3-2019

Cyber threats, harsh environment and the European High North (EHN) in a human security and multi-level regulatory global dimension: Which framework applicable to critical infrastructures under “Exceptionally critical infrastructure conditions” (ECIC)?

Sandra Cassotta

Roman Sidortsov

Christer Pursiainen

Michael Evan Goodsite

Scientific Research Publishing

Beijing Law Review, 2019, 10, 317-360
http://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-Level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under "Exceptionally Critical Infrastructure Conditions" (ECIC)?

Sandra Cassotta[1,2,3,4,5,6], Roman Sidortsov[7], Christer Pursiainen[8], Michael Evan Goodsite[9]

[1]Department of Law, Aalborg University, Aalborg, Denmark
[2]Western Sydney University (WSU), Sydney, Australia
[3]The Sustainable College Bruges (SCB), Bruges, Belgium
[4]The Institute for Security and Development Policy (ISDP), Stockholm, Sweden
[5]The Intergovernmental Panel on Climate Change (IPCC) on Polar Issues and Governance (2017-20), United Nations (UN)
[6]The International Economic Crime and Cybercrime Research Centre (IEEC) at Aalborg University, Aalborg, Denmark
[7]Energy Policy Department of Social Sciences, Michigan Technological University, Houghton, Michigan, USA
[8]Societal Safety and Environment, Department of Engineering and Safety, UiT, The Arctic University of Norway, Tromsø, Norway
[9]Australian School of Petroleum, School of Civil, Environmental and Mining Engineering, The University of Adelaide, Adelaide, Australia

Email: sac@law.aau.dk

How to cite this paper: Cassotta, S., Sidortsov, R., Pursiainen, C., & Goodsite, M. E. (2019). Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-Level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under "Exceptionally Critical Infrastructure Conditions" (ECIC)? *Beijing Law Review, 10,* 317-360.
https://doi.org/10.4236/blr.2019.102020

Received: November 24, 2018
Accepted: March 22, 2019
Published: March 25, 2019

Abstract

Business opportunities in the European High North (EHN) are accompanied by the danger of cyber-threats, especially to critical infrastructures which in these Arctic regions become "extra critical" because of the harsh environmental climatic conditions and remoteness of distances. Critical infrastructures (CI) in the EHN are crucial for numerous sectors, such as the energy sector which is completely depended on digitalization, internet and computers' commands. Such a new condition of extra criticality should also include human security concerns to avoid human disasters. An effective legal framework under "exceptionally critically infrastructure conditions" (ECIC) for this technology is important not only in terms of national legislation, but also in view of a regional, international and global networks character. This paper links for the first time, law, internet and cybersecurity, environment and society in a global human security dimension in a multi-regulatory contextual analysis. The aim is to trace the legal framework for response to a cyber-attack to

critical infrastructure in the energy sector and takes Norway as a case study because this country is highly dependent on cyber technology and on critical infrastructures. The question of research is: *using a human security focus in the case of cyber-threats under ECIC in the EHN, what ways can an assessment recommend to improve international, and regional law*? Five analytical tasks are undertaken: 1) the concept of critical infrastructure vulnerability to cyber-attacks under "exceptionally critically infrastructure conditions" (ECIC) in the EHN with focus on the energy sector is explained in connection to the notion of human security, 2) a backdrop of regional and international collaboration is followed, 3) a trajectory of multilevel contextual analysis of the different sources of law and policy applicable to cyber-threats to CI is outlined, and 4) an examination of cooperation under the North Atlantic Treaty Organization (NATO).

Keywords

Cybersecurity, Environmental Threats and Critical Infrastructures, Human Security, Global Law, Energy Sector

1. Introduction

Economic development opportunities in the European High North[1] (EHN) are accompanied by the danger of cyber-threats, especially to critical infrastructures (CIs) which in the Arctic EHN countries become "extra critical" because of environmental threats including the harsh environmental climatic conditions and the vast distances.[2] Such a new condition of extra criticality should also include human security concerns to avoid human disasters. Amongst the CIs, the energy sector[3] is especially relevant in the EHN. This sector is in large part dependent on digitalization, the Internet, and demands of computers. Interferences between the CI's digitalization subject to possible cyber-threats with climatic conditions, such as ice and natural disasters, will require new methodologies of assessment and effective legal frameworks able to protect these CIs against cyber-threats through the prism of human security. Thus, human security will become a "virtual hu-

[1]The European High Nord (EHN) in this article refers mainly the three Arctic areas of Norway, Sweden and Finland. However, it is worth noting that the term EHN has different definitions. The term is defined in different ways by different researchers and there is no one single official consolidated definition. See for that point Czarny, R.M., (2015). The High North. Springer International Publishing, 2, 7-41. Nevertheless, a precise and established definition of the term would not be relevant in the case of the approach of this article, given that it consider both European law which applies in all EHN territories (Norway is not a EU member but a party of EEA), and the interactions between cybersecurity and climate environmental conditions, a space the latter very difficult to delimit since both cyber-threats and climate change effects are trans-regional and trans-boundary and do not know any border delimitations.

[2]"Environmental threats" in this article refers to the threats of impacts of climate change such as, sea level rise (SLR) due to melting glaciers including threats of coastal regions that can affect both the environment and humans. Therefore, not only the environment but also infrastructures and people who lives in areas difficult to reach becoming remotes and with risks of flooding, are example of environmental threats that can affect not only the ecology of the areas but also human security.

[3]The "energy sector" in this article is defined by four components: oil, gas, electricity and nuclear.

man security" that societies will have to face in the future as a new kind of security concerns.

Because cyber-threats can come from anywhere in the word, an examination of the CIs under such "exceptionally critically infrastructure conditions" (hereinafter, the ECIC) requires a comprehensive analysis of the existing sources of law and policy at three levels national, regional and international[4], to observe how the pluralistic systems of legal and political sources could apply and interact with complementary legal and non-legal tools. In this article, Norway represents the domestic level, the EU represents the regional level, and several selected treaties, the international level. The concept of ECIC is based on the recent existing Norwegian criticality definitions, especially those of the recent Norwegian "model approach" consisting of a collection of reports, laws and strategies as it will be explained in Section 3.3. The reason for adoption of the Norwegian model's approach is due to the fact that this model takes into account vulnerability, locations where CIs are situated in particularly harsh environmental conditions, as it will be explained in the case of Svalbard. The Norwegian model also includes a specific and inspiring cybersecurity[5] response framework. All these mentioned components of the Norwegians model are for example lacking in other regional levels, such as the EU level or the international level. According to the Norwegian perspective, even though it could be argued that the Arctic is much less critical, as there is smaller population for instance that can be affected by CIs disruptions, there is less redundancy and longer distances in some areas at times cold whether that can justify this concept. The consequence could be enormous in terms of severity rather than impact number of victims.

But there are also other justifications supporting the existence of ECIC: firstly "cascading effects of CIs",[6] and secondly a general "climatic cascading effect", not linked to cybersecurity and CIs but to the peculiar geographical location of the Arctic. The authors of this article advocate that these two types of cascading effects act cumulatively and interact. The first cascading effect of CIs explains that increasing dependencies among CIs could trigger cascading failures and multi-sectorial collapse. This cascading effect belongs to the category of events with low probability and high consequence. The potential of domino effect seems to be undeniable. Organizations and states' involvement is not clear and

[4]In this article the term "international law" will be used in an interchangeably way with the term "global law" when referring to law other than the regional level of sources of law. This is to differential "global law" to "regional law".

[5]The term "cybersecurity" in this article commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructures and the confidentiality of the information contained therein. See the 2013 European Union Strategy, European Commission, "*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*", 7.2.2013, JOIN (2013) 1 final, High Representative of the European Union for Foreign Affairs and Security Policy, pp. 1-20.

[6]Van Eeten M., et al. (2011). The State and the Threat of Cascading Infrastructures across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. Public Administration, 89, 2, 381-400.

not easy, and states do not actually know how to deal with these events.[7] The second type of cascading effect of the CIs defined in this article as "climatic cascading effect of the Arctic" has to be differentiated from the previous "cascading effect of CIs". According to the climatic cascading effect, what happens in the Arctic does not stay there, as it is the thermic regulator of the whole planet. If there is an oil spill or a nuclear explosion, for example, this will have an enormous repercussion at global level in the rest of the planet. This is enough to justify the need for extraordinary measures protecting legally and politically, these CIs. The impact of this second cascading effect could affect not only the cultural heritage of the indigenous rural populations contributing to jeopardise their survival and thus leading to humankind extinction, but also the rest of the world due to the critical position of the Arctic.

In the EHN areas, the management of natural resources' appropriations is now increasingly becoming under cyber-control. Outlining the identification of a possible regulatory framework for this technology is important, not only in terms of national legislation, but also in view of a network at regional, international, diplomatic level. An examination of the laws governing cyber-threats to CIs under ECIC is also important for practical experts and policy-makers in a position to influence decisions in the field of international security, thus, contributing, to add a new piece in the puzzle of the concept of human security. This article map the *legal and political framework protecting critical infrastructures in the EHN with Norway as a case study* because this country is highly dependent on both cyber technology and on critical infrastructures, such as the offshore industries for example. In Norway, digitalized offshore activities are very relevant, since this country is highly dependent on these kinds of operations, especially on transportation, aquaculture and fish farming. The article aim to examine whether and which areas of international and regional law are applicable to address cyber-attacks in the energy sector of the EHN under ECIC conditions. Thus, not only an overview of the many global and regional accords operating in different areas of law is undertaken, but also domestic mechanisms are considered. In this instance, the Norwegian experience provides the case study.

Hence, the question of research of this article is the following: *using a human security focus in the case of cyber-threats under ECIC in the EHN, what ways can an assessment recommend to improve international and regional law*?

