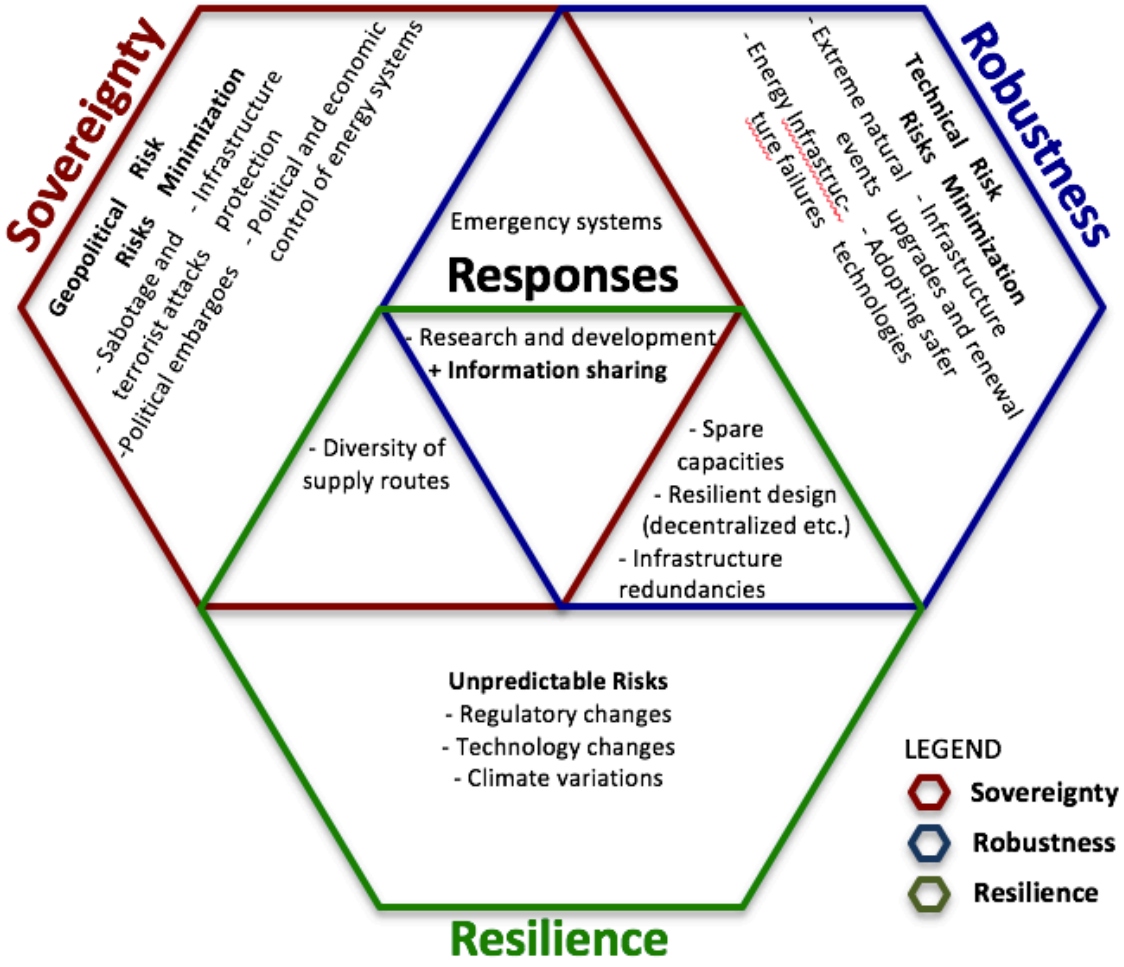
ii. What risks are they willing to take? Identify the perceived acceptable means of achieving goals (compare to norms of members or society) and the mechanisms the group uses to control risks.

4. What is the level of influence they hold with other groups?
    a. From their perspective: identify the perceived chances of achieving their goals (look at short term and larger goals).
    b. From society's perspective: identify their level of support (polls, media, political/economical).
        i. What is the perceived cyber and environmental security role of the group in the larger group/culture?

5.3.2 Redefining the cyber threat: back to the three perspectives

In addressing objective 5—interpret and extrapolate results to validate the feasibility of CSAs to integrate the protection of national cyber-physical energy systems (CPES) into their mandate (the ends)—analyzing the multitude of perspectives makes is easy to lose focus and get overwhelmed. It is easier, then, to rearrange these into three perspectives, previously addressed: sovereignty, resilience and robustness. Cyber threats to CSA CEI can come from sabotage and terrorist attacks or political/technology embargoes (the sovereignty perspective), extreme natural events or energy infrastructure failures (the robustness perspective), and unexpected regulatory/technology changes or natural events (the resilience perspective)—see figure 21. These cyber threats affect a multitude of infrastructures and stakeholders in different ways. Within the Sovereignty, Resilience, and Robustness perspectives there are a multitude of groups, many with conflicting interests and priorities (as seen in 5.3.1); meaning that no two CSAs are affected by cyber security threats to CEI in the same way. Lack of clear understanding of who these groups are at the regional geo-energy levels, means that while risk minimization "in cyber security is

undoubtedly occurring in the energy sector, [...] this appears to be mostly ad hoc and not the product of specific coordinated and focussed objectives" (Healey et al. 2016, 8). As a result, cyber security efforts within the energy sector often fail to fully achieve their intended objectives.



Source: Adapted from (Cherp and Jewell 2011/9)
Figure 21. Cyber Connected Threats to CEI and Mitigation Strategies based on Cherp & Jewell's three perspectives on energy security.

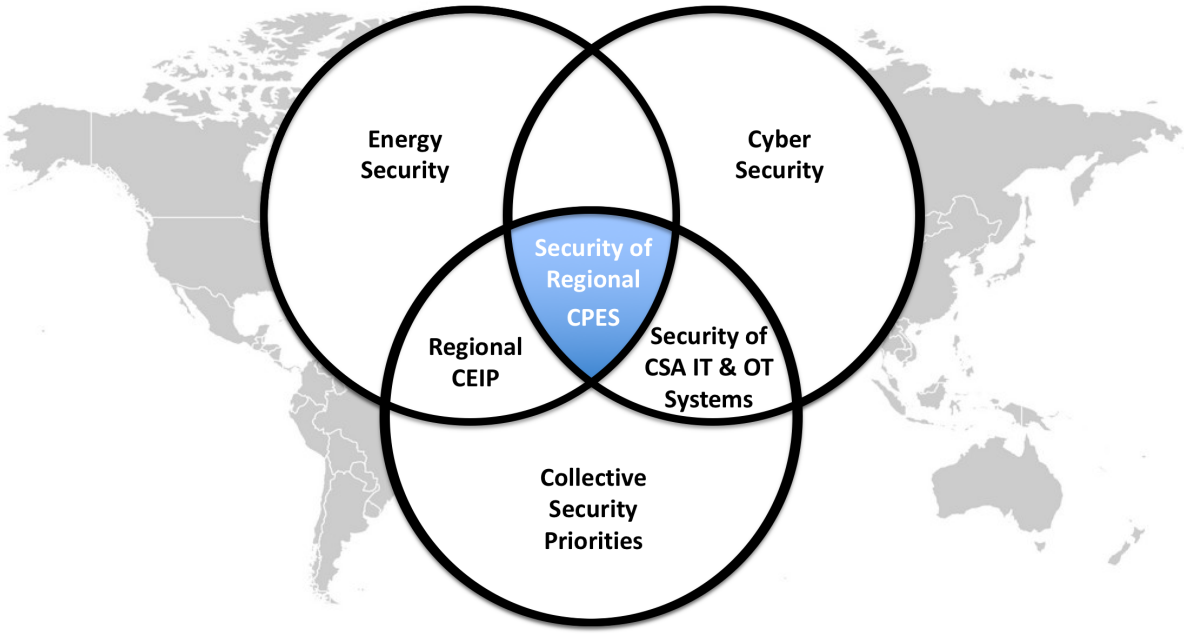
In the cyber domain, not all risks and responses discussed by Cherp and Jewell apply. Nevertheless, the risk minimization and/or response categories fit well in the GCI's categories used in the proposed framework. For example, environmental considerations fit well under 'adopting safer technologies' category and corelates with 'best practices' category of the GCI. On this note,

it needs to be emphasized that information sharing needs to be added within this three perspectives framework; especially if cyber threats to energy security are addressed at the regional/supra-national level. Information sharing and collaboration is also an element that has been identified where most NATO member states could do better at; and will determine the effectiveness of future CSA cyber security policies.

Chapter 6

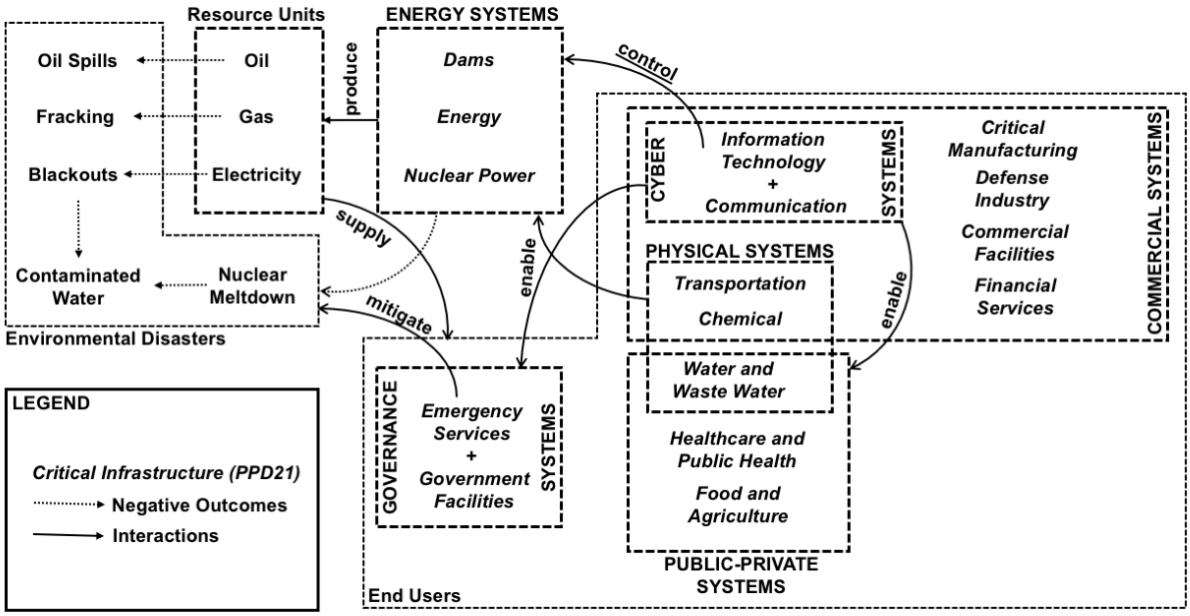
Conclusions

The CSAs of the 21st Century have been challenging the centrality of states in the anarchical nature of the international system. These alliances are emerging as polycentric governance systems "with various parts fostering complementary approaches necessary for addressing the highly interlinked energy challenges" (Cherp, Jewell, and Goldthau 2011, 75) at the advent of cyber-physical risks (Herd and Kriendler 2013). Within these alliances, the definitions of energy and cyber security are shaped today more by "how countries manage their relations with one another, whether bilaterally or within multilateral frameworks" (Yergin 2006, 82) than by domestic and/or global cyber-physical policy decisions. This synthesizes how energy security and cyber security are perceived by CSAs in the contemporary security environment; which was the first objective of this research paper. Since most energy cyber-physical threats "travel more easily over short distances than over long ones," (Buzan and Wæver 2003, 4) one can observe the emergence of geo-energy spaces "where a precise set of energy relationships take place, among different agents—producer states, enterprises and consumer governments—who are active within it," (Mañé-Estrada 2006, 3785) and where a nexus of regional (rather than domestic and/or global) energy and cyber security strategies act as a more efficient driver CSA CPES security. Here, it is necessary to highlight the increased collaboration between NATO and the EU under the Technical Arrangement on Cyber Defence, which was signed in 2016; as well as the availability of NATO Cyber Rapid Reaction teams to conduct defensive cyber operations and protect domestic CEI of NATO member states. This empirically validates the means and ways of CSAs in complementing domestic CEIP efforts in the cyber domain (objective 4).



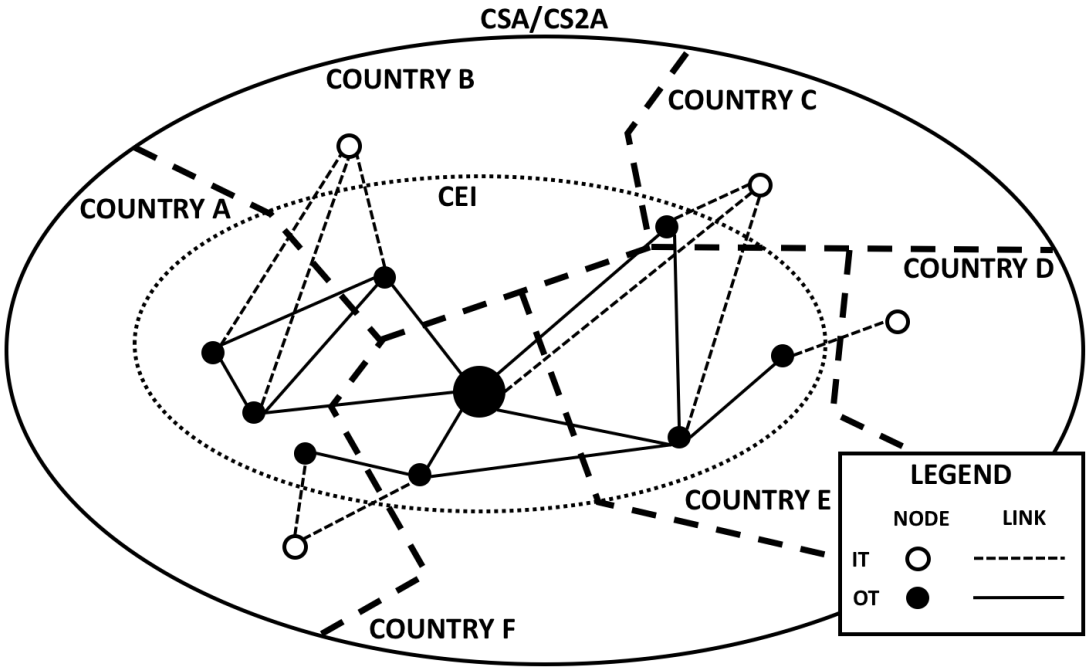
Source: Author's own representation.
Figure 22: The nexus between energy security, cyber security, and collective security priorities and the role of CSAs in securing regional Cyber Physical Energy Systems (CPES).

The cyber threat against CEI extends beyond threats to fuels and renewables production and distribution. Data collection from the application of the proposed framework (which was objective 3) showed that in order to better understand the wider impact of cyber security against CEI, it is important to look at multiple areas and interactions. Some of these are covered, for example, by the US Presidential Policy Directive 21 (critical infrastructure security and resilience), or PPD-21, which was released in 2013. The document highlights that governance systems are responsible "for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions" and must take all necessary steps to strengthen the resilience, robustness, and security of critical infrastructure against both cyber and physical threats (Presidential Policy Directive 21 2013). As indicated by the 30 CEPS experts interviewed, national assessments require a clear understanding of cyber physical energy systems and their interactions (figure 23). This consideration also implies that the proposed framework (objective 2) should expand beyond CSAs prioritizing just threats to geo-energy systems.



Source: Author's representation of PPD21 Critical Infrastructure Areas and Interactions.
Figure 23. Industrial Control Systems as Potential Vulnerabilities of Energy Systems.

At the regional level, the CEPS case highlighted that the links between the critical infrastructures listed above must be considered "in various contexts and under different circumstances" (Joensson 2010, 18), including across borders (figure 24). This validates not only that CSAs must integrate the protection of national-level CPES into their mandate, but also that a broader approach must be taken to complement the domestic protection critical infrastructures in general.



Source: Author's representation.
Figure 24. Simplified model of Critical Energy Infrastructure (CEI) with convergence of IT' & OT systems across borders, within the context of a Collective (Cyber) Security Alliance.

Almost all aspects of society (across borders) could be impacted by failure of critical energy infrastructure. From an environmental perspective, an oil spill in Belgium caused by a cyber-attack against the NATO CEPS infrastructure that originated from Germany could also lead to contaminated water in The Netherlands. It could also cause major economic losses if Amsterdam civilian airport fails to receive its jet fuel on time. Costs of response could skyrocket, depending on the time to recover and clean the spill. Finally, entire systems could be left at the mercy of attackers if a ransomware attack locks production, distribution, and refinery chains out of their systems. Replacing CEPS systems can be expensive, and host nations resources are very limited, so prioritizing responses across borders based on likelihood and potential of damage is critical. Understanding how CSA stakeholders are impacted by these threats is thus important in prioritizing responses (as discussed in chapter 5).

One of the realizations of most CEPS host nations in response to cyber threats from nation states is the need for more collaboration and information sharing among the host nations. At the

NATO level, this could be done through the "cyber-security center in Mons Belgium" (Efthymiopoulos 2019). This collaboration is needed for defending NATO critical infrastructures (such as CEPS) in Europe. CSA solutions must also go beyond panacea solutions and must also include environmental considerations (as exemplified in the proposed CARVER methodology).

As seen with the CEPS case, Cyber security of CEI at regional levels would be influenced not only by national and systemic networks of influence—"and their capacity to mobilize the resources" (Schmeer 1999), that is, what means do they have? What means are they willing to use? Can they ensure that 1) no member state is vulnerable to external influences threatening the CSA cyber security strategy; 2) energy infrastructure is secure from cyber-attack; 3) energy LOCs are open and secure from cyber-attacks; 4) crisis cyber response centers/offensive cyber capabilities are trained and ready?—but also by regional situations and technological capabilities supporting the regional cyber resilience during smart and sustainable low-carbon energy transitions; all of which are considered in a multitier stakeholder analysis approach (Chevalier 2001; R. Freeman and Gilbert 1987). This approach is both flexible and context-specific helping to "focus attention on specific problems, actors and opportunities for change" (Chevalier 2001) during the smart and sustainable low-carbon energy transitions, which is needed to gain a better understanding of energy and cyber security for CSAs.

Bibliography

Abrams, Marshall, and Joe Weiss. 2008. "Malicious Control System Cyber Security Attack Case Study--Maroochy Water Services, Australia." *McLean, VA: The MITRE Corporation*. https://www.acsac.org/2008/program/case-studies/Abrams.pdf.

Adler, Emanuel, Michael Barnett, and Steve Smith. 1998. *Security Communities*. Cambridge University Press.

Alagappa, Muthiah. 1998. "Regional Arrangements, the UN, and International Security: A Framework for Analysis." In *Beyond UN Subcontracting: Task-Sharing with Regional Security Arrangements and Service-Providing NGOs*, edited by Thomas G. Weiss, 3–29. London: Palgrave Macmillan UK.

Alderson, Duncan, and Robert Di Pietro. 2016. "Operational Technology: Are You Vulnerable?" *Governance Directions* 68 (6): 339–43.

Anantharaman, Prashant, J. Peter Brady, Patrick Flathers, Vijay H. Kothari, Michael C. Millian, Jason Reeves, Nathan Reitinger, William G. Nisen, and Sean W. Smith. 2018. "Going Dark: A Retrospective on the North American Blackout of 2038." In *Proceedings of the New Security Paradigms Workshop*, 52–63. NSPW '18. New York, NY, USA: ACM.

Anderson, Irvine H. 1975. "The 1941 De Facto Embargo on Oil to Japan: A Bureaucratic Reflex." *Pacific Historical Review* 44 (2): 201–31.

Andersson, G., P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, et al. 2005. "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance." *IEEE Transactions on Power Systems* 20 (4): 1922–28.

Andreeva, Oxana, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova, Evgeniya Potseluevskaya, Sergey I. Sidorov, and Alexander A. Timorin. 2016. "Industrial Control Systems Vulnerabilities Statistics." Kaspersky Security Intelligence Service. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/07/07190426/KL_REPORT_ICS_Statistic_vulnerabilities.pdf.

Andress, Jason, and Steve Winterfeld. 2013. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Elsevier.

Annan, Kofi. 1999. "The Meaning of International Community." In *Address to the 52nd DPI/NGO Conference, UN Doc. SG/SM/7133*. Vol. 15.