In order to assess the possibility of refitting existing legal and non-legal instruments to fill the gap of uncertainties, deficiencies and voids, especially of international and regional law, and, most importantly, to address the question of research, two main assumptions are formulated. The first assumption is if the Norwegian model could represent a legal and policy model to improve the applicability of international and regional law in designing proactive legal mechanisms achieving human security goals in a pluralistic context. The second as-

[7]Van Eeten M., et al. (2011). The State and the Threat of Cascading Infrastructures across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. Public Administration, 89, 2, 381-400.

sumption is whether the Norwegian model needs to be combined with a pluralistic and polycentric patchwork of instrument mix and governance, such as standards, strategic tools, risk assessment approaches, or a backdrop of cooperation and coordination at the geopolitical level in order to enhance the applicability of international and regional law rather than standing in an isolated way. The issue of cyber-attacks to critical infrastructures under ECIC conditions in the EHN is perceived, on one hand, in a positive way, which means as an opportunity to expand the notion of human security. On the other hand, it could also be perceived negatively, as a "disrupter" to Arctic collaboration and coordination. Next is the question of, how this coordination could be reconciled with the activity of some relevant international organizations, such as the North Atlantic Treaty Organization (NATO) and the European Union (EU). In that sense, it is important to remember that two of the EHN countries, Finland and Sweden, are not part of NATO, and that Norway is not a member of the EU although a Party of the European Economic Agreement (EEA) and thus covered by EU legislation on cybersecurity. In addition, Russia is taken as an example which is also a country located in the Arctic but not in the EHN area, manifests an ambiguous position vis-à-vis critical infrastructure in the energy sector. The vulnerability of EHN is also an important factor to consider, not only in the field of an international law, but also to security in the Arctic. Norway is vulnerable to cyber-attacks, and one wonders how this country would react if Russia should sabotage and attack Norwegians' critical, structural energy assets with the consequence of causing a serious oil spill, for example. The energy sector, especially the smart grids, is strictly dependent on digitalization, pc organisation and Internet activity. For example, in case of cyber's interferences and threats, these critical infrastructures would become "extra-critical" should communications would be totally interrupted. Vessels would be in distress and communications would be jeopardized in the harsh environment which would render hard the conduction of rescue operations. Currently, at international, EU and nation levels, the law protecting CIs looks inhomogeneous and there is a lack of uniformity. There is no regional or even global approach from the prism of human security and absence of a global treaty. Even though it seems that there could be a theoretical, applicable, regulatory framework that could be applied, there is fragmentation. Existing international legal frameworks are not directly aimed to cover expressly cyber-attacks but can be used in cyber-attacks. This is also due to the fact that these legal regimes were formed prior to the emergence of a cyber-attack and therefore not expressly aimed at regulating a cyber-attack appearing to regulate only small fraction of cyber-attacks.[8] A satisfactory regulatory framework integrating law and policy should look uniform and homogeneous including the possibility to govern freedom from risks in order to design a law based on a precautionary and proactive approach rather than reactive. In terms of governance,

[8]Hathaway, O. A., et al. (2012). The Law of Cyber Attack. Yale Law School, California Law Review, 817-885.

such a framework should not be based on a monistic[9] vision of the sources of law but rather on a pluralistic and polycentric vision[10] where sources of law and policy in provenance from different areas of law both from the public and private sector, overlap and coexist. Law and policy with different policy tools based on *standards*, *soft law*, and *technical expertise*, would thus "coexist" in a patchwork of instrument mix. Thus, critical infrastructures under ECIC conditions represent a crucial empirical opportunity to understand how to strategically design a patchwork palimpsest composed of a mix of different regulatory pluralistic instruments that will aid policy makers in policy design including freedom from hazard. In the light of this pluralistic and polycentric perspective, this article examines the interactions, the *pros* and *cons* of different categories of regulatory instrument mixes. The study emphasizes that this mix of instruments is connected to collateral to both global and non-global governance issues, such as environmental climate threats, international relations, the factor of human security, private and public approach, standards, all operating in a context of cyber-realpolitik. The regulatory protection of energy infrastructures of the EHN countries will be sketched out and discussed not only to identify applicable sources of law and policy, but also as tool to refine and expand the notion of human security in the pluralistic context.

This article is structured with the following plan. Firstly, the concept of CIs vulnerability to cyber-attacks under the ECIC conditions in the EHN with a focus on the energy sector is presented (2), and explained in connection with the notion of human security (2.1) and the energy sector (2.2). This is because impacts on CIs due to cyber-attacks jeopardize human security shift attention to risk assessment and resilience approaches as defined by both civilian and military activities. In turn, this contributes to perceiving the concept of human security in an untraditional way (not only focusing on states security but also societal challenges including environmental threats). This new perception of human security and risks under ECIC conditions linked to cybersecurity leads to understanding what existing responses in regional and international cooperation linking environmental governance and cybersecurity to CIs are, and considering if these responses are sufficient to cover risks and cyber-threats in the following sections (2.3 and 2.4). For that purpose, the link between cybersecurity under ECIC conditions and the activity of an international organization dealing with such link, namely the North Atlantic Treaty Organization (NATO), is taken as an example to see how responses are being done and how they can be improved. In the following section (3), a multi-regulatory analysis of the existing sources of law and policy is undertaken in order to identify which are the possible sources that could be applicable in case of cyber-threats and cyber-attacks to CIs in the

[9]The monistic approach of sources of law and policy as opposed to the pluralistic approach is and approach according to which the sources of law are hierarchical and not interactive.

[10]This study drawn on the theoretical approach of polycentrism and pluralism in law as treated by the legal thinking of Petersen, Zahle and Arnaud. See Petersen, H., & Zhale, H. (1995). Legal Polycentrycity: Consequences of Pluralism in Law. Dartmouth Publishing Company; Arnaud A. J. (1995). Legal Pluralism and the Building of Europe. In Petersen, H., & Zhale, H. (Eds), Legal Polycentrycity: Consequences of Pluralism in Law (pp. 127-149). Darthmouth Publishing Company.

EHN areas. In particular, in this section 3, the domestic system of Norway is taken as a source of inspiration to design a framework to protect CIs against cyber-threats under ECIC conditions. Finally, the last section (4) presents conclusions (4.1), recommendations (4.2) and future pathways linking environmental governance and cybersecurity (4.3) directed to policy-makers and international organizations on how to face the challenges of regulatory fragmentation and imperfections of international law applicable under ECIC, using the Norwegian model as a source of inspiration.

2. Exceptionally Critical Infrastructure Conditions (ECIC) Forged by Climate Change and Cyber-Threats

The Arctic and the EHN provides a lucid case to examine CIs[11] operating under extraordinary special climatic and harsh environmental conditions. The impact of climate change in the Arctic could be more devastating than in other areas of the world. This means that the national critical infrastructures of the EHN simply become "exceptionally critical". Increased sea levels, due to melting glaciers threaten the coastal regions, infrastructures and people who live in remotes and difficult distances. The increasing risk of flooding of the ecological Arctic basins affects human security, health and safety of the ecological Arctic basins.

CIs in the energy sector, connected with major military installations and hurricane evacuation routes are more vulnerable to impacts of climate change. Since it has been scientifically proven that climate change is affecting the Arctic more rapidly than the rest of the planet, this renders an already vulnerable CIs sector even more vulnerable.

The energy sector including fuel supply (gas and oil) is already the top vulnerable sector[12] compared to all the other CIs. This is a crucial sector also because it is highly interconnected with other critical infrastructures (transportation, electricity, communication, etc.) in what is defined as "critical infrastructure dependencies".[13] This means that if there were a cyber-attack[14] on the energy sector, it would also reflect in the other, dependent, CIs nested in the web of the critical infrastructures.

[11]The term critical infrastructure is defined as physical and information systems networks, services, and assets, which, if disrupted or destroyed, would have a devastating impact on the health, safety, security, or economic well-being of citizens or the active functioning of governments. The most common associated critical infrastructures are energy, finance, transport, communications, water supply, agriculture and food production, public health and security services (police and military). It is worth noticing that, the precise definition and what this definition should include in the concept, is not the same in all countries. Nevertheless, there is some guidance from the EU and NATO concerning what is considered as being a critical infrastructure. Tsagourias N. & Buchan R., (2015). Research Handbook on International Law and Cyberspace: Edward Elgar.

[12]See more at https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyber-attacks/.

[13]On the Critical Infrastructure Dependencies, see more at: https://triecker.wordpress.com/tag/critical-infrastructure-protection/.

[14]Cyber-attacks is a generic term for attacks on the e-facilities of governments, such as critical infrastructures, business, and citizens. This include, for example, spam, denial of access service attacks, spyware, and hacking. See Radzziwill, Y. (2015). Cyber-Attacks and the Exploitable Imperfections of International Law. Brill Nijholff; Gorge, M. (2007). Cyberterrorism: Hype or reality? Computer Fraud & Security.

In the light of this extreme vulnerability, it is worth noticing that both the energy and electricity sectors are amongst the only critical infrastructure sectors with mandatory cyber-security standards[15] and thus regulated both by the public and private sectors. For example, if it is considered the energy power plants, these can be owned both by the state and by private companies. In that sense, the ECIC, is a concept according to which the "exceptionally critical infrastructure conditions", are forged by the sea level rise, coupled with storm surges which will continue to increase the risk of major coastal impacts on transportation infrastructure, including both temporary and permanent flooding of airports, ports and harbors, road, rail lines, tunnel, bridges, maritime routes interrupted with vessels in distress, with the risk that entire populations could remain completely isolated from the rest of the world.

Due to the existence of the two cumulative effects of cascading effects to CIs, the nexus between the exceptional vulnerability of critical infrastructure under these special climatic conditions and cyber-threats needs a special care to be mitigated, regulated and managed. This special care, should not only be understood from a concrete, practical and management side, to mitigate the risks of both cyber security insecurity and climatic conditions, but as an urgent need to design a special proactive legal protection that could actually provide real protection including risk assessment due to the existence of the cumulative effects of cascading effects to CIs.

A cyber-attack to critical infrastructure in the energy sector under ECIC can be compared to extreme climatic events, because of the unpredictability, the rapidity and vulnerability of the area touched with the consequences of a profound black out, in an environment with less resilience. In such an environment, the time needed to go back to normality would certainly be longer. The threats are also changing rapidly and it impossible to predict what this change will look like, even if in a short horizon of time, which makes it very difficult to design mitigation strategies from a political and legal vantage point. Even adaptation plans from a climate change law and policy perspectives, will be difficult to draw, especially from a proactive approach rather than reactive.

Such problems, might even lead us to think about a new idea to enlarge the notion of adaptation to climate change, in order to include in it, also cyber-threats as well, and their consequence on the environment and human security, since energy critical infrastructure are closely woven into environmental climatic conditions, and cannot be managed and regulated one at a time for the sake of human security and to avoid human disasters.

2.1. How Does the Cybersecurity of Critical Infrastructures under ECICof the EHN Contribute to the Notion of Human Security at Global Level?

The world is at a point of non-return for an historical transformation from fossil

[15]Zhang, Z. (2013). Cybersecurity Policy for the Electricity Sector: The First Step to Protecting our Critical Infrastructure from Cyber Threats. Boston University Journal of Science and Technology Law, 19.

fuel to an energy system of global interconnected infrastructures where the power network from generation to transmission and distribution to consumption is dependent on information and cyber technologies. The future network will encompass hundreds of millions Distributed Energy Resources (DERs) such as solar panels, wind turbines, electric vehicles, energy storage devises, smart grids and other power electronics.