Atsumi, Masahiro. 2007. "Japanese Energy Security Revisited." *Asia-Pacific Review* 14 (1): 28–43.

Bagdonas, Gintaras. 2016. "Energy Security: Operational Highlights." 10. ENSEC COE.

https://www.enseccoe.org/data/public/uploads/2017/02/no-10_20160410.pdf.

———. 2017. "NATO Energy Security Centre of Excellence." presented at the Brief to the U.S. Ambassador to Lithuania, Vilnius, Lithuania.

Baldwin, David A. 1997. "The Concept of Security." *Kokusaigaku Revyu = Obirin Review of International Studies* 23 (1): 5–26.

Balitskiy, Sergey, Yuriy Bilan, and Wadim Strielkowski. 2014. "Energy Security and Economic Growth in the European Union." *Journal of Security & Sustainability Issues* 4 (2). http://www.lka.lt/download/24241/journal%20of%20security%20and%20sustainability%20issues%20nr4_%202_2.pdf.

Bambawale, Malavika Jain, and Benjamin K. Sovacool. 2011/5. "China's Energy Security: The Perspective of Energy Users." *Applied Energy* 88 (5): 1949–56.

Barabasi, Albert-Laszlo. 2010. *Bursts: The Hidden Patterns Behind Everything We Do, from Your E-Mail to Bloody Crusades*. Penguin.

Barnett, Michael, and Martha Finnemore. 2004. *Rules for the World: International Organizations in Global Politics*. Cornell University Press.

Beck, Ulrich. 2006. "Living in the World Risk Society: A Hobhouse Memorial Public Lecture given on Wednesday 15 February 2006 at the London School of Economics." *Economy and Society* 35 (3): 329–45.

Belgian Pipeline Organisation. 2019. "Belgium-Louvain: Pipeline-Inspection Services 2019/S 067-157425." Contract Notice (Services). Services - 157425-2019. https://ted.europa.eu/TED/notice/udl?uri=TED:NOTICE:157425-2019:TEXT:EN:HTML&tabId=2.

Ben Khelil, Haykel, Leila Othmani, and Neji Bouslama. 2015. "Modeling the Role of Consumer Happiness on Online Buying Intention." *Leila and Bouslama, Neji*. https://doi.org/10.2139/ssrn.2615480.

Bennett, Andrew, and Joseph Lepgold. 1993. "Reinventing Collective Security after the Cold War and Gulf Conflict." *Political Science Quarterly* 108 (2): 213–37.

Bentley, R. W. 2002. "Global Oil & Gas Depletion: An Overview." *Energy Policy* 30 (3): 189–205.

Bettel, Xavier. 2018. "National Cybersecurity Strategy III." Luxembourg Government Council.

Biberacher, M., R. De Miglio, M. Gargiulo, R. Gerboni, E. Lavagno, L. Schranz, and G. C. Tosato. 2011. "Risk of Energy Availability Common Corridors for Europe Supply Security—summary Report, REACCESS Final Workshop, Brussels, 13 May 2011."

Bijleveld-Schouten, A. T. B. 2018. "Defence White Paper Investing in Our People, Capabilities and Visibility." The Netherlands Ministry of Defence.

Bodeau, Deb, Jenn Fabius-Greene, and Rich Graubart. 2010. "How Do You Assess Your

Organization's Cyber Threat Level." *The MITRE Corporation, USA*. https://www.researchgate.net/profile/Deb_Bodeau/publication/267861392_How_Do_You_Assess_Your_Organization%27s_Cyber_Threat_Level/links/5588434608ae8c4f34063a62/How-Do-You-Assess-Your-Organizations-Cyber-Threat-Level.pdf.

Boland, Julie. 2011. "Ten Years of the Shanghai Cooperation Organization." *21st Century Defense Initiative*. https://www.brookings.edu/wp-content/uploads/2016/06/06_shanghai_cooperation_organization_boland.pdf.

Bridge, Gavin, Stefan Bouzarovski, Michael Bradshaw, and Nick Eyre. 2013. "Geographies of Energy Transition: Space, Place and the Low-Carbon Economy." *Energy Policy* 53 (February): 331–40.

Broersma, Matthew, ed. 2017. *US Acknowledges Cyber Attack On Nuclear Power Plant*. Silicon UK. https://www.silicon.co.uk/workspace/us-acknowledges-cyber-attack-kansas-nuclear-plant-216891.

Brown, Marc. 2011. "Embedded Device Security in the New Connected Era." *Electronic Engineering Journal*. http://www.mistralsolutions.com/newsletter/Oct13/Device_Security.pdf.

Brugha, R., and Z. Varvasovszky. 2000. "Stakeholder Analysis: A Review." *Health Policy and Planning* 15 (3): 239–46.

Bryant, William D. 2016. "Mission Assurance through Integrated Cyber Defense." *Air & Space Power Journal* 30 (4): 5–18.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17 (2): 212–27.

Bull, Hedley. 2012. *The Anarchical Society: A Study of Order in World Politics*. Macmillan International Higher Education.

Bush, George W. 2002. "The National Security Strategy of the United States of America." Executive Office Of The President Washington DC. https://apps.dtic.mil/docs/citations/ADA406411.

Butrimas, Vytautas. 2018. "NATO ENSEC COE Further Conducts a Cyber Risk Study of Central Europe Pipeline System." NATO ENSEC COE. September 26, 2018. https://enseccoe.org/en/newsroom/nato-ensec-coe-further-conducts-a-cyber-risk-study-of-central-europe-pipeline-system/366.

———. 2019a. "NATO CEPS Cyber Risk Study Continues This Week with a Visit to the Dutch Pipeline Organisation." NATO ENSEC COE. March 27, 2019. https://www.enseccoe.org/en/newsroom/nato-ceps-cyber-risk-study-continues-this-week-with-a-visit-to-the-dutch-pipeline-organisation/407.

———. 2019b. "NATO ENSEC COE Subject Matter Experts' Visit to the Dutch Pipeline Organisation Continues." NATO ENSEC COE. April 3, 2019. https://www.enseccoe.org/en/newsroom/nato-ensec-coe-subject-matter-experts-visit-to-the-dutch-pipeline-organisation-continues/410.

Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations*. Wheatsheaf Books.

Buzan, Barry, and Ole Wæver. 2003. *Regions and Powers: The Structure of International Security*. Cambridge University Press.

Byres, Eric J., and P. Eng. 2009. "Cyber Security and the Pipeline Control System." *Pipeline & Gas Journal*, February. https://www.tofinosecurity.com/sites/default/files/Cyber_Security_and_The_Pipeline_PGJ_Feb_2009.pdf.

Carayannis, E., and J. Alexander. 2006. *Global and Local Knowledge: Glocal Transatlantic Public-Private Partnerships for Research and Technological Development*. Springer.

Carayannis, E. G., D. F. Campbell, and M. P. Efthymiopoulos. 2014. *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory, Policy and Practice*. Edited by Elias G. Carayannis, David F. J. Campbell, and Marios Panagiotis Efthymiopoulos. Springer.

Carayannis, E. G., E. Grigoroudis, D. F. J. Campbell, Dirk Meissner, and Dimitra Stamati. 2018. "The Ecosystem as Helix: An Exploratory Theory-building Study of Regional Co-opetitive Entrepreneurial Ecosystems as Quadruple/Quintuple Helix Innovation Models." *R&D Management* 48 (1). https://onlinelibrary.wiley.com/doi/abs/10.1111/radm.12300.

Carayannis, E. G., E. Grigoroudis, S. S. Rehman, and N. Samarakoon. 2019. "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience." *IEEE Transactions on Engineering Management*, 1–12.

Carayannis, Elias G. 2015-2018. "GW Lecture Notes." The George Washington University: Washington, DC.

———. 1999. "Fostering Synergies between Information Technology and Managerial and Organizational Cognition: The Role of Knowledge Management." *Technovation* 19 (4): 219–31.

———. 2008. "Knowledge-Driven Creative Destruction, or Leveraging Knowledge for Competitive Advantage: Strategic Knowledge Arbitrage and Serendipity as Real Options Drivers Triggered by Co-Opetition, Co-Evolution and Co-Specialization." *Industry and Higher Education* 22 (6): 343–53.

———. 2011. "The Open Innovation Paradigm and Strategic Options for EU-U.S. Innovation

Partnerships. The FREIE Concept in the Context of Open Innovation Diplomacy." presented at the BILAT 2011, Vienna, Austria, March. http://archive.euussciencetechnology.eu/uploads/docs/CARAYANNIS_BILAT_2011_final%20(2).pdf.

Carayannis, Elias G., Thorsten D. Barth, and David F. J. Campbell. 2012. "The Quintuple Helix Innovation Model: Global Warming as a Challenge and Driver for Innovation." *Journal of Innovation and Entrepreneurship* 1 (1): 2.

Carayannis, Elias G., and David F. J. Campbell. 2009. "'Mode 3'and'Quadruple Helix': Toward a 21st Century Fractal Innovation Ecosystem." *International Journal of Technology Management = Journal International de La Gestion Technologique* 46 (3-4): 201–34.

———. 2010. "Triple Helix, Quadruple Helix and Quintuple Helix and How Do Knowledge, Innovation and the Environment Relate to Each Other?: A Proposed Framework for a Trans-Disciplinary Analysis of Sustainable Development and Social Ecology." *International Journal of Social Ecology and Sustainable Development (IJSESD)* 1 (1): 41–69.

Carayannis, Elias G., Aris Kaloudis, and Age Mariussen. 2008. *Diversity in the Knowledge Economy and Society: Heterogeneity, Innovation and Entrepreneurship*. Edward Elgar Publishing.

Carayannis, Elias G., and Ruslan Rakhmatullin. 2014. "The Quadruple/Quintuple Innovation Helixes and Smart Specialisation Strategies for Sustainable and Inclusive Growth in Europe and Beyond." *Journal of the Knowledge Economy* 5 (2): 212–39.

Carayannis, Elias G., Elpida T. Samara, and Yannis L. Bakouros. 2015. *Innovation and Entrepreneurship: Theory, Policy and Practice*. Springer, Cham.

Carpenter, Ted Galen. 1997. "The Mirage of Global Collective Security." *Delusions of Grandeur: The United Nations and Global Intervention, Ed. Ted Galen Carpenter. Washington: Cato Institute.*

CERT. 2019. "Belgian Centre for Cyber Security." CCS. 2019. https://www.ccb.belgium.be/en.

Chang, Youngho, and Swee Lean Collin Koh. 2012. "Rethinking Market Governance and Energy Security." In *Energy and Non-Traditional Security (NTS) in Asia*, edited by Mely Caballero-Anthony, Youngho Chang, and Nur Azha Putra, 13–30. Berlin, Heidelberg: Springer Berlin Heidelberg.

Cheema, P. I. 2011. "Pakistan as an Energy Corridor for Iran and Central Asia: The EU's Interests." *Journal of European Studies*. http://search.proquest.com/openview/c2ad38a52611f029fbcf06da53b41ab3/1?pq-origsite=gscholar&cbl=616525.

Cheng, Han, I. Ferguson, T. Guan, T. Johnson, Y. Ma, Z. Mao, and Others. 2013. "Energy Governance Outlook: Global Scenarios and Implications." *Global Public Policy Institute (GPPi)*.

Chen, Wei-Ming, Hana Kim, and Hideka Yamaguchi. 2014. "Renewable Energy in Eastern Asia:

Renewable Energy Policy Review and Comparative SWOT Analysis for Promoting Renewable Energy in Japan, South Korea, and Taiwan." *Energy Policy* 74 (November): 319–29.

Cherp, Aleh, Adeola Adenikinju, Andreas Goldthau, Larry Hughes, J. Jansen, Jessica Jewell, Marina Olshanskaya, R. Soares de Oliveira, B. Sovacool, and Sergey Vakulenko. 2012. "Energy and Security." http://pure.iiasa.ac.at/id/eprint/10062/1/GEA%20Chapter%205%20Energy%20and%20Security.pdf.

Cherp, Aleh, and Jessica Jewell. 2011/9. "The Three Perspectives on Energy Security: Intellectual History, Disciplinary Roots and the Potential for Integration." *Current Opinion in Environmental Sustainability* 3 (4): 202–12.

———. 2013. "Energy Security Assessment Framework and Three Case Studies." In *International Handbook of Energy Security*, edited by Hugh Dyer and Maria J. Trombetta, 146–73. Northhampton, MA: Edward Elgar Publishing.

———. 2014. "The Concept of Energy Security: Beyond the Four As." *Energy Policy* 75 (December): 415–21.

Cherp, Aleh, Jessica Jewell, and Andreas Goldthau. 2011. "Governing Global Energy: Systems, Transitions, Complexity." *Global Policy* 2 (1): 75–88.

Chester, Lynne. 2010/2. "Conceptualising Energy Security and Making Explicit Its Polysemic Nature." *Energy Policy* 38 (2): 887–95.

Chevalier, Jaques M. 2001. "Stakeholder Analysis and Natural Resource Management." https://vtechworks.lib.vt.edu/handle/10919/66508.

Chi, Sung-Do, Jong Sou Park, Ki-Chan Jung, and Jang-Se Lee. 2001. "Network Security Modeling and Cyber Attack Simulation Methodology." In *Information Security and Privacy*, 320–33. Springer Berlin Heidelberg.

Chuang, Ming-Tung, Shih-Yu Chang, Ta-Chih Hsiao, Yun-Ru Lu, and Tsung-Yeh Yang. 2019. "Analyzing Major Renewable Energy Sources and Power Stability in Taiwan by 2030." *Energy Policy* 125 (February): 293–306.

CISA. 2018. "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." Alert (TA18-074A). Department of Homeland Security. https://www.us-cert.gov/ncas/alerts/TA18-074A.

Ciută, Felix. 2010. "Conceptual Notes on Energy Security: Total or Banal Security?" *Security Dialogue* 41 (2): 123–44.

Claude, Inis L. 1971. *Swords into Plowshares: The Problems and Progress of International Organization*. Random House.

———. 1975. "Comment on' An Autopsy of Collective Security."' *Political Science Quarterly* 90 (4): 715–17.

Climent, Francisco, and Angel Pardo. 2007/1. "Decoupling Factors on the Energy–output Linkage: The Spanish Case." *Energy Policy* 35 (1): 522–28.

Colesniuc, Dan. 2013. "Cyberspace and Critical Information Infrastructures." *Informatica Economica* 17 (4). http://www.revistaie.ase.ro/content/68/11%20-%20Colesniuc.pdf.

Congressional Research Service. 2018. "Electric Grid Cybersecurity." R45312. Congressional Research Service.

———. 2019. "Pipeline Security: Homeland Security Issues in the 116th Congress." IN11060.

Cook, Allan, Richard Smith, Leandros Maglaras, and Helge Janicke. 2016. "Measuring the Risk of Cyber Attack in Industrial Control Systems." In . BCS eWiC. https://www.dora.dmu.ac.uk/handle/2086/13839.

Council for Excellence in Government. 2006. "Public Readiness Index." Council for Excellence in Government.

Crane, Keith, Andreas Goldthau, Michael Toman, Thomas Light, and Stuart E. Johnson. 2009. *Imported Oil and U.S. National Security*. Rand Corporation.

Czosseck, C., and K. Ziolkowski. 2013. "State Actors and Their Proxies in Cyberspace." *Peacetime Regime for State Activities in*. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.645.1982&rep=rep1&type=pdf#page=36.

Daniel, S. L., M. G. Lauby, and G. Maillant. 1989. "Multiarea Transfer Capability: Is a Methodology Needed?" *IEEE Computer Applications in Power* 2 (4): 18–21.

Deane, J. P., Francesco Gracceva, Alessandro Chiodi, Maurizio Gargiulo, and Brian P. Ó. Gallachóir. 2015. "Assessing Power System Security. A Framework and a Multi Model Approach." *International Journal of Electrical Power & Energy Systems* 73 (December): 283–97.

Deng, Francis M., Sadikiel Kimaro, Terrence Lyons, Donald Rothchild, and I. William Zartman. 2010. *Sovereignty as Responsibility: Conflict Management in Africa*. Brookings Institution Press.

Diehl, Paul F., and Joseph Lepgold. 2003. "Regional Conflict Management: Strategies, Necessary Conditions, and Comparative Effectiveness." *Regional Conflict Management*, 41–77.

Donde, Vaibhav Deepak, and Jean-Charles Albert Tournier. 2016. Centralized control center for electrical network computational services. USPTO 9396504. *US Patent*, filed April 18, 2012, and issued July 19, 2016. https://patentimages.storage.googleapis.com/9c/bf/a0/811f0bcc6ba0f7/US9396504.pdf.

Donnelly, Jack. 2000. *Realism and International Relations*. Cambridge University Press.

Donnini, Frank P. 2003. "Ploesti: The Great Ground-Air Battle of 1 August 1943." *Air & Space*

Power Journal 17 (2): 110.

Downs, Erica S. 2004. "The Chinese Energy Security Debate." *The China Quarterly*, no. 177: 21–41.

Downs, George W. 1994. "Beyond the Debate on Collective Security." *Collective Security Beyond the Cold War*, 1–13.

Dunn Cavelty, Myriam, and Victor Mauer. 2009. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence." *Security Dialogue* 40 (2): 123–44.

Efthymiopoulos, Marios Panagiotis. 2014. "NATO's Cyber-Defence: A Methodology for Smart Defence." In *Cyber-Development, Cyber-Democracy and Cyber-Defense*, 303–17. Springer.

———. 2019. "A Cyber-Security Framework for Development, Defense and Innovation at NATO." *Journal of Innovation and Entrepreneurship* 8 (1): 12.

Elam, Carolyn C., Catherine E. Gregoire Padró, Gary Sandrock, Andreas Luzzi, Peter Lindblad, and Elisabet Fjermestad Hagen. 2003. "Realizing the Hydrogen Future: The International Energy Agency's Efforts to Advance Hydrogen Energy Technologies." *International Journal of Hydrogen Energy* 28 (6): 601–7.

Encke, Florian. 2015. "Energy Security and Energy Policy. A View from NATO." presented at the NATO Energy Security Strategic Awareness Course, Oberammergau, Germany, March 17. http://www.niss.gov.ua/public/File/2016_table/5_Enke-NATOs%20Role%20in%20Energy%20Security%20and%20Ukraine.pdf.

Endsley, Mica R. 2016. *Designing for Situation Awareness: An Approach to User-Centered Design*. CRC press.

Erker, Susanna, Rosemarie Stangl, and Gernot Stoeglehner. 2017. "Resilience in the Light of Energy Crises--Part I: A Framework to Conceptualise Regional Energy Resilience." *Journal of Cleaner Production* 164: 420–33.

Etzioni, Amitai. 2008. *Security First: For a Muscular, Moral Foreign Policy*. Yale University Press.

EUROSTAT. 2017. "Energy Balance Flow Sankey Diagram." https://ec.europa.eu/eurostat/cache/sankey/sankey.html.

Evans, Nathaniel, and William Horsthemke. 2019. "Regional Critical Infrastructure." In *Cyber Resilience of Systems and Networks*, edited by Alexander Kott and Igor Linkov, 355–80. Cham: Springer International Publishing.

Fägersten, Björn. 2015. "Intelligence and Decision-Making within the Common Foreign and Security Policy." *European Policy Analysis. Swedish Institute of European Security Studies*. http://www.academia.edu/download/38978720/Fagersten_EPA_2015_eng.pdf.

Farer, Tom J. 1993. "The Role of Regional Collective Security Arrangements." *Collective Security in a Changing World* 153: 167.

Farrell, Alexander E., Hisham Zerriffi, and Hadi Dowlatabadi. 2004. "ENERGY INFRASTRUCTURE AND SECURITY." *Annual Review of Environment and Resources* 29 (1): 421–69.

Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (1): 23–40.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917.

Firdous, Afeera. 2018. "Formulation of Pakistan's Cyber Security Policy." *CISS Insight Journal* 6 (1): 70–94.

Fischhendler, Itay, and Daniel Nathan. 2014. "In the Name of Energy Security: The Struggle over the Exportation of Israeli Natural Gas." *Energy Policy* 70 (July): 152–62.

Flamant, Renaud, and Pieter-Jan Parrein. 2017. "The Strategic Vision for Defence." D-2017/9376/1. Belgian Ministry of Defence.