On the one hand, this energy system transformation will create great opportunities for the business sector. On the other hand, energy systems networks will become targets of significant threats. Given the easy and speed at which malicious cyber activities occurs and the low cost of cyber weapons, the anonymity that cyberspace[16] affords and the interconnectivity of networks, malicious cyber activities pose a serious threat not only to individuals, corporations and industry but also for states.[17] The discussion on the possibility of a cyber-war, which shifts the attention from civilian to military engagement to potential attacks against state infrastructures, especially when hypothetical threats and the consequence on societal security are in play, is an argument justifying the need to consider the concept of human security in a broader context at global level, not only confined to state security and to physical actions.

The role of international law can be relevant for maintaining access to cyberspace but also in dealing with such threats. Cyberspace where global digital communication and any kind of critical infrastructure operate, is an "international and global space", thus subject to international law.

Different international law frameworks may be applicable and can overlap, as will be explained in section 3 of this article. One type of cyber threats, could be a cyber-attack, which can be addressed both by international law regime on the use of force (*jus ad bellum*) or in peace time (*jus in bellum*).

The EHN face different kinds of security risks that range from disputes over territory and maritime delimitations weapon testing, shipping accidents or marine pollution, hazardous accidents and waste disposals, competition for living or non-living resources, and the adverse effects of climate change increasing the frequency of extreme events. The sources of all these threats are both human and environmental. The consequences of these threats affect both human security and the integrity of the natural world. In addition, if the Arctic regions were affected from these threats, this would have enormous repercussions, not only in the Arctic region, but also in the rest of the world. Note the "cascading effects of the Arctic" means that what happen in the Arctic, does not stay there, but re-

[16]Cyberspace or Cyber-Realm is a virtual realm created as a result of the use of information technology. See Radzwill, Y. (2015). Cyber–Attack and the Exploitable Imperfection of International Law. Glossary, Brill Nijhoff.

[17]Tsagourias & Buchan (2015). Cyber-Threats and International Law. In "*Security and International Law*" Edited by Footer, E. M, Schimt, J., White D. N., Bright, D. L (Eds.). Oxford and Portland, Oregon.

flects in the rest of the planet.[18]

Hence, the authors of the present article advocate that the concept of human security is tied to cyber-security[19] which is now including the security of CIs against cyber-threats.

The concept of human security is extremely controversial not only for the way that the different disciplines have conceptualized it,[20] but also among proponents of different conceptualizations within single disciplines.

Security is a societal value, a political goal and also a tool of protection, of risk reduction, certainty and predictability in contrast to danger risk and threat. Security in an objective sense measure the absence that such values will be attacked. Security in an intersubjective sense, is "what actors make of it" by putting relevance to issues which are considered at utmost importance and which require "extraordinary measures".[21] The concept of human security refers to a fundamental shift in the referent object of security from the state world (national, regional international or global security) to a people–centered approach. In that sense, not only human beings, families, and communities constitute a "referent object" but also humankind.[22] This is a non-traditional way to conceive the concept of human security and also the main approach used in this article.

In the Arctic and in the EHN areas the additional increase resource competition between major powers and strategies with additional risks and conflicts, such as nuclear, bioenergy, energy are all digitalized, and thus the risk of cyber threats against their CIs will increase.

The concept of human security should therefore include the protection against the risk of cyber-attacks to CIs. The notion of human security should be a dynamic one as well and should also include cyber-security and take into consideration in the wide range of threats to security (such as human rights violations, drugs, terrorism, piracy) also cyber-attacks linked to environmental threats and in particular those against critical infrastructures in the energy sector because more exposed to environmental conditions and social vulnerability.

At the United Nations (UN) level, the environmental dimension of international security proposed a fourth human security dimension pillar as "Freedom

[18]Intergovernmental Panel on Climate Change (IPPC), Forth Assessment Report: Climate Change. (2007). Working Group II: Impacts, Adaptation and Vulnerability; IPCC: Author. Cassotta S., et al. (2016). Climate Change and Human Security in a Multi-level and Multidisciplinary Dimension: The Case of the Arctic Environmental Ocean. In Climate Change Management, Springer, Berkam P. A. & Vylegzhanin A. (2010). Environmental Security in the Arctic Ocean. Nato Science for Peace and Security Series: C Environmental Security, Springer.

[19]In the 20013 EU Strategy, the term cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.

[20]The concept of human security in international relations, in the scientific discourse or at theoretical analytical level or in legal terms, differs significantly.

[21]Wæver, O. (1995), (1997), (2008). In Sheffran J., et al. (2012). Climate Change, Human Security and Violent Conflicts in the Anthropocene, Springer, 3.

[22]Brauch, H.G., et al. (2012). Global Human and Environmental Security Handbook for the Anthropocene. Springer.

from Hazard Impacts".[23] While hazard cannot be prevented, their impact can be preventative reduced. The background for this fourth pillar of human security as "Freedom from Hazard Impacts" is to deal with the environment, sustainable development, disasters, early warning, disaster preparedness and reduction of social vulnerability.

In essence, human security can be viewed as a holistic global transnational non-traditional approach. A crucial aspect of the concept of human security that has emerged on the international agenda is "energy security" defined by the International Security Agency (ISA) as the "uninterrupted availability of energy resources at an affordable price."[24]

This means that also cyber-threats should be taken into account to guarantee the availability and affordability in a way to create a link between CIs, energy and cyber-security under the umbrella of the concept of human security to guarantee security and to try to govern freedom from risk of hazard. There are currently no treaties or regional agreements that guarantee such a linkage.

In the EHN, the security agenda could thus be said to encompass all international rules that regulate and guide human conduct and the concept of human security should be used to design an agreement protecting CIs against cyber-attacks under ECIC conditions. Arctic human security is to be conceived broader that regional as a wide range of international law is relevant despite the gaps due to the presence of both states and rural human indigenous population, even if smaller.

In the Arctic and specifically in the EHN regions the human security agenda should include cybersecurity and elaborate a sort of "Arctic energy security agenda under ECIC conditions" that could encompass international, regional or national rules that regulate in a proactive way and guide human security.

At a general global level, and not only in relation to the Arctic, the notion of human security should be broadened in order to include cyber threats against critical infrastructures in the energy sector. The Arctic is an example showing the need for broadening the notion of human security from a traditional to a non-traditional way to perceive the phenomenon. The reason why it is imperative to broaden the notion of human security is given by the fact that CIs on the energy sector are extremely vulnerable to climatic conditions. CIs are also key arteries both for civilian and military strategies and also more exposed to cyber-attacks, which combined with climatic conditions and climate change ef-

[23]As in the political debate in the UN, the scientific discourse on human security and scientific efforts to define this concept have primarily focused on three pillars: a) "freedom from fear" addressing the conflict and humanitarian agenda; b) "freedom from want" in the context of the human development agenda; and c) "freedom to live in dignity" with reference to human rights, the rule of law and good governance. See Report of the United Nations Trust Fund for Human Security Human Security from Theory to Practice, and overview of Human Security Concept and the UN Trust Fund for Human Security, Human Security Unit – UN, and the Report for the United Nations University Institute on Environment and Human Security (UNU-EHS), in Braunch, H. G., (2012). Re conceptualizing Security: A Contribution for the 4th phase of research on human security and environmental security and peace (HSEP). Proceeding for the ISA Conference in Montreal, Canada.

[24]See more at https://www.iea.org/topics/energysecurity.

fects, could result in a disastrous binomial combination. In the Arctic, climatic conditions are harsh, and therefore climate change has been linked to security by means of the concept of "climate security" and another component extremely relevant and sensitive for Arctic security, is the issue of energy security.

The notion of human security should therefore encompass cyber-security and should be perceived holistically. In turns, this call for a set of rules that addresses and guide human conduct and that should be designed in a way to cover not only conflicts among states, but also among citizens, private sectors and stock-holders. Civil society's use of energy resources and the protection of CIs under ECIC and management of the cybersecurity space under which these infrastructure operates, should be regulated, and with a holistic vision, interconnecting all the dots. In the EHN, however, cyber-threats have not been included in the notion of security. Security, in the Arctic, in the traditional sense, has encompassed a series of issues, such as transportation of nuclear weapons by sea or nuclear weapons. Today, the notion of human security must also include cyber-threats, especially against CIs due to the increasing of the number of networks especially in the energy sector.

In addition, human security is not only physical but with cyber threats, becomes also a "virtual human security risk". This implies that the society must be protected by rules regulating this new kind of human security risks. Society's growing dependency on critical infrastructures and systems has given birth to a new class of cyber-physical threats that may facilitate physical attacks with a cyber-attack: a so-called "cyber enabled attack on CIs".

The attack would be virtual but with a physical impact striking, not only human and environmental spheres but also the most vulnerable people of the Arctic: the indigenous people living in remotes areas and who are often confronted with a harsh environment. Therefore, a broader notion of human security in the case of the EHN would include special features that provide protection for people living in close contact with the environment and climatic conditions which are more exposed to the impact of cyber-attacks. This mainly because of the proximity and the nexus among Arctic critical infrastructures in the energy sector under ECIC, energy resources and indigenous style life, which need special legal protection.

Human security approach to CIs under ECIC conditions would thus address sources of insecurity which require a private and public security approach based on rule of law and effective enforcement and a legal framework able to guarantee a threshold of severity. Such a threshold-based approach useful to establish when it can be established that human security is at threat and that limit threats by their severity rather than their cause, still need to be fixed.

2.2. Focus on the Energy Sector: Peculiarities, Climatic Conditions, Cyber-Threats and the Case of Norway as an Example of ECIC

The analysis of hypothetical threats on computerized objects that society relies upon, begins with the critical infrastructures of the energy sector, a top priority

in the range of cyber threats to critical infrastructure, as already observed in the previous section. Discussing cyber-threats to critical infrastructures in the energy sector in the Arctic is challenging because it is possible to observe this phenomenon only by looking at hypothetical incidents since these kinds of threats, have never really occurred, yet.

Nevertheless, outside the Arctic, the world is certainly not exempted from cases of cyber-attacks of this genre.[25]

The tendency, today, is to acknowledge through military exercise, the protection of critical infrastructures of the energy sector. In particular, it has been stressed that during such operations, power grids are the most vulnerable parts.

In a more concrete way, what is at the most risk and a highly vulnerable systemic element is what is defined as the Supervisory Control and Data Acquisition (SCADA), which is a computerized control system that monitors and regulates physical industrial processes. In particular, the SCADA in system of power grids is highly vulnerable, especially during a hypothetical ice storm, which is the EHN, occurs frequently.