Fletcher, Max E. 1975. "From Coal to Oil in British Shipping." *The Journal of Transport History* ss-3 (1): 1–19.

Frederking, Brian. 2003. "Constructing Post-Cold War Collective Security." *The American Political Science Review* 97 (3): 363–78.

Freeman, R. E. 2010. *Strategic Management: A Stakeholder Approach*. Cambridge University Press.

Freeman, R., and D. Gilbert. 1987. "Managing Stakeholder Relations." In *Business and Society: Dimensions of Conflict and Cooperation*, edited by S. Prakash and C. Falbe. Toronto, Canada: Lexington Books.

Frondel, Manuel, Nolan Ritter, Christoph M. Schmidt, and Colin Vance. 2010. "Economic Impacts from the Promotion of Renewable Energy Technologies: The German Experience." *Energy Policy* 38 (8): 4048–56.

Gallarotti, Giulio M. 1991. "The Limits of International Organization: Systematic Failure in the Management of International Relations." *International Organization* 45 (2): 183–220.

Garimella, P. K. 2018. "IT-OT Integration Challenges in Utilities." *2018 IEEE 3rd International Conference on*. https://ieeexplore.ieee.org/abstract/document/8586807/.

Garrett, Russell K. 1993. "Is a Single Fuel on the Battlefield Still a Viable Option?" 94-07540. National Defense University. https://apps.dtic.mil/docs/citations/ADA276757.

Garvin, Thomas, and Others. 2015. "IT and OT Convergence, or Collision? Managing the Merger for Greenfield LNG." In *Abu Dhabi International Petroleum Exhibition and Conference*. Society of Petroleum Engineers. https://www.onepetro.org/conference-paper/SPE-177443-MS.

Geels, Frank W. 2014. "Regime Resistance against Low-Carbon Transitions: Introducing Politics

and Power into the Multi-Level Perspective." *Theory, Culture & Society* 31 (5): 21–40.

Geers, Kenneth. 2010. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26 (3): 298–303.

Gheorghe, Adrian V., and Liviu Muresan. 2011. *Energy Security: International and Local Issues, Theoretical Perspectives, and Critical Energy Infrastructures*. Springer Science & Business Media.

Gleason, G., and M. E. Shaihutdinov. 2005. "Collective Security and Non-State Actors in Eurasia." *International Studies Perspectives* 5: 274–84.

Gnansounou, Edgard. 2008. "Assessing the Energy Vulnerability: Case of Industrialised Countries." *Energy Policy* 36 (10): 3734–44.

Goldthau, Andreas, and Benjamin K. Sovacool. 2012. "The Uniqueness of the Energy Security, Justice, and Governance Problem." *Energy Policy* 41 (February): 232–40.

Goldthau, Andreas, and Jan Martin Witte. 2010. *Global Energy Governance: The New Rules of the Game*. Brookings Institution Press.

Good, Robert C. 1962. "State-Building as a Determinant of Foreign Policy in the New States." *Neutralism and Nonalignment*, 3–12.

Gordenker, Leon, and Thomas G. Weiss. 1993. "The Collective Security Idea and Changing World Politics." *Collective Security in a Changing World*, 3–18.

Government Accountability Office. 2018. "Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management." GAO-19-48. https://www.gao.gov/assets/700/696123.pdf.

Gracceva, Francesco, and Peter Zeniewski. 2014. "A Systemic Approach to Assessing Energy Security in a Low-Carbon EU Energy System." *Applied Energy* 123 (June): 335–48.

Greaver, Bradley, Leo Raabe, William P. Fox, and Robert E. Burks. 2018. "CARVER 2.0: Integrating the Analytical Hierarchy Process's Multi-Attribute Decision-Making Weighting Scheme for a Center of Gravity Vulnerability Analysis for US Special Operations Forces." *The Journal of Defense Modeling and Simulation* 15 (1): 111–20.

Grubliauskas, Julijus, and Michael Rühle. 2018. "Energy Security: A Critical Concern for Allies and Partners." NATO Official Page. July 26, 2018. https://www.nato.int/docu/review/2018/Also-in-2018/energy-security-a-critical-concern-for-allies-and-partners/EN/index.htm.

Haas, Ernst B. 1968. *Collective Security and the Future International System*. University of Denver.

Haghighi, Sanam S. 2008. "Energy Security and the Division of Competences between the European Community and Its Member States." *European Law Journal* 14 (4): 461–82.

Hansen, Lene, and Helen Nissenbaum. 2009. "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly: A Publication of the International Studies*

Association 53 (4): 1155–75.

Healey, David, Sacha Meckler, Usen Antia, and Edward Cottle. 2016. *Cyber Security Strategy for the Energy Sector*. http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf.

He, Fan, and Donghai Qin. 2006. "China's Energy Strategy in the Twenty-First Century." *China & World Economy* 14 (2): 93–104.

Heinl, Caitriona H. 2013. "Enhancing ASEAN-Wide Cybersecurity: Time for a Hub of Excellence?" https://dr.ntu.edu.sg/handle/10220/20101.

Herd, Graeme P., and John Kriendler. 2013. *Understanding NATO in the 21st Century: Alliance Strategies, Security and Global Governance*. Routledge.

Hernández, Félix, Miguel Ángel Gual, Pablo Del Río, and Alejandro Caparrós. 2004/2. "Energy Sustainability and Global Warming in Spain." *Energy Policy* 32 (3): 383–94.

HLR. 1989. "Realism, Liberalism, and the War Powers Resolution. Note." *Harvard Law Review* 102: 637.

Hochman, J. Å. 1982. "The Soviet Union and the Failure of Collective Security (1934-1938): A Study in Shared Responsibility." https://etd.ohiolink.edu/!etd.send_file?accession=osu1487174863875751&disposition=inline.

Hogan, Willard N. 2015. *International Conflict and Collective Security*. University Press of Kentucky.

Holsti, Ole R., P. Terrence Hopmann, and John D. Sullivan. 1973. *Unity and Disintegration in International Alliances: Comparative Studies*. John Wiley & Sons.

Hook, Steven W., and Richard Robyn. 1999. "Regional Collective Security in Europe: Past Patterns and Future Prospects." *European Security* 8 (3): 82–100.

Hoven, Jeroen van den, Martijn Blaauw, Wolter Pieters, and Martijn Warnier. 2018. "Privacy and Information Technology." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N. Zalta, Summer 2018. Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/sum2018/entries/it-privacy/.

Huang, Yu-Lun, Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Hsin-Yi Tsai, and Shankar Sastry. 2009. "Understanding the Physical and Economic Consequences of Attacks on Control Systems." *International Journal of Critical Infrastructure Protection* 2 (3): 73–83.

Hubbert, M. King. 1956. "Nuclear Energy and the Fossil Fuel." In *Drilling and Production Practice*. American Petroleum Institute. https://www.onepetro.org/conference-paper/API-56-007.

Hughes, Larry. 2009. "The Four 'R's of Energy Security." *Energy Policy* 37 (6): 2459–61.

Hughes, Michael B. 2017. "Impact of EMP on Air Operations." Air Command and Staff College,

Air University Maxwell AFB United States. https://apps.dtic.mil/dtic/tr/fulltext/u2/1054561.pdf.

Hughes, Rex. 2009. "NATO and Cyber Defence." *Atlantisch Perspectief* 33. https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf.

Hunker, Jeffrey, Bob Hutchinson, and Jonathan Margulies. 2008. "Role and Challenges for Sufficient Cyber-Attack Attribution." *Institute for Information Infrastructure Protection*. http://www.scis.nova.edu/%7Ecannady/ARES/hunker.pdf.

Hurrell, Andrew. 1992. "Collective Security and International Order Revisited." *International Relations* 11 (1): 37–55.

IBM. 2015. "Security Attacks on Industrial Control Systems." IBM Security. https://www.ibm.com/downloads/cas/4PE7DQ3G.

IEA. 2019a. "Country Energy Security." IEA. 2019. https://www.iea.org.

———. 2019b. "Energy Security." IEA Energy Security. 2019. https://www.iea.org/topics/energysecurity/.

Ilic, Marija D., Le Xie, Usman A. Khan, and José M. F. Moura. 2010. "Modeling of Future Cyber--Physical Energy Systems for Distributed Sensing and Control." *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 40 (4): 825–38.

Intharak, Narumon. 2007. "A Quest for Energy Security in the 21st Century." Edited by Alicia A. Aponte. Asia Pacific Energy Research Centre.

ITU. 2019. "Global Cybersecurity Index (GCI)." 978-92-61-28191-5. ITU.

Jewell, Jessica. 2011. "The IEA Model of Short-Term Energy Security (MOSES)." https://www.oecd-ilibrary.org/content/workingpaper/5k9h0wd2ghlv-en.

———. 2013. "Energy Security and Climate Change Mitigation. the Interaction in Long-Term Global Scenarios." *Environmental Sciences and Policy. Central European University*. http://www.etd.ceu.hu/2013/jewell_jessica.pdf.

Jewell, Jessica, Aleh Cherp, and Keywan Riahi. 2014. "Energy Security under de-Carbonization Scenarios: An Assessment Framework and Evaluation under Different Technology and Policy Choices." *Energy Policy* 65 (February): 743–60.

Joensson, Jibecke H. 2010. "Understanding Collective Security in the 21st Century: A Critical Study of UN Peacekeeping in the Former Yugoslavia." diana-n.iue.it. http://diana-n.iue.it:8080/handle/1814/14711.

Johnson, Chris W. 2007. "Analysing the Causes of the Italian and Swiss Blackout, 28th September 2003." In *Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-Related Programmable Systems - Volume 86*, 21–30. SCS '07. Darlinghurst, Australia, Australia: Australian Computer Society, Inc.

Jones, G. Gareth. 1977. "The British Government and the Oil Companies 1912-1924: The Search for an Oil Policy." *The Historical Journal* 20 (3): 647–72.

Jones, Matthew, Chris Hope, and Richard Hughes. 1990. "A Multi-Attribute Value Model for the Study of UK Energy Policy." *The Journal of the Operational Research Society* 41 (10): 919–29.

József, Venekei. 2013. "Role of Bulk Fuel Installations (BFIS) and Field Pipeline Systems in Operational Supply Chain." *HADMÉRNÖK* 8 (3): 30–36.