Cyber-attacks against again critical infrastructures in the energy sector management also shuts down electricity for a prolonged period of time, and have devastating effects, also on other critical infrastructures, especially on communications and the gas industry.

Energy power stations are connected to each other and to a centralized SCADA system, which also explains the high vulnerability of this sector that becomes extra critical under Arctic climatic conditions, thus putting the whole system at high risks.

The national security implications of climate change include threats to risks to energy and critical infrastructures operating under extreme events. These events affect energy production as well as transportation, transmission and distribution infrastructure, with the possibility of causing supply disruptions of immense magnitude, exposing Arctic zones to complete isolation due to the black out of electricity supply. In addition, higher summer temperatures will increase electricity use causing higher summer peak loads while warmer winters will decrease energy demands for heating.

Cyber-attacks in the Arctic could occur under certain climatic conditions determining sea-level rise, or extreme storm surge events, all of which would intensify the consequence of these cyber-attacks and impact on coastal facilities and infrastructures on which many energy system, markets and consumers de-

[25]Amongst the examples of cyber-attacks to critical infrastructures to the energy sector, it should be recalled: 1) the Nigerian Pipeline explosion in 2006, that was reported to have killed at least 260 people, 2) the famous 2003 cyber-attack employing the Stuxnet work and aimed at crippling the Iranian nuclear program, involving also health hazard, 3) the 1995 cyber-attack against the US Departments of Defence and Energy, giving the Argentinian cracker Julio Ardita access to satellite, radiation and energy research, 4) the 2012 cyber-attack against the Saudi Arabian Oil Company (Aramco) when the Shamon virus wiped out hard disks on thirty thousand computers leading Saudi Arabia to conclude that it was an attack against, its economy, possibly from Iran, 5) the 1999 attack against the Russian Gazprom directed at the digital system controlling gas flows in pipelines.

pend which will in turn high cause disruptions of essential services across the EHN.[26]

In the Nordic countries, compared with aerospace, defense, healthcare, shipping and government, the energy sector is among the second key sector at risk for cyber-attacks. This sector is particularly relevant to Norway's resources and role as a top supplier to the EU. In particular, Norway's key industries at risks are those of oil and gas exploration, production and distribution, green energy development and industrial control systems.

Norway is increasing its portion of the market in supplying the EU and Baltic States, despite the dependence of these countries on Russian energy, which has decreased following the Ukrainian crisis.[27] This is also a sector where Norway plays a particular role, also from a geopolitical perspective because it provides an alternative to dependence on Russian gas. Norway has also a big responsibility in trying to disentangle Europe and the Baltic States from Russia. This explains why Norway's police claim that Russia is increasing its intelligence collection with regards to the Norwegian energy sector, with the intent to sabotage it.[28] The Norwegian government is well aware on the fact that the nation should be kept prepared for the improbable and the existence of a real threat for the Norwegians energy providers.[29] The Norwegian private sector, in particular, the companies, already perceive themselves at risk and find it difficult to prepare for something that might happen, but has not happened already. In 2014, around 50 companies in the oil and energy sector were exposed to the biggest attack in Norway's history.[30] In August of the same year, the Norway's National Security Authority (NSM) reported that among the 50 companies, also Statoil firm was compromised. Other 250 Norwegians companies were advised to check their networks for evidence of malicious activity.

This activity is believed to be associated with the Russian's actors behind the Ferger/Havex malware[31] family that has been referred to by other researcher as "Energetic Bear" or "Dragonfly".[32] Society's vulnerability will only increase not only because of evident cyber-threats but also considering that by 2019 "smart meters", which are Advance Metering Infrastructures, will be installed in all Norwegian households providing increased capacity of electric power supply which will also increase the vulnerability to cyber-attacks at the same time. The

[26]Report from the White House, Washington (2015). Findings form Selected Federal Reports: The National Security Implications of a Changing Climate-Readiness in a Changing Arctic), 7.

[27]Oxford Institute for Energy Studies, Reducing European Dependence on Russian Gas: distinguishing natural gas security from geopolitics, (2014) retrieved from: http://www.oxfordenergy.org/wpcms/wp-content/uploads/2014/10/NG-92.pdf.

[28]Norway Intelligence Claims Russian Intelligence Intensifies Monitoring Norwegian Energy Activities. The Nordic Page. (24 March 2015).

[29]Report from the Norwegian National Security Authority (NSM), the Norwegian Police Security Service (PST) and the Norwegian Government's Cyber Security Strategy for Norway (2012).

[30]Skotnes, R. Ø. (2015). Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector. Ph.D. Thesis, Faculty of Social Science: University of Stavanger.

[31]Malware is a malicious software used to facilitate or carry out cyber-attacks.

[32]Report, Fireeye Threat Intelligence. (2015a). Cyber Threats to the Nordic Region. 10.

Finnish Ministry of Foreign Affairs reported events of cyber-espionage in 2013 as well as reporting that it has been victim of cyber espionage and data theft of political intelligence for approximately four years. Even though the Finns did not identify any suspects, it is believed that, Russian, and the Chinese actors were behind the event.[33]

2.3. Link between CI's Cybersecurity under ECIC Conditions and International Cooperation: NATO's Role

Regional cooperation on cyber security for critical infrastructure in the energy sector is aimed at controlling and making secure any disclosure of vulnerabilities and incidents affecting the energy sector in its crucial role and meeting the need for effective communication. This also includes cooperation and collaboration among stakeholders.[34] The linkage between environmental governance, particularly between climate change and cybersecurity under ECIC conditions is important in term of responses occurring through international cooperation, for example to achieve resilience. In that context, it is relevant to stress that linking environmental governance to cybersecurity and to resilience is of specific interest. Specifically, what is of interest, is the link that has been made with the North Atlantic Treaty Organization (NATO)'s approach in this regards. Approaches for Arctic risks assessment and resilience in the EHN as defined by both civilian and military agencies, are focusing on system resilience which are required for unknown and hybrid threats. Resilience and increased civil-military readiness is recognized as a key NATO goal in the Warsaw Summit of 2016.[35] The Warsaw Summit discussed threat to digitalized CIs including anthropogenic (i.e. cyber-attacks) as well as environmental threats (i.e. natural threats such as space weather or other extreme weather events). Nevertheless, there is no explicit cooperation or coordination among the EHN' areas under ECIC conditions. It is also worth noticing that sometimes NATO nation member states and EU Member States do not correspond. There is a need to bind and build up a framework that interconnects countries that are not included in the different frameworks such as, for example, Finland and Sweden that are members of the EU but not of NATO, and Norway which is not a member of the EU but a member of NATO. This is because all the systems are interconnected especially in the energy grids. The protection of energy grids has various aspects and there is no such EHN's framework except some kind of collaboration and form of cooperation in cyber security between NATO and the EU. This should be defined in a cyber-response

[33]Report, Fireeye Threat Intelligence. (2015b). Cyber Threats to the Nordic Region. 13.

[34]The cooperation and role of stakeholders has been particularly highlighted by Elinor Ostrom's framework on polycentric governance. This author produced an important study connecting cyber-attack, CIs and the environment. Particularly, the study on Institutional Analysis and Design (IAD) and Socio-Economical Systems (SES) frameworks to the topic of atmospheric governance which suits the purpose of complementing the gaps of law. See Ostrom, E. (2012a). Polycentrism Systems: Multilevel Governance Involving a Diversity of Organization. In Global Environmental Commons: Analytical and Political Challenges Involving a Diversity of Organization. Eric Brousseau, et al. eds, 105, 177.

[35]Warsaw Summit Communiqué, Issued by Head of State and Government participating in the meeting of North Atlantic Council in Warsaw, 8-9 July 2016-06/July/2016, Press Release (2016).

framework taking into account harsh environmental conditions as a consequence of climate change impacts, namely resilience The basis and fundaments of such a necessity is not inconsequential if it is considered that EHN areas often cooperates in different efforts aimed enhancing cyber security, not only from a logistic point of view but also in terms of research. Two examples of such kinds of EHN collaboration are, firstly, the Nordic Cyber Security Exercise conducted in Linköping in 2015.[36] The exercise was a strategic collaborative effort for enhancing cyber security within the Nordic Countries. The collaboration was part of efforts to assess and strengthen cyber preparedness, examine incident response processes in response to ever-evolving threats and most importantly, enhance information sharing amongst Nordic countries.[37] A second example is the effort of the Finnish Cyber Environment Project started in 2014 analyzing cybersecurity trends and the current status of and development needs in the public and private sectors in six countries, including Sweden.[38] However, it seems that there is a lack of awareness concerning the need to establish a special framework for EHN countries, taking into account ECIC conditions except for a recognition of the need to establish a special coordination and cooperation in the EHN on resilience. Nevertheless, resilience is a concept that is not only pertinent to climatic and environmental conditions but also to human, socio-technical, societal, organizational, political and transnational conditions.[39] The national programme focuses on societal security in the Nordic programme administered by the Research Council of Norway. It dedicates attention to the effects of climate change on security implications of climate change and critical infrastructures, especially after examination of the positions of Norway, Finland, Sweden and Denmark.[40]

The problem of coordination and cooperation in case of attack to CIs in the energy sector in EHN countries would still arise for those countries that are not members of NATO, such as Finland and Sweden. So, developing an international practice involving also non-NATO countries, would be prudent, especially by starting to identify, common core problems. In that sense, it is worth noticing that a Joint Cyber Trading Nordic Priority Programme exists in the area of cyber warfare technology under the umbrella of the military–run Nordic Defense Cooperation (NORDEFCO) programme. This programme pools information gained from military operated cyber defense centers with research and intelligence units. The NORDEFCO's pan-Nordic Warfare Collaboration Project (CWCP) also interacts with the NATO CCDCE.[41] Even though the CCDCE

[36]Press release. (2015). Nordic Cyber Security exercise was conducted in Linköping, Centre for Cyber Security.

[37]The objective of the exercise were to strengthen the Nordic National CERT Collaboration (NCC) and to develop collaboration on a technical level and testing the existing standards of cooperation procedures and mechanism as effective responses to Nordic Cyber-crises requires cross-country cooperation.

[38]Press Release, Finnish cyber security environment-current situations, targets and measures to achieve these, 2017, 77, Prime Minister's Office.

[39]Report, Norden, NordForsk, (2013). Societal Security in the Nordic Countries. Policy Paper 1, 6.

[40]Report, Norden, NordForsk, (2013). Societal Security in the Nordic Countries. Policy Paper, 23-24.