Kamal, S. Z., S. M. Al Mubarak, B. D. Scodova, P. Naik, P. Flichy, G. Coffin, and Others. 2016. "IT and OT Convergence-Opportunities and Challenges." In *SPE Intelligent Energy International Conference and Exhibition*. Society of Petroleum Engineers. https://www.onepetro.org/conference-paper/SPE-181087-MS.

Karabaich, B. 2004. "Towards a Working Taxonomy of Groups." In *Proceedings of 13th Annual BRIMS Conference*. cc.ist.psu.edu. http://cc.ist.psu.edu/BRIMS/archives/2004/Papers/04-BRIMS-090.pdf.

Kárník, Vit, Zdenˇka Schenkova, and Vladimir Schenk. 1984. "Vulnerability and the MSK Scale." *Engineering Geology* 20 (1): 161–68.

Keohane, Robert O. 1978. "The International Energy Agency: State Influence and Transgovernmental Politics." *International Organization* 32 (4): 929–51.

———. 2006. "Decisiveness and Accountability as Part of a Principled Response to Nonstate Threats." *Ethics & International Affairs* 20 (2): 219–24.

Khamashuridze, Zurab. 2008. "Energy Security and NATO: Any Role for the Alliance?" *Connections* 7 (4): 43–58.

King, Marcus Dubois, and Jay Gulledge. 2013. "The Climate Change and Energy Security Nexus." *The Fletcher Forum of World Affairs* 37: 25.

Koyama, Ken, Ichiro Kutani, and Others. 2012. "Study on the Development of an Energy Security Index and an Assessment of Energy Security for East Asian Countries." *Books*. https://ideas.repec.org/b/era/eriabk/2011-rpr-13.html.

Krasner, Stephen D. 1983. *International Regimes*. Cornell University Press.

Kratochwil, Friedrich V., and Edward D. Mansfield. 1994. *International Organization: A Reader*. Longman Publishing Group.

Kratsios, Michael. 2018. "White House Hosts Summit on Artificial Intelligence for American Industry." *White House Office of Science and Technology Policy* (blog). May 10, 2018. https://www.whitehouse.gov/articles/white-house-hosts-summit-artificial-intelligence-american-industry/.

Kruyt, Bert, D. P. van Vuuren, H. J. M. de Vries, and H. Groenenberg. 2009/6. "Indicators for Energy Security." *Energy Policy* 37 (6): 2166–81.

Kulawiak, Marcin, Zbigniew Lubniewski, Krzysztof Bikonis, and Andrzej Stepnowski. 2009. "Geographical Information System for Analysis of Critical Infrastructures and Their Hazards due to Terrorism, Man-Originated Catastrophes and Natural Disasters for the City of Gdansk." In *Information Fusion and Geographic Information Systems*, 251–62. Springer Berlin Heidelberg.

Kupchan, Charles. 1994. "The Case of Collective Security." *Collective Security Beyond the Cold War*, 42–44.

Kupchan, Charles A., and Clifford A. Kupchan. 1995. "The Promise of Collective Security." *International Security* 20 (1): 52–61.

Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum* 3 (50): 48–53.

Kuzemko, Caroline. 2011. "UK Energy Governance in the Twenty-First Century: Unravelling the Ties That Bind." University of Warwick. https://core.ac.uk/download/pdf/9053636.pdf.

Lacher, Wolfram, and Dennis Kumetat. 2011. "The Security of Energy Infrastructure and Supply in North Africa: Hydrocarbons and Renewable Energies in Comparative Perspective." *Energy Policy* 39 (8): 4466–78.

Lake, David A. 2001. "Beyond Anarchy: The Importance of Security Institutions." *International Security* 26 (1): 129–60.

Langner, R. 2011. "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security & Privacy* 9 (3): 49–51.

Lee, E. A. 2008. "Cyber Physical Systems: Design Challenges." In *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, 363–69. ieeexplore.ieee.org.

Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. "Analysis of the Cyber Attack on the Ukrainian Power Grid." *Electricity Information Sharing and Analysis Center (E-ISAC)*. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Leszczyna, Rafał. 2018. "Standards on Cyber Security Assessment of Smart Grid." *International Journal of Critical Infrastructure Protection* 22 (September): 70–89.

Leung, Guy C. K., Aleh Cherp, Jessica Jewell, and Yi-Ming Wei. 2014. "Securitization of Energy Supply Chains in China." *Applied Energy* 123 (June): 316–26.

Lewis, Ted G., Rudolph P. Darken, Thomas Mackin, and Donald Dudenhoeffer. 2012. "Model-Based Risk Analysis for Critical Infrastructures." *WIT Transactions on State-of-the-Art in Science and Engineering* 54. https://www.witpress.com/elibrary/wit-transactions-on-state-of-the-art-in-science-and-engineering/54/23054.

Liska, George. 1962. *Nations in Alliances: The Limits of Interdependence*. Baltimore: The Johns Hopkins Press.

Löschel, Andreas, Ulf Moslener, and Dirk T. G. Rübbelke. 2010. "Indicators of Energy Security in Industrialised Countries." *Energy Policy* 38 (4): 1665–71.

Luiijf, Eric, Kim Besseling, and Patrick De Graaf. 2013. "Nineteen National Cyber Security Strategies." *International Journal of Critical Infrastructures 6* 9 (1-2): 3–31.

Luiijf, Eric, Albert Nieuwenhuijs, Marieke Klaver, Michel van Eeten, and Edite Cruz. 2009. "Empirical Findings on Critical Infrastructure Dependencies in Europe." In *Critical Information Infrastructure Security*, 302–10. Springer Berlin Heidelberg.

MacArthur, J. M. 1997. "Stakeholder Roles and Stakeholder Analysis in Project Planning"." *A Review of Approaches in Three Agencies--World Bank*.

Macron, Emmanuel. 2017. "Defence and National Security Strategic Review 2017." Government of France.

Mälksoo, Maria. 2018. "Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO." *European Security* 27 (3): 374–92.

Mañé-Estrada, Aurèlia. 2006. "European Energy Security: Towards the Creation of the Geo-Energy Space." *Energy Policy* 34 (18): 3773–86.

Manning, Robert. 2000. *The Asian Energy Factor: Myths and Dilemmas of Energy, Security and the Pacific Future*. Macmillan.

Martin, Lisa L., and Beth A. Simmons. 1998. "Theories and Empirical Studies of International Institutions." *International Organization* 52 (4): 729–57.

Marvin, H. J. P., G. A. Kleter, L. J. Frewer, S. Cope, M. T. A. Wentholt, and G. Rowe. 2009. "A Working Procedure for Identifying Emerging Food Safety Issues at an Early Stage: Implications for European and International Risk Management Practices." *Food Control* 20 (4): 345–56.

Mattli, Walter. 1999. *The Logic of Regional Integration: Europe and beyond*. Cambridge University Press.

McCain, J. 2007. "An Enduring Peace Built on Freedom - Securing America's Future." *Foreign Affairs* 86 (6).

Mearsheimer, John J. 1994. "The False Promise of International Institutions." *International Security* 19 (3): 5–49.

———. 1995. "A Realist Reply." *International Security* 20 (1): 82–93.

Merkel, Angela, and Ursula von der Leyen. 2016. "White Paper on German Security Policy and the Future of the Bundeswehr." Bundeswehr.

Miller, Lynn H. 1999. "The Idea and the Reality of Collective Security." *Global Governance* 5: 303.

Mills, Harry. 2000. *Artful Persuasion: How to Command Attention, Change Minds, and Influence People*. AMACOM Div American Mgmt Assn.

Miron, D., and M. Preda. 2009. "Stakeholder Analysis of the Romanian Energy Sector." *Review of*

International Comparative 10 (5): 877–92.

Mitchell, Ronald K., Bradley R. Agle, and Donna J. Wood. 1997. "Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts." *AMRO* 22 (4): 853–86.

Mix, Derek E. 2011. *The European Union: Foreign and Security Policy*. Vol. 25. Congressional Research Service.

Modelski, George. 1963. "The Study of Alliances: A Review." *The Journal of Conflict Resolution* 7 (4).

Mol, A. P. J. 1995. *The Refinement of Production*. Netherlands: Utrecht : International Books.

Molis, Arūnas, and Tomas Vaišnoras. 2010. "Energy Security through Membership in NATO and the EU: Interests and Achievements of Lithuania." *Electricity Journal* 23 (1): 57.

Møller, Joakim Erma, and Magnus Petersson. 2019. "Sweden, Finland, and the Defence of the Nordic-Baltic Region—Ways of British Leadership." In *The United Kingdom's Defence After Brexit: Britain's Alliances, Coalitions, and Partnerships*, edited by Rob Johnson and Janne Haaland Matlary, 215–43. Cham: Springer International Publishing.

Monaghan, Andrew. 2008. "Energy Security: NATO's Limited, Complementary Role." Research Division-NATO Defense College, Rome. https://www.files.ethz.ch/isn/56022/rp_36en.pdf.

Moore, D., V. Paxson, S. Savage, and C. Shannon. 2003. "Inside the Slammer Worm." *IEEE Security & Privacy*. https://www.computer.org/csdl/mags/sp/2003/04/j4033.pdf.

Morgenthau, Hans J. 1978. *Politics Among Nations: The Struggle for Power and Peace, Revised*. New York: Knoph.

Moteff, John, Claudia Copeland, and John Fischer. 2003. "Critical Infrastructures: What Makes an Infrastructure Critical?" Congressional Research Service Resources, Science, and Industry Division. https://apps.dtic.mil/docs/citations/ADA467306.

Mudrinich, Erik M. 2012. "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem." *The Air Force Law Review* 68: 167.

Murad, Md Wahid, Md Mahmudul Alam, Abu Hanifa Md Noman, and Ilhan Ozturk. 2019. "Dynamics of Technological Innovation, Energy Consumption, Energy Price and Economic Growth in Denmark." *Environmental Progress & Sustainable Energy* 38 (1): 22–29.

Narula, Kapil. 2019. *The Maritime Dimension of Sustainable Energy Security*. Springer.

NATO. 2016. "Joint Declaration by the Heads of State and Government." presented at the Nato Summit, Warsaw, Poland. https://franceintheus.org/spip.php?article668.