[41]Opitz, C., (2015). Potential for Nordic Baltic Security Cooperation-Shared Threat Perceptions Strengthens Regional Collaboration, German Institute for International and Security Affairs.

primarily serves the objectives of NATO and the NATO nations, it is worth noticing that it does run cooperation and coordination projects jointly with specialized cyber military and law enforcement agencies in NATO partners' countries, which includes Sweden and Finland the two non-NATO members.[42]

2.4. Cyber Threats against the Backdrop of Regional and Industry Collaboration and Cooperation

The EHN and the Arcticregion has benefited from strong international cooperation, through official and unofficial channels and involving Arctic Eight,[43] Arctic Five,[44] as well as neighboring Arctic states.[45] Some of examples of productive Arctic cooperation include the Agreement on Cooperation and Aeronautical and Maritime Search and Rescue in the Arctic (SAR), developed under the canopy of the Arctic Council and signed by the eight Arctic states, and the Treaty between the Kingdom of Norway and the Russian Federation concerning Maritime Delimitation and Cooperation in the Barents Sea and the Arctic Ocean (Treaty between Norway and Russian Federation") that put a four-decade maritime boundary dispute between at rest. Yet despite the clear benefit of and occasional need for cooperation, competition takes center stage, often clad in military fatigues. Thus, the international dynamic in the region is also characterized, *inter alia*, by: 1) the competition among the Artic littoral states over economic space and geopolitical influence; 2) the struggle of non-littoral Arctic states to not be overshadowed by the Arctic Five; and 3) the effort of economic powers to ensure that their interests are protected once Arctic ice recedes.[46] The image of a Russian submarine planting a flag on the seafloor at the North Pole illustrate the conflicting nature of international relations in the Arctic.[47] The tension between cooperation and competition is particularly present in the EHN. For example, the Russian Federation resumed Cold War era bomber patrols over the Norwegian exclusive economic zone (EEZ) in 2007.[48] The annexation of Crimea in 2014 brought the tensions between Russia and the West to a new level. Yet the competition is eclipsed by arguably the most fruitful and extensive cooperation in the entire Arctic. EHN, has seen international cooperation on virtually every level and of every kind. Established by the Kirkenes Declaration in 1993, the Barents

[42]O'Dwyer, G., (2015). Join Cyber Training New Nordic Priority. White paper: Global Defense Perspectives, see more at http://www.defensenews.com/story/defense.

[43]These counties include: Canada, Denmark (including Greenland and the Faroe Islands), Finland, Iceland, Norway, Russian Federation, Sweden, and the United States of America.

[44]Arctic littoral states.

[45]*E.g.* the Russian Federation and Norway.

[46]For example, six nations (China, India, Japan, the Republic of Korea, Singapore, and Italy) were given an observer status at the Arctic Council's Ministerial Meeting in Kiruna on 15 May 2013. Arctic Council, Observers, http://www.arctic-council.org/index.php/en/about-us/arctic-council/observers (last visited June 10, 2013).

[47]Russia Plants Flag under N Pole, BBC, (Aug. 2, 2007), available at: http://news.bbc.co.uk/1/hi/world/europe/6927395.stm.

[48]Russian Strategic Bombers Carry out North Patrols, Ria Novosti, (Sep. 12, 2012), *available at* http://en.rian.ru/military_news/20120912/175920165.html.

Euro-Arctic Council (BEAC) has been the forum for intergovernmental cooperation at the ministerial level.[49] The Barents Regional Council, also founded under the Kirkenes Declaration in 1993, facilitates cooperation among "counties or their equivalents."[50] The BEAC has also supported cooperation among cultural leaders, entrepreneurs, as well as educational and research institutions.[51] However, because only Norway and Russia have control over the continental shelf in the region, these two states are poised to work together on energy issues. The aforementioned Norway-Russia Treaty not only established a regime for development of joint hydrocarbon deposits but also mandated close cooperation should such a field be developed.[52] The pre-Crimea era saw a flurry of joint industry initiative. The partnership between Russian and Norwegian oil and gas industries at large has become a natural fit, with the Norwegian side providing technological and operational know-how while filling a huge need on the Russian side.[53] Barents 2020, a joint Norwegian-Russian initiative directed at harmonization of health, safety, and environmental (HSE) standards serves as an example of multisectoral international cooperation.[54] Barents 2020 was initiated and funded by the Norwegian government and involved government agencies, oil and gas industry, scientific and research institutions, and NGOs.[55] Yet the cooperation was not only centered on the question of *how* to find and extract hydrocarbons in the most efficient and safe manner. Environmental groups in both countries worked together to raise awareness as to the question of *whether* offshore oil and gas development in the EHN is a sound policy decision.[56] Indigenous communities across the region whose livelihoods are often affected the most by oil and gas development pondered the same question as well.[57] As noted above Russia's annexation of the Crimean peninsula slowed down and, in some cases, halted cooperation completely. The United States and European Union imposed economic sanctions that all but ended oil and gas industry cooperation

[49]Beac. St. Barents Euro-Arctic Council http://www.beac.st/in_English/Barents_Euro-Arctic_Council/Barents_Euro-Arctic_Council.iw3 (last visited June 10, 2013).

[50]Beac.St Barents Regional Council (BRC) http://www.beac.st/in_English/Barents_Euro-Arctic_Council/Barents_Regional_Council.iw3 (last visited June 10, 2013).

[51]Beac.St, The Barents Projects, http://www.beac.st/?DeptID=25430 (last visited June 10, 2013).

[52]Norway-Russia Treaty, Ann. II.

[53]Hakon S. (2011). How to Establish Cross-Border Business and Become a Part of the Existing Supply Chain. (Eds), Frode Mellemvik and Sergey Vasilev [hereinafter Skretting].In Perspectives of Norwegian-Russian Energy Cooperation.

[54]Barents (2012). Assessment of International Standards for Safe Exploration, Production and Transportation of Oil and Gas in the Barents Sea, Final Report Phase 4, 9. Bellona, Oil.

[55]*Id* at 12.

[56]Bellona, Oil http://www.bellona.org/subjects/Oil (last visited June 10, 2013). Bellona is an international NGO founded in Norway with offices in Russia and other countries. Bellona, about Bellona, http://www.bellona.org/subjects/1140449074.91/aboutussection_view (last visited June 10, 2013).

[57]Norwegian Barents Secretariat, Barents Indigenous People's Office, Economic Development in the Indigenous North http://www.barentsindigenous.org/economic-development-in-the-indigenous-north.5143491.html (last visited June 10, 2013).

in offshore and Arctic projects.[58] The 2017 round of sanctions imposed by U.S. Congress made any cooperation in the oil and gas sector a remote possibility.[59] An argument can be made that the prior transboundary bridges in the EHN can serve as pathways for cyber threats emanating from Russia. The Kremlin has a vital interest in developing Arctic offshore oil and gas deposits. Russia's oil reserves are declining. In fact, Russia saw the largest decline in oil reserves in 2014, 1.9 billion, among oil producing states.[60] The Russian leadership designated Arctic oil fields, including offshore as a key area for the "resource base expansion."[61] In fact, this area according to President Putin, will greatly contribute to Russia's growth.

Lomonosov once said that Russia will grow through Siberia—he was right, it is already happening. However, it will certainly grow through the Arctic. And not just because of its gigantic—global, I would say—all-planet mineral resources. I am talking about oil, gas, and metals also, because this region is very suitable for developing a transportation infrastructure.[62]

However, Russian companies need Western, particularly Norwegian, expertise to operate in Arctic waters. For example, Rosneft and ExxonMobil selected Norwegian company and Seadrill to operate the West Alpha drilling platform in the South Kara Sea.[63] Therefore, it is not unreasonable to presume Kremlin's motivation to engage in cyber espionage for the purpose of obtaining valuable technological data or carrying out a cyber-attack in retaliation for compliance with the sanctions or as a method convincing to cease complying with them. It is also possible that the prior attempts to cooperate (educational and industry exchanges, for example) could have been used by the Russian intelligence to "plant seeds' in Norwegian, Swedish, and Finish computer networks.

3. Legal and Policy Framework Applicable to ECIC in a Pluralistic and Polycentric Approach

As introduced previously, this section explains that a coherent, homogenous regulatory framework protecting critical infrastructure in the Arctic and in the EHN specifically, is not in place. However, this does not mean that there is a le-

[58]U.S. Energy Information Administration, Russia, https://www.eia.gov/beta/international/analysis.cfm?iso=RUS (last visited 15 December 2017).

[59]Sidortsov, R. (2017a). At the Crossroads of Policy Ambitions and Political Reality: Reflections on the Prospects of LNG Development in Russia. Oil, Gas & Energy Law Journal (OGEL), LNG Special Issue, 15.

[60]BP. (2015). BP, Statistical Review of World Energy 2015, Oil Reserves. Retrieved June 16, 2015, from http://www.bp.com/en/global/corporate/about-bp/energy-economics/statistical-review-of-world-energy/review-by-energy-type/oil/oil-reserves.html.

[61]Sidortsov, R. (2017b). The Russian Offshore Oil and Gas Regime: When Tight Control Means Less Order. In Pelaudeix, C., and Basse, E.M., (Eds.), Governance of Offshore Hydrocarbon Activities in the Arctic.

[62]The President of Russia, All-Russia Youth Forum "Seliger", 29 August 2014a, accessed 1 September 2017 http://news.kremlin.ru/news/46507/print (hereinafter, Presidential meeting transcript, 29 August 2014).

[63]The President of Russia, Videoconference with the West Alpha Platform in the Kara Sea, 9 August 2014b, accessed 1 September 2017 http://news.kremlin.ru/news/46421/print.

gal *vacuum* or that there are no laws applicable. It means that the combination of international law with a policy approach, which can be applicable, has not been identified yet.

The following section of this article (3.1) will examine international law in a pluralistic and polycentric approach with particular reference to *jus ad bellum* and *jus in bello*, and on how they can coexists rather than being in a hierarchical relationship. Both *jus ad bellum* and *jus in bello*as are not "self-contained regimes". This means that they are related to each other and to other legal regimes pertaining to difference areas of law. Furthermore, both state and international organizations and behaviors of different actors are involved in the regulation, protection and management.

From 3.1 to 3.4 this article will address the political component and explore how does international relations influence the design and the applicability of a possible framework applicable. In that sense, the discussion of the role of international organizations and the existence of cooperation already in place, as well as non-state actors is pertinent.

The discussion on the applicability of international law and the analysis of how this law could "fit for purpose" is entrenched with the political factors that exercise a direct influence on the law applicability and in that sense law and policy are clearly interwoven. This investigation will lead to understand which the international law applicable can fit for purpose for the protection of critical infrastructures. Is it international law, international humanitarian law, space law or IT law? Which are the main actors connected to critical infrastructures for energy systems in the Arctic EHN and operating in the areas? Which kind of instruments would be available? For example, command and control, self-regulations, standards, voluntary measures, liability rules or risk assessment and management combined with private initiative or only public? The template of a possible framework that could fulfill this for purpose clearly denotes the characteristics of a regulatory package of mixed instruments.