———. 2017. "NATO Pipeline System." NATO Official Page. March 9, 2017. https://www.nato.int/cps/en/natohq/topics_56600.htm?selectedLocale=ru.

———. 2018a. "Civil Preparedness." NATO Topics. June 8, 2018.

https://www.nato.int/cps/en/natohq/topics_49158.htm.

———. 2018b. "NATO's Role in Energy Security." NATO Official Page. September 14, 2018. https://www.nato.int/cps/en/natohq/topics_49208.htm.

NATO Heads of State and Government. 1999. "The Alliance's Strategic Concept." NATO Official Page. April 24, 1999. https://www.nato.int/cps/en/natohq/official_texts_27433.htm.

———. 2008. "Bucharest Summit Declaration." NATO Official Page. April 30, 2008. https://www.nato.int/cps/en/natolive/official_texts_8443.htm.

———. 2018. "Brussels Summit Declaration." Official NATO Page. July 11, 2018. https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en.

Nazir, S., and M. Kaleem. 2018. "Random Network Coding for Secure Packet Transmission in SCADA Networks." In *2018 3rd International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*, 1–4. ieeexplore.ieee.org.

Nepal, Rabindra, and Tooraj Jamasb. 2013. "Security of European Electricity Systems: Conceptualizing the Assessment Criteria and Core Indicators." *International Journal of Critical Infrastructure Protection* 6 (3): 182–96.

Newman, Edward, Ramesh Thakur, and J. Tirman. 2006. *Multilateralism Under Challenge: Power, International Order, And Structural Change*. New York, Paris: United Nations University Press.

Nye, Joseph S. 1980. "Energy Nightmares." *Foreign Policy*, no. 40: 132–54.

Olah, George A. 2005. "Beyond Oil and Gas: The Methanol Economy." *Angewandte Chemie* 44 (18): 2636–39.

Olson, Mancur, and Richard Zeckhauser. 1966. "An Economic Theory of Alliances." *The Review of Economics and Statistics* 48 (3): 266–79.

Oneal, John R. 1990. "Testing the Theory of Collective Action: Nato Defense Burdens, 1950-1984." *The Journal of Conflict Resolution* 34 (3): 426–48.

Onyeji, Ijeoma, Morgan Bazilian, and Chris Bronk. 2014. "Cyber Security and Critical Energy Infrastructure." *Electricity Journal* 27 (2): 52–60.

Organski, Abramo F. K. 1958. *World Politics*. Knopf.

Ostrom, Elinor. 2007. "A Diagnostic Approach for Going beyond Panaceas." *Proceedings of the National Academy of Sciences of the United States of America* 104 (39): 15181–87.

O'Sullivan, Meghan L. 2013. "The Entanglement of Energy, Grand Strategy, and International Security." *The Handbook of Global Energy Policy*, 30–47.

Øverland, Indra, Ellen Scholl, Kirsten Westphal, and Katja Yafimava. 2016. "Energy Security and the OSCE: The Case for Energy Risk Mitigation and Connectivity." https://brage.bibsys.no/xmlui/bitstream/handle/11250/2452171/2016+-

+Energy+security+and+the+OSCE+-+SWP+comment.pdf?sequence=1.

Oxenaar, Sem. 2017. "Mapping the Financial and Organizational Interdependencies between the Dutch State and the Fossil Fuel Industry." Humboldt University Berlin. https://www.researchgate.net/profile/Sem_Oxenaar2/publication/323486424_Mapping_the_financial_and_organizational_interdependencies_between_the_Dutch_State_and_the_fossil_fuel_industry/links/5a981550a6fdccecff0c10a3/Mapping-the-financial-and-organizational-interdependencies-between-the-Dutch-State-and-the-fossil-fuel-industry.pdf.

Pamir, Necdet. 2007. "The Black Sea: A Gateway to Energy Security and Diversification." *Southeast European and Black Sea Studies* 7 (2): 245–63.

Paradis, S., A. Benaskeur, M. Oxenham, and P. Cutler. 2005. "Threat Evaluation and Weapons Allocation in Network-Centric Warfare." In *2005 7th International Conference on Information Fusion*, 2:8 pp. – . ieeexplore.ieee.org.

Pearson, Ivan L. G. 2011. "Smart Grid Cyber Security for Europe." *Energy Policy* 39 (9): 5211–18.

Perlroth, Nicole, and Clifford Krauss. 2018. "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try." *The New York Times*, March. https://cyber-peace.org/wp-content/uploads/2018/03/A-Cyberattack-in-Saudi-Arabia-Had-a-Deadly-Goal.-Experts-Fear-Another-Try.-The-New-York-Times.pdf.

Pernik, Piret. 2014. "Improving Cyber Security: NATO and the EU." *International Centre for Defence Studies*. https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf.

Pescaroli, Gianluca, and David Alexander. 2016. "Critical Infrastructure, Panarchies and the Vulnerability Paths of Cascading Disasters." *Natural Hazards* 82 (1): 175–92.

Peters, Katie. 2018. "Disasters, Climate Change, and Securitisation: The United Nations Security Council and the United Kingdom's Security Policy." *Disasters* 42 Suppl 2 (October): S196–214.

Peters, Susanne. 2004. "Coercive Western Energy Security Strategies: 'resource Wars' as a New Threat to Global Security." *Geopolitics* 9 (1): 187–212.

Platts. 2016. "French Refinery, Port Disruption Continues; Tugboat Crews Join Strike." Platts. June 2, 2016. https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/060216-french-refinery-port-disruption-continues-tugboat-crews-join-strike.

Pohl, Phillip Isabio, Shawn P. Burns, Jason Brown, Madison Link, Robert Browitt, Lee Eubanks, and Regina Hunter. 2013. "RAMPART CARVER and Resilience." Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). https://www.osti.gov/servlets/purl/1115970.

Poulsen, K. 2003. "Slammer Worm Crashed Ohio Nuke Plant Net." *The Register of the Kentucky*

Historical Society. http://rbcshield.com/Slammer_worm_crashed_Ohio_nuke_plant_net.pdf.

Presidential Policy Directive 21. 2013. "Critical Infrastructure Security and Resilience. PPD-21, Released February 12, 2013."

PRMPS. 2009. "What Is Stakeholder Analysis?" World Bank.

Pursiainen, Christer. 2009. "The Challenges for European Critical Infrastructure Protection." *Journal of European Integration* 31 (6): 721–39.

Qinhua, Xu. 2007. "China's Energy Diplomacy and Its Implications for Global Energy Security." *Friedrich Ebert Stiftung Briefing Paper:"Dialogue on Globalization", Beijing* 13. http://library.fes.de/pdf-files/iez/global/04763.pdf.

Quade, Edward S. 1972. "Analysis for Public Policy Decisions." https://www.rand.org/pubs/papers/P4863.html.

Ragin, Charles C. 2009. *Redesigning Social Inquiry: Fuzzy Sets and Beyond*. University of Chicago Press.

Raphael, Sam, and Doug Stokes. 2014. "US Oil Strategy in the Caspian Basin: Hegemony through Interdependence." *International Relations* 28 (2): 183–206.

Ravenal, Earl C. 1975. "An Autopsy of Collective Security." *Political Science Quarterly* 90 (4): 697–714.

Raven, R. P. J. M., and G. P. J. Verbong. 2009. "Boundary Crossing Innovations: Case Studies from the Energy Domain." *Technology in Society* 31 (1): 85–93.

Reed, Thomas C. 2005. *At the Abyss: An Insider's History of the Cold War*. Presidio Press.

Rhee, Changyong. 2013. "Asian Development Outlook 2013: Asia's Energy Challenge." Asian Development Bank.

Riley, Michael, Jennifer A. Dlouhy, and Bryan Gruley, eds. 2017. *Russians Are Suspects in Nuclear Site Hackings, Sources Say*. Bloomberg. https://www.bloomberg.com/news/articles/2017-07-07/russians-are-said-to-be-suspects-in-hacks-involving-nuclear-site.

Rinaldi, S. M. 2004. "Modeling and Simulating Critical Infrastructures and Their Interdependencies." In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, 8 pp. – . ieeexplore.ieee.org.

Ringert, Jan O., Bernhard Rumpe, and Andreas Wortmann. 2015. "Transforming Platform-Independent to Platform-Specific Component and Connector Software Architecture Models." *arXiv [cs.SE]*. arXiv. http://arxiv.org/abs/1511.05365.

Roberts, John M. 2006. "The Black Sea and European Energy Security." *Southeast European and Black Sea Studies* 6 (2): 207–23.

Rochester, M. 1995. "The United Nations in a New World Order: Reviving the Theory and Practice of International Organization." In *Controversies in International Relations Theory: Realism and the Neoliberal Challenge*, edited by Charles Kegley. New York: St. Martin's Press.

Roelich, Katy, David A. Dawson, Phil Purnell, Christof Knoeri, Ruairi Revell, Jonathan Busch, and Julia K. Steinberger. 2014. "Assessing the Dynamic Material Criticality of Infrastructure Transitions: A Case of Low Carbon Electricity." *Applied Energy* 123 (June): 378–86.

Roe, Paul. 2012. "Is Securitization a 'Negative'concept? Revisiting the Normative Debate over Normal versus Extraordinary Politics." *Security Dialogue* 43 (3): 249–66.

Rosner, Kevin. 2004. "Critical Energy System Infrastructure Protection in Europe and the Legitimate Economy." In *Business and Security Public-Private Sector Relationships in a New Security Environment*, edited by Alyson J. K. Bailes and Isabel Frommelt, 210–16. Solna, Sweden: Stockholm International Peace Research Institute.

Ruggie, John Gerard. 1996. *Winning the Peace: America and World Order in the New Era*. Columbia University Press.

Rulska, Anna M. 2010. *The Tale of Two Narratives: NATO as a Collective Defense and a Collective Security Institution*. Old Dominion University.

Salem, Ahmed Ali. 2006. "International Relations Theories and International Organizations: Realism, Constructivism, and Collective Security in the League of Arab States." University of Illinois at Urbana-Champaign. https://www.ideals.illinois.edu/handle/2142/82572.

Schmeer, Kammi. 1999. "Stakeholder Analysis Guidelines." *Policy Toolkit for Strengthening Health Sector Reform*, 1–33.

Scholl, Ellen, and Kirsten Westphal. 4/2017. "European Energy Security Reimagined: Mapping the Risks, Challenges and Opportunities of Changing Energy Geographies." Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-51587-3.