From a legal point of view, the theoretical approaches of polycentrism and pluralism, offer an important tool in explaining which law would best fits the purpose to protect critical infrastructures in the energy sector under ECIC conditions and it is particularly suitable in the analysis and systematization of fragmentation in international law and multi-level governance. Polycentrism and pluralism is a theoretical approach useful to design comprehensive and coherent legal frameworks that systematize the game of multilevel governance. The design of a comprehensive and homogeneous framework is much needed to address cyber-attacks at both the domestic and international levels especially in order to understand how the different levels of sources can interact to complement each other and create an applicable more effective legal framework.[64] This legal approach is complemented by a second theory of political science of polycentric governance applied to cyberspace from Elinor Ostrom which can help to con-

[64]Hathaway, O. A., et al. (2012). The Law of Cyber Attack, Yale School, California Law Review, Paper 3852, 817-885.

ceptualize the dynamics of multi-regulatory systems, given it embrace a multistakeholder governance approach, norms, bottom-up regulations and targeted measures to enhance cybersecurity in the case of multipolar politics. Elinor Ostrom, produced an important study applicable to cyber-attacks which is defined as an Institutional Analysis and Design (IAD) and Social-Ecological Systems (SES) frameworks to the topic of atmospheric governance[65] which suits the purpose of complementing the gaps of the law. The law cannot explain it all and there is a need to analyze the "law in context" where international law cannot be separated from political context and the behaviors and interests of official and non-official actors, including international organizations and stakeholders.

Just as this multilevel system is important for environmental governance in large ecological systems with distinct local dynamics, so too is it essential for enhancing cyber-security given the local, national and global impact of cyber-attacks on economic development and human security. This is linked to the framework complexes that can form the theoretical substratum of cyberspace where several different systems coexists in the same issue area without clear hierarchy which can be caused by various and continuously evolving of political coalitions.

The regime complexes recognize the relevance of the need for industry best practices to proactively adopt the rapidly threat matrix based on risk assessment which could become a model for polycentric regulation or cyberspace.

The regulatory environment where cyber-threats can occur is proactively implementing not only public law but also private law due to the private sector, including best practices to better manage cyber threats where standards apply.

In order to understand not only the domestic, but also regional and international legal mechanisms at play in regulating cyberspace and enhancing cyber-security, it is relevant to analyze the possible applicability of international law that could fit the purpose. Certainly, for a policy vision, market, laws, norms, codes, standards, voluntary instruments have a major role to play within a polycentric framework applicable to cyber-attacks.

The combination of law and policy for our analysis is key to understanding if multi-regulatory governance can improve cybersecurity in the Arctic. This could easily turn out to be "critical" for future enactment of technical, economical, legal and policy lessons. It is relevant to understand if the current multi-regulatory system of regimes (law) in combination with institutional analysis of the main actors involved (policy) can help to improve a cyber space in the energy sector, under ECIC climatic conditions, as it will be outlined in the next section.

3.1. International Law and the Main Institutional Actors Involved

The role of international law is important in maintaining the security of the Arctic in the EHN cyberspace in the face of threats of different nature and under different conditions, for example, during war time relating to the use of force (*jus ad bellum*) or during in peace time (*jus in bellum*).The objective of this sec-

[65]Ostrom, E. (2012b). A General Framework for analysing sustainability of social-ecological systems.

tion is to identify which are the different international law regimes applicable to the cyber threats to critical infrastructures with focus on the energy sector and their capacity to improve Arctic cyber-security.

Practitioners, policy-makers, and academia have recognized that there is a need to develop a legal and political framework against cyber-threats to critical infrastructure in general, and not only specifically for the regional level of the Arctic. Such a framework does not exist. The existing international law applicable in the EHN countries to cyber security is very fragmented with the absence of specific provisions pertaining to the cyber component typifying cyber threats that can be regulated and applied. It is extremely complex and uncertain if the provisions of the existing treaties that will be presented in this section, could become applicable to cyber-threats situations, not only for the subject matter but also because there have never been any cyber-attacks in the Arctic, and in the EHN targeting critical infrastructure in the energy sector until now. However, it is possible to include in the scope of the applicable international global treaty law, and by legal reasoning *per analogia*, the typified acts of cyber-threat that might occurring in the Arctic. Nevertheless, it is not possible to ascertain the applicability of the law with a logical theoretical exercise alone but only with the experience as well. A true understanding will come after the unfortunate event.

The legal framework under *jus ad bellum* conditions to manage cyber-attacks to critical infrastructure in the Arctic is very fragmented and it is the one covered by the Law of Armed Conflict (LOAC), the law of the United Nations (UN) Charter, cyber space law, the law of state responsibility, international humanitarian law, international criminal law, international law applicable to terrorism, human rights law and IT law. Specifically, several treaties could apply, such as the UN Treaty, relevant treaties of space law, the International Criminal Court Treaty, the Montreal Convention for the Suppression of Unlawful Acts against Safety of Civil Aviation of 1971, and the International Covenant on Civil and Political Rights (ICCPR).[66] As a valuable complement to understand and asses the international law applicable to cyber-threat, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation (hereinafter the Tallinn Manual 2.0)[67], an updated version of the Tallinn Manual 1.0, has produced extensive analysis.

The LOAC has opened up a debate among those who maintain that it could be easily applicable, especially to *jus ad bellum* conditions. Others advocate the

[66]International Covenant on Civil and Political Rights (ICCPR), Doc. E, 95-2, (1978), 999 U.N.T.S, entered into force on March 25, 1976.

[67]See Schmitt, M. & Vihul, L. (2017). Tallinn Manual on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. Tallinn Manual 2.0 is the new version prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence which is replacing the old version of this manual published in 2013 (Tallinn Manual 1.0).The Tallinn Manual 2.0 on the International Law applicable to Cyber Operations had made a significant contribution to clarifying the application the possible application of international laws related to cyber uses of force and armed conflicts involving cyber operations.

need for a new regulatory structure, such as a treaty. A third category even denies the usefulness of international law. However, the applicability of international law and in particular of *jus ad bellum* is ascertained.

The UN Charter is the most relevant instrument applying to cyber-threats because it lays down important principles and rules guiding the relations between states and establishes a collective security system. Thus, if the Security Council (SC) determine that there is a threat to peace and security, it can adopt military as well as non-military measures in order to maintain or restore peace and security.[68] The frequency of cyber-attacks on state infrastructures especially when the targets are communications or energy facilities or energy structures that can both represent civilian and military targets, have pushed states to consider them as "military attacks" and therefore requiring interpretation according to Art. 5 of the NATO treaty. This means engaging its collective self-defense mechanism in support. In that respect, in the Estonian case of 2007 for example, Estonia argued that the cyber-attacks against its country required engaging its collective and armed attack, within the meaning of Art. 5.

However, NATO refused to engage Art. 5, and did established instead a Cyber Defense Centre of Excellence (CCDCOE) in Tallinn (Estonia) in order to enhance cyber security for NATO Member States. The *raison d'être* of the CCDCOE was thus that cyber-security can be best achieved through military means, which lead the Centre to publish the Tallinn Manual which represents to date, especially in its very recent second and latest version published in the current year, the most important framework of international law applying to cyber-warfare and specifically to attacks on critical infrastructure.

However, the legal uncertainties and disagreement among over the precise definition of "attack" still persist and the different nuances on what constitute and "attack" in this manual are numerous, especially when it is a question of establishing the threshold for when an attack should be viewed as the equivalent of an armed attack under international law because such a threshold is unknown.[69]

The manual does not offer a solution either for when critical infrastructures are strictly interconnected with military ones and the damage is unpredictable and uncontrollable. Nevertheless, the manual prove the existence of applicable customary norms and represents a valuable applicable instrument.

In addition, also space law applies because outerspace is similar to cyberspace and they both deal with territorial and extraterritorial components. Like weapons systems that have been developed to attack satellites, cyber-attacks could have a large-scale strategic impact. This means that among conventions covering

[68]The UN Charter can address many facets of cyber-threats, for example cyber-threats that amount to a use of force or to an armed attack, as well as those that constitute a threat to, or a breach of, international peace and security.

[69]Schmitt & Vihul (2017). Tallinn Manual 2.0, on the International Law applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. Rule 92 Definition of cyber-attack, 415-420; Schmitt, N. M. (2017). Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. Harvard National Security Journal, 8, 245.

infrastructures those concerning civil aviation may be the most relevant models to follow.[70] Furthermore, laws covering acts against aviation infrastructures are very effective.[71]

In that respect, the 1967 Outer Space Treaty (OST)[72] which laid down the foundations for cyber space governance, can be applied to cyber-security regarding critical infrastructure, as well as the treaty on principles governing the activities of states in the exploration and use of outer space, including the Moon and other Celestial Bodies.[73] In that sense, space and telecommunications systems are in that sense strictly interconnected.

State responsibility remains also a key component in dealing with an attack on critical infrastructures in general, and specifically for the Arctic security. Threats also arise from states that may constitute violation of the state's conventional or customary international law obligations. The matrix of state responsibility founded the conditions according to which states can be held directly or directly responsible for activities of its own organs. The law of war requires that a state must identify itself when it attacks another state under *jus in bello* according to the International Law Commission's Draft Articles on the Responsibility of States for International Wrongful Acts. Also the international humanitarian law applies during an international or non-international armed conflict, and contains provisions concerning the protection afforded to persons caught in the armed conflict. The applicable international conventions are the Hague Regulations of 1899 and 1907, the four Geneva Conventions of 1949 and their two Additional protocols of 1977 including all the principles of humanitarian law. International criminal law applies when one of the four core crimes are committed using cyber means: 1) aggression, 2) genocide, 3) crimes against humanity and 4) war crimes, Also international law applicable to terrorism can be applicable in the case of cyber-attack to critical infrastructures. In that sense the relevel applicable convention is the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)[74] and the 1988 Convention for the Suppression of Terrorist Bombings.[75] In addition, there are a number of international treaties on human rights that can be applied such as the ICCPR as

[70]Goodman, S. (2008). Critical Information Infrastructures Protection: Responses to Cyber-terrorism, Centre of Excellence Defense Against Terrorism, Ankara, Turkey Editions, IOS Press, 32.

[71]Example of Civil Aviation Conventions applicable to critical infrastructures are the Civil Aviation Convention of 1944 and 1963.

[72]Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, which is a treaty that forms the basis of international space law. The treaty was opened for signature in the United States, the United Kingdom, and the Soviet Union on 27 January 1967, and entered into force on 10 October 1967.

[73]Shackelford, S., J. (2014). Managing Cyber Attacks in International Law Business, and Relations in Search of Cyberspace: An Introduction to the law of Cyber War and Peace. Cambridge University Press, 274.

[74]Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, (Montreal Convention) 1971.

[75]International Convention on the Suppression of Terrorist Bombing on 15 December 1997.

mentioned above, but also the European Convention on Human Right (ECHR),[76] and the Inter-American Convention on Human Rights.[77] Finally, International Communication Law is relevant. It was in many circumstances the precursor to cyber law. In that sense, the Convention applying is the International Telecommunication Union Convention against "harmful interference" more concretely it's Annex 3 stating that: "*anyone that endangers … safety services, or seriously degrades, obstructs or repeatedly interrupts a radio communication service …*" The safety services include technologies, human life and property including critical infrastructures and energy plants. Nevertheless, there are no mandatory enforcement mechanisms.

With regards, to the law applicable under *jus in bellum*, it is always difficult to understand if an attack should be viewed as the equivalent of an armed attack under international law because the threshold for when it is considered as such is unknown. Some authors have argued that an attack could be considered as an "armed attack" when comparable to the effect of a nuclear weapon.

Several bilateral and multilateral agreements are applicable to secure the cyber space of Arctic critical infrastructures specifically for the protection of the energy sector. In that respect, some of the most important instrument when it comes to criminal offences, are the European Council Convention (better known as the Budapest Convention),[78] the United Nations Convention on the Law of the Sea (UNCLOS),[79] and the dozen of Multilateral Legal Assistance Treaties (MLTA)[80] that could be used to seek criminal prosecution of cyber-attacks that either specifically mention IT or are broad enough to cover all law enforcement investigations.[81] In addition, also the International Maritime Organization (IMO) treaty,[82] the International Convention for the Prevention of Pollution from Ships (MARPOL),[83] the already mentioned Arctic Search and Rescue Agreement (SAR Agreement)[84] and the 2013 Oil Pollution Agreements,[85] can be taken into ac-

[76]European Convention on Human Rights (ECHR) (formally the Convention for the Protection of Human Rights and Fundamental Freedoms) is an international treaty to protect human rights and fundamental freedoms in Europe. Drafted in 1950 by the then newly formed Council of Europe, the convention entered into force on 3 September 1953.

[77]American Convention on Human Rights, also known as the Pact of San José, is international human rights. It was adopted by many countries in the Western Hemisphere in San José, Costa Rica on 22 November 1969.

[78]The Council of Europe Convention on Cyber-Crime of 2001, entered into force on the 1 July 2004).

[79]United Nations Convention on the Law of the Sea, Dec. 10, 1982. The Convention has been ratified by many countries except for the United States. The United States has refused to ratify the convention because of the deep-sea bed mining provision.

[80]A mutual legal assistance treaty (MLAT) is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

[81]With regards to the Multilateral Legal Assistance Treaties (MLAT) it is worth noticing that Norway does not have a MLAT with the US.

[82]International Maritime Organization (IMO), known as the Inter-Governmental Maritime Consultative Organization (IMCO) until 1982.

[83]International Convention for the Prevention of Pollution from Ships (MARPOL, 73/78), 1973 as modified by the Protocol of 1978.

count for their possible applicability.

As previously mentioned, one of the most relevant international criminal law treaties applying is the European Council Convention on Cybercrime that aim to establish a common criminal policy among parties by adopting appropriate legislation and by fostering international cooperation. States investigate on certain offences and cooperate on the investigation and prosecution of such offences. The Convention requires states to criminalize illegal access, interception, data interference and system interference including energy power infrastructures. Russia, which is an Arctic country, deliberately withdrew its signature from this treaty.

An interesting parallel that can be traced is with the one between the law of the sea and cyberspace, especially with the UNCLOS. Several provisions of the UNCLOS are potentially applicable to the cyber-security of critical infrastructure in the energy sector such as for example, Article 19 and Article 113.[86] Article 19 states that states should not use another nation's territorial sea to engage in activities prejudicial to the peace, good order, or security of coastal state. This includes the collection of information, distribution of propaganda, or interference with any system of communications. Article 113 requires domestic criminal legislation to punish willful damage to submarine cables. Article 19 should be also applicable to Article 21 and 113 claims involving submarine cables because this would include also cyber attackers who send code through submarine cables to a costal state, thus breaching of UNCLOS.[87]

The MLAT agreements could be used to seek criminal prosecution of cyber-attacks given that they include IT and cover all the enforcement. Several Arctic Countries are part of these conventions, specifically, Sweden, Finland and Norway. Even though these Arctic countries are part of the MLAT it does not regulate only among the Arctic states themselves but rather stipulates agreements with non-Arctic states. After examining the IMO treaty, the MARPOL, the International Convention for the Safety of Life at Sea of 1974, the SAR Agreement and the 2013 Oil Pollution Agreement that can be applicable to cyber threats on critical infrastructure in the energy sector of the Arctic states, it is ascertained that there are no provisions that could be applicable to cyber-threats under ECIC in the EHN countries.

From all the above, it is clear that international law shows evident imperfections and does not cover the situation of cyber-threats under ECIC conditions in

[84]The Arctic Search and Rescue Agreement (formally the Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic) is an international treaty concluded among the member states of the Arctic Council—Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden and the United States—on 12 May 2011 in Nuuk, and Greenland.

[85]Agreement on Cooperation on Marine Oil Pollution Preparedness and Response in the Arctic (signed 2013).

[86]Hathaway, O. A., et al. (2012). The Law of Cyber Attack. Yale School, California Law Review, Paper 3852, 817-885.

[87]Schackelford, S. J. (2014). Managing Cyber Attacks in International Law Business, and Relations in Search of Cyberspace—An Introduction to the law of Cyber War and Peace. Cambridge University Press, 6, 282-283.

the EHN area. Even if there are norms of customary law, the current *jus ad bellum* and *jus in bello* that are theoretically able to accommodate this new type of threats, existing norms leaves uncertainties and gaps that are dangerous to leave without the cogent development international law. Despite, the applicability of the Budapest Convention, the 2.0 Tallinn Manual and some provisions of UNCLOS, and the possible application of space law and IT treaties, there is an urgent need to develop a regulatory patchwork of precise instruments mixed that can be applicable to protect ECIC in the EHN area.

The question is which actors would enact new law applicable to ECIC in the EHN countries and succeeding in fulfilling in the gaps and imperfections of the current existing fragmented framework. International law is inseparable from state's behavior and international organization's activities. In the context of the existing framework applicable under ECIC in the EHN, it is therefore, relevant to identify the role of international organizations, as well as non-state actors in the applicability of norms. These actors are crucial for decision-makings and for providing both hard and soft law instruments that guide state's behaviors and the enforceability of conventions, as well as and for filling international law's gaps and reinforcing mechanisms of collective behavior.

A notable example, in that sense is the UN with the UN Security Council (UNSC) which imposes a spectrum of measures (under Chapters VI and VII of the UN Charter) ranging from sanctions to authorizing the use of force against violation of international law. The Security Council can decide whether its decisions bind all members or only certain states, even though all countries are expected to act accordingly with mutual assistance and cooperation. The UNSC relies on regional agencies, states and regional coalitions or military organizations, such as NATO in their capacity to enforce its decisions under the Chapter VII of the UN Charter. In that sense, the Tallinn Manual foresees similar arrangements in case of cyber-attacks to critical infrastructures, which also applies in case of cyber-attacks under ECIC. NATO has therefore a constructive role to play and assisting regional organizations and states in case of cyber-attacks, not only among the parties which includes the Arctic States, except Finland and Sweden which are not a member of NATO, but also in cooperating with non-member states. In particular, NATO today, is cooperating with Russia and China. NATO's aim is thus not to create new laws in general, and in particular laws that could be applicable under ECIC conditions in the Arctic, but rather a role of interpretations of the existing norms, which tends to favor only the alliance members. Therefore, in order to avoid NATO continuing to exploit imperfections and gaps of the existing international law, it is prudent that the UN supervise, any NATO's interpretation of existing laws protecting ECIC in the Arctic.

Another actor, that should be considered in the case of cyber-attacks to critical infrastructures in ECIC areas is the Arctic, is Arctic Council (AC). The AC is the principal cross-sectorial intergovernmental forum for the Arctic region but military security issues are excluded from its activities and mission. Founded in 1996, the AC keeps predominantly an environmental agenda.

Nevertheless, this does not impede that in the future this institution could broaden its agenda to include co-operation agreements that include military activities, defense and security issues including cyber-security as part of the concept of human security. In the Arctic region there a cyber-security forum able to negotiate targeted measures that address common problems, more importantly problems related to ECIC, is missing. Such a forum should have a global potential, not only regional as cyber-threats are transnational and do not know any boundaries. Memberships should include also the US and its close NATO and non-NATO allies that a share common vision for Internet governance and cyber-security. Hence, cyber-threats should be addressed protecting the security of Polar regions through international law and not only political talks. This is a pertinent issue to deal with for international law. The parties of the AC could manage conflicts and enhance cooperation by dealing with these issues in unison.

Finally, the EU is another relevant actor in cyber-security protecting norms, values, fundamental rights, democracy and rule of law to protect cyberspace. In 2013, the EU adopted, the Cyber-security Strategy of the European Union, adopted jointly by the European Commission and the High Representative. The EU refers to cyber-security as an obvious "Digital Single Market".

Cybersecurity for the EU forms parts of what is called "Common Security and Defense Policy (CSDP) forming the basis of the EU external security action. The EU has the ambition as a global actor to link internal and external policies, and has therefore, enacted, a series of acts of secondary law, which will be examined in the next section.

3.2. Regional Law at the EU Level

European cyber-security policy is formulated and implemented in a multi-stakeholder structure where legislation is both private and public and actors are interacting with each other. The European cyber security is connected with both international developments and domestic implementation sphere.

ECIC's cyber-threats in the EHN countries are covered by EU legislation. The EU level structure of cyber security also involves the private sector and experiences from private companies. For example, the established European Network and Information Security Agency (ENISA) seek to reinforce and coordinate capabilities of the Computer Emergency Response Plans (CERP) conducts regular emergency drills and has developed the Information Sharing and Alert System (EISAS) to guard against attacks on critical infrastructures. ENISA has also established a comprehensive guide to public-private sector cooperation, which is called the "Partnership for Resilience" (EP3R) with the aim to improve government capabilities through private expertise and thus produce legislation that protects private firms from cyber threats.