Scholl, Ellen, Kirsten Westphal, Katja Yafimava, and Indra Øverland. 2016. "Energy Security and the OSCE: The Case for Energy Risk Mitigation and Connectivity." https://www.ssoar.info/ssoar/handle/document/47127.

Seebruck, Ryan. 2015. "A Typology of Hackers: Classifying Cyber Malfeasance Using a Weighted Arc Circumplex Model." *Digital Investigation* 14 (September): 36–45.

Serrano-Calle, Silvia, and Erik Delarue. 2018. "Smart Technologies Applied to the Energy Sector. Renewable Energy Expansion Strengthened by Digital Communications and Distributed Ledger Technologies?" https://www.econstor.eu/handle/10419/184966.

Shahidehpour, M., Z. Li, and M. Ganji. 2018. "Smart Cities for a Sustainable Urbanization: Illuminating the Need for Establishing Smart Urban Infrastructures." *IEEE Electrification Magazine* 6 (2): 16–33.

Shamasastry, R. 1915. *Kautilya's Arthashastra*. Bangalore: Government Press.

Simon, Jeffrey. 2005. "NATO Expeditionary Operations: Impacts upon New Members and

Partners." National Defense University. https://apps.dtic.mil/docs/citations/ADA432683.

Sim, S., and A. Duffy. 1994. "A New Perspective to Design Intent and Design Rationale." In *Artificial Intelligence in Design Workshop Notes for Representing and Using Design Rationale*, 1518:4–12. academia.edu.

Singer, J. D., and M. Small. 1966. "Formal Alliances, 1815-1939: A Quantitative Description." *Journal of Peace Research* 3 (1): 1–31.

Skidmore, Ellen Towne. 1981. "Pierre Cot: Apostle of Collective Security, 1919-1939." https://elibrary.ru/item.asp?id=7293802.

Skopik, Florian, Giuseppe Settanni, and Roman Fiedler. 2016. "A Problem Shared Is a Problem Halved: A Survey on the Dimensions of Collective Cyber Defense through Security Information Sharing." *Computers & Security* 60 (July): 154–76.

Slater, Jerome. 1965. *A Reevaluation of Collective Security: The OAS in Action*. Vol. 1. Ohio State University Press.

Snyder, Glenn H. 2007. *Alliance Politics*. Cornell University Press.

Sovacool, Benjamin K., Ishani Mukherjee, Ira Martina Drupady, and Anthony L. D'Agostino. 2011. "Evaluating Energy Security Performance from 1990 to 2010 for Eighteen Countries." *Energy* 36 (10): 5846–53.

Stefanova, Boyka. 2006. "Regional Integration as a System of Conflict Resolution: The European Experience." *World Affairs* 169 (2): 81–93.

Stirling, A. 2014. "From Sustainability, through Diversity to Transformation: Towards More Reflexive Governance of Technological Vulnerability." In *Vulnerability in Technological Cultures: New Directions in Research and Governance*, edited by A. Hommels, J. Mesman, and W. Bijker, 391. Inside Technology. Cambridge, MA: MIT Press.

Suzuki, Masahiro. 2014. "Adherence to the Past or Hope for the Future? The Historical Development of Japan's Energy Politics and Its Implications for Future Nuclear Policy." Master of Science, Central European University.

Sweeney, J. L., and J. P. Weyant. 1979. "The Energy Modeling Forum: Past, Present and Future." *Energy Policy: The Global Challenge*, 295–320.

Taormina, Robert J. 2015. "Adult Personal Resilience: A New Theory, New Measure, and Practical Implications." https://psycharchives.org/handle/20.500.12034/1598.

Teune, Henry, and Sig Synnestvedt. 1965. "Measuring International Alignment." *Journal of World Affairs* 9 (1): 171–89.

Thakur, Ramesh. 2016. *The United Nations, Peace and Security: From Collective Security to the Responsibility to Protect*. Cambridge University Press.

Thakur, Ramesh, Ramesh Chandra Thakur, Andrew Fenton Cooper, Associate Director and

Distinguished Fellow Andrew F Cooper, and John English. 2005. *International Commissions and the Power of Ideas*. United Nations University Press.

Tharoor, Shashi. 2003. "Saving Humanity from Hell." In *SEMINAR-NEW DELHI-*, 14–17. MALYIKA SINGH.

Thompson, Kenneth W. 1953. "Collective Security Reexamined." *The American Political Science Review* 47 (3): 753–72.

Thorpe, Keir. 2007. "The Forgotten Shortage: Britain's Handling of the 1967 Oil Embargo." *Contemporary British History* 21 (2): 201–22.

Tirranen, V. A. 2018. "Cryptoviral Extortion as a Global Problem of Cybersecurity." *Criminal Justice and Security in Central and Eastern*, 548–52.

Toft, Peter, Arash Duero, and Arunas Bieliauskas. 2010. "Terrorist Targeting and Energy Security." *Energy Policy* 38 (8): 4411–21.

Transportation Security Administration. 2018. "Pipeline Security Guidelines."

Trombetta, Maria Julia. 2008. "Environmental Security and Climate Change: Analysing the Discourse." *Cambridge Review of International Affairs* 21 (4): 585–602.

Umbach, Frank. 2010. "Global Energy Security and the Implications for the EU." *Energy Policy* 38 (3): 1229–40.

Valls, Manuel. 2015. "French National Digital Security Strategy." Government of France.

Van der Linde, C. 2007. "The Art of Managing Energy Security Risks." *EIB Papers, ISSN 0257-7755* 12 (1): 50–78.

Vego, Milan. 2008. *Operational Warfare at Sea: Theory and Practice*. Routledge.

Vera, Ivan, and Lucille Langlois. 2007. "Energy Indicators for Sustainable Development." *Energy* 32 (6): 875–82.

Verrastro, Frank, and Sarah Ladislaw. 2007. "Providing Energy Security in an Interdependent World." *The Washington Quarterly* 30 (4): 95–104.

Victor, David G., Sarah Joy, and Nadejda M. Victor. 2006. "The Global Energy Regime." *Unpublished Manuscript (on File with Authors)*.

Victor, David G., and Linda Yueh. 2010. "The New Energy Order: Managing Insecurities in the Twenty-First Century." *Foreign Affairs* 89 (1): 61–73.

Von Hippel, David, Timothy Savage, and Peter Hayes. 2011. "Introduction to the Asian Energy Security Project: Project Organization and Methodologies." *Energy Policy* 39 (11): 6712–18.

Wadhawan, Yatin, and Clifford Neuman. 2015. "Evaluating Resilience of Oil and Gas Cyber Physical Systems: A Roadmap." In *Annual Computer Security Application Conference (ACSAC) Industrial Control System Security (ICSS) Workshop*. acsac.org. https://www.acsac.org/2015/workshops/icss/Yatin%20Wadhawan-paper.pdf.

Walker, Ryan, Paul McKenzie, Christine Liddell, and Chris Morris. 2015. "Spatial Analysis of Residential Fuel Prices: Local Variations in the Price of Heating Oil in Northern Ireland." *Applied Geography* 63 (September): 369–79.

Walt, S. 1987. *The Origins of Alliances*. New York: Cornell University Press.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Waveland Press.

Waltz, Kenneth Neal. 2001. *Man, the State, and War: A Theoretical Analysis*. Columbia University Press.

Wang, Bing, Qian Wang, Yi-Ming Wei, and Zhi-Ping Li. 2018. "Role of Renewable Energy in China's Energy Security and Climate Change Mitigation: An Index Decomposition Analysis." *Renewable and Sustainable Energy Reviews* 90: 187–94.

Ward, Michael Don. 1982. *Research Gaps in Alliance Dynamics*. Vol. 19. Graduate School of International Studies, University of Denver.

Weitsman, P. 2004. *Dangerous Alliances: Proponents of War, Weapons of Peace*. Stanford: Stanford University Press.

Wittkop, Jeremy. 2016. "The Problem We Are Facing." In *Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices*, edited by Jeremy Wittkop, 1–20. Berkeley, CA: Apress.

Wolfe, Richard A., and Daniel S. Putler. 2002. "How Tight Are the Ties That Bind Stakeholder Groups?" *Organization Science* 13 (1): 64–80.

Wolfers, Arnold. 1965. *Discord and Collaboration: Essays on International Politics*. Johns Hopkins Univ Pr.

Wong, W. E., V. Debroy, A. Surampudi, H. Kim, and M. F. Siok. 2010. "Recent Catastrophic Accidents: Investigating How Software Was Responsible." In *2010 Fourth International Conference on Secure Software Integration and Reliability Improvement*, 14–22. ieeexplore.ieee.org.

World Economic Forum. 2019. "The Global Risks Report 2019." 14. World Economic Forum. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

Yamashita, Koji, Sung-Kwan Joo, Juan Li, Pei Zhang, and Chen-Ching Liu. 2008. "Analysis, Control, and Economic Impact Assessment of Major Blackout Events." *European Transactions on Electrical Power* 18 (8): 854–71.

Yassierli, Yassierli, Vinsensius Vinsensius, and M. S. Syed Mohamed. 2019. "The Importance of Usability Aspect in M-Commerce Application for Satisfaction and Continuance Intention." *Makara Journal of Technology* 22 (3): 149–58.

Yergin, Daniel. 1988. "Energy Security in the 1990s." *Foreign Affairs* 67: 110.

———. 2006. "Ensuring Energy Security." *Foreign Affairs* 85 (2): 69–82.

Yi-chong, Xu. 2006. "China's Energy Security." *Australian Journal of International Affairs* 60 (2):

265–86.

Yilmaz, Muzaffer Ercan. 2009. "The United Nations as Conflict Manager: A Discussion on Global Collective Security." *Journal of Social Sciences* 33 (2): 1–18.

Zou, Caineng, Qun Zhao, Guosheng Zhang, and Bo Xiong. 2016. "Energy Revolution: From a Fossil Energy Era to a New Energy Era." *Natural Gas Industry B* 3 (1): 1–11.

Zou, Zhenyu, Shuai Zheng, and Zhicheng Sha. 2018. "Study and Design on the Typical Plan for Regional Hybrid Energy Internet." *IOP Conference Series: Earth and Environmental Science* 133 (1): 012018.