The EU level has a rather wide set of regulation, strategies and policies, dealing with cyber security in the context of critical infrastructure. First and foremost, there exists the European Programme for Critical Infrastructure Protec-

tion (EPCIP). The concept of Critical Infrastructure Protection (CIP) is a recent area of EU interest which was non-existent prior to the 9/2011 attacks. Despite the impact of natural disasters on infrastructures was informally discussed in the aftermath of the 2004 Indian Ocean tsumami.[88] Hence, it was only after 9/11 in the US, that the concept of Critical Infrastructures (CIs) and its CIP became more widely prevalent also in Europe, first via NATO, and soon thereafter also within the EU. After the 2004 Madrid and 2005 London terrorist attacks, the EU debate culminated in the development of the EPCIP and its corresponding act of secondary legislation: Directive 2008 on the Identification and Designation of European Critical Infrastructures (ECIs).[89] Yet, the Council Directive from 2008 on CIP[90] never became a success.

The 2008 Directive aimed to formulate a common procedure for designating CIs in Europe and a common approach to improve resilience. It requests member states to identify ECIS, starting from the energy and transport sectors, and offer non-binding guidelines for the listing process.

According to the Directive, that part of CI—and only within two sectors, energy and transport—that is defined and designated as European Critical Infrastructure (ECI), is to be defined and designated by a Member State, and the identity of this ECI remains secret. Only a few Member States have chosen to use the option to designate categories of CIs as they do not want to be regulated. Member states do not want to proceed in designating and defining critical infrastructures because this would entail not so much to protect CIs but instead put it at risk because there would be too much information put into circulation.[91] Thus, most of the Members States have not defined or designated any ECI, because they do not need to. Even those who have, they have defined and designated some few close-to-border CI, like power stations or grids that provide services across borders.

According to the Directive, this means that one has to have a preparedness plan following a certain EU Commission template. As these ECI are not only rather randomly selected or nominated, but also secret to almost anyone, the visible effect of the EPCIP is very low. What is left, then, is that the EPCIP provides member States some kind of financial support to secure national CIs.

A report of the UK house of Lords argued that the designation of many categories of sensitive infrastructures as ECI would, because of wide sharing of information entail not protecting critical infrastructures but actually potentially

[88]Interview conducted by Javier Argomaniz with Council Secretariat official, DG I Civil Protection Unit, January 2006, in Argomaniz, J. (2013). The European Union Policies on the Protection of Infrastructures from Terrorist Attacks: a Critical Assessment. Intelligence and National Security, Routledge, 262.

[89]For a detailed discussion, see Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection. Journal of European Integration, 31, 6, 721-739.

[90](European) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[91]Argomaniz, J. (2013). The European Union Policies on the Protection of Infrastructure from Terrorist Attack: A Critical Assessment. Intelligence and National Security. Routledge, Francis and Taylor, 264.

put it at risk given the possibility to divulgate very sensitive information.[92] This turn to be a problem as the lack of trust is an additional alibi for the Member States. This is also because per definition, a directive, gives considerable room for manoeuvre to national governments to avoid complying with their duties and obligations, in the case in point, by simply producing a minimal list of designated ECIs or failing to enact rules on private actors or national authorities that have to take measure to implement the Directive. This entails that a key principle running through EU actions is the subsidiarity principle and that cyber-security is definitely an area where member states are reluctant to delegate legislation to the EU. Nevertheless, CIPs are transnational in nature and have a transnational impact of some natural and man-made disasters. There is a tension here between the notion of national sovereignty versus trans-border character of ECIs and member states are irritated to delegate power to the EU but at the same time conscious of the need to enhance cross-border cooperation.

More indirect but perhaps in the longer term more effective tool has been the European Reference Network for Critical Infrastructure Protection (ERNCIP). It is based on *voluntary expert cooperation* between the member States, coordinated by the EC. The aim is to contribute to *standardization* of protection and resilience measures within different CI sectors, including cyber threats against industrial automated control systems.[93]

There exists naturally a rather large body of international information and cyber security related *standards*, most notably the International Organization of Standardization (ISO) *27000 family of standards*, the latter alone comprising of almost 50 *standards* or their classification[94].

However, the EU has its own normative framework too even if fragmented.[95] In terms of legislation, the most important one is Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.[96] It regulates information system security of two types of entities, namely operators of "essential services" and "digital service providers". The former is essentially the same as critical infrastructure operators.

The term is defined in the directive as an entity that provides a service which is essential for the maintenance of critical societal and/or economic activities, the provision of which depends on network and information systems, and where an incident would have significant disruptive effects on the provision of that service.

[92]UK, House of Lords. (2010) Protecting Europe against Large-scale Cyber-attacks, HL Paper 68, London: HSMO.

[93]See https://erncip-project.jrc.ec.europa.eu/.

[94]International Organization of Standardization, *ISO 27000*. Available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/.

[95]The EU normative framework applicable to cyber security in the Energy Sector is an extremely fragmented and incoherent framework which depends on Member States capacity to implement and it is first and foremost based on acts of secondary legislation that give freedom to Member States on complying with obligations and freedom to the national authorities at local level and it is thus very much delegated in the hands of national responsibility.

[96]Directive (EU) 2016/1148 of The European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194/1, 19.7.2016.

The Directive states that the essential services operators should be regulated by national legislation taking into account country-specific and sectorial idiosyncrasies, whereas the digital service providers, which are more of cross-border character, are regulated in more harmonised manner by the Directive.

However, also the essential services operators should respect the minimum requirements set by the EU legislation and when the services have a cross-border character, the regulation should be agreed with respective countries. The Directive obliges the Members States to identify both the essential services operators and the digital service providers, to establish a national authority for information (cyber) security, and it defines the cooperation bodies where the Member States harmonize their approaches with each other.

More important however in the field of cybersecurity is, the previously mentioned ENISA. It coordinates cooperation in this field and publishes *pre-standards*, *guidelines* and *fact-based reports* on ICT vulnerabilities. As a suitable example in our context, one might mention *Communication network dependencies for ICS/SCADA Systems*.[97] This rather comprehensive report is essentially a generic but still rather detailed *risk assessment* or *risk assessment guideline*, with gap analysis part and normative recommendations for risk treatment, which gives a good ground for the critical infrastructure operators to build their own systems.

During the last review of EPCIP, it was discussed that Information and Communication Technology (ICT) should be added to the EPCIP Council Directive along energy and transport. Moreover, the focus of CIP should become more cross-sectoral and instead of focusing only on protective measures, one should pay more attention to resilience that is not only withstanding threats but also recovering from materialized crises rapidly. "From the point of view of energy supply, for instance, this would involve the energy, transport, and ICT sectors."[98]

However, ICT is included in many other policies of the EU, and most notably formulated in the *EU Cybersecurity Strategy* from 2013. It does not propose any supranational model, but emphasizes the need for national legislation, which challenge is to overcome the fact that private actors still lack effective incentives to provide reliable data on the existence or impact of incidents, to embrace a risk management culture or to invest in security solutions. This, it is said, is especially important in a number of key areas: energy, transport, banking, stock exchanges, and enablers of key internet services, as well as public administrations.[99]

Last year, in February 2017, the Energy Expert Cyber Security Platform EECSP—Expert Group, has issued an important report[100] to provide guidance to

[97]European Union Agency for Network and Information Security—ENISA. (2017). Communication network dependencies for ICS/SCADA Systems. Available at: https://www.enisa.europa.eu/publications/ics-scada-dependencies.

[98]European Commission Staff Working Document on the Review of the EPCIP, Brussels, 22.6.2012. SWD (2012). 190 final, 8.

[99]EU Cybersecurity Strategy (2013). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013), 1 final, 12.

the EU Commission on policy and regulatory directions at European level addressing the energy sector key points including infrastructural issues, security of supply, smart grids technologies and nuclear. According to this report, under the lead of DG Energy, the EU Commission is preparing, a strategy on cyber security for the whole energy sector to reinforce and complement the implementation of the NIS Directive and also to foster synergies between the Energy Union and the Digital Single Market agenda. A common approach to address cyber threats across Europe, building on the existing Cyber Security Strategy at the EU launched in 2013, is still missing.

In particular, the EECSP—Expert group has identified 39 gaps not covered by existing legislations. Most importantly the absence of a formalized and effective threat and risk management system, especially concerning how to identify operators of essential services for the energy sector at EU level[101] has been acknowledged. In this regards a harmonization criteria for the identification of operators of essential services is not available nor is as a consistent set of commonly accepted criteria for the identification of the energy essential operators which is missing.[102]

In addition, another relevant existing gap, needs to be filled in order to improve cyber resilience in the energy sector[103] and the willingness of different stakeholders to cooperate and collaborate in this effort especially when they operates in cross-border interconnected energy network in order to manage the "cascading effect"[104] across regions. The electricity grid and gas transport pipelines are strongly interconnected across Europe. The cascading effect could be serious, as demonstrated in a major European blackout in 2006.[105]

Another gap to be filled at EU level is the handling and governance of crisis management. Crisis management depends strongly on communication capabilities for example between operators and governmental authorities. In particular, a successful handling of crises depends on ensuring a clear and well-functioning description of roles and responsibilities as well as insuring that communications between roles and responsibilities parties is working well.

Other relevant gaps identified in the report concerns information sharing on threats, risk and vulnerabilities that are not well defined and designed and lack-

[100]Report, Cyber Security in the Energy Sector – Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector-Energy Expert Cyber Security Platform, (2017) 1-71.

[101]Report *Cyber Security in the Energy Sector—Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector.* Energy Expert Cyber Security, Platform, 2017, page 9.

[102]Report, *Cyber Security in the Energy Sector—Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector. Energy Expert Cyber Security Platform*, (2017). 53.

[103]Report, *Cyber Security in the Energy Sector—Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector.* Energy Expert Cyber Security Platform, (2017), 10-11.

[104]For an understanding of the concept of "cascading effect to CIs", see section 1 (introduction) of the present article.

[105]See the European blackout. (2006). At https://en.wikipedia.org/wiki/2006 European_blackout.

ing from a common applicable classification scheme.

This means that the EU lacks a clear cyber response framework including 1) classification of attacks 2) definition of responsibilities and capabilities needed to respond adequately on different level of cyber-attacks, 3) cooperation and information sharing between the attacked organization, Member States, Nations States, EU, OSCE, NATO and international alliances.[106]

There is still pending work in designating and defining infrastructures that are critical and define under which set of circumstances is a challenging step because there is no absolute definition but only vary degrees of criticality which can even change due to technologic development.

3.3. Domestic Law and Policy with Norway

In the Norwegian national context, there is a growing body of regulative acts, strategies, guidelines, action plans and respective policies aiming at securing critical infrastructure from cyber-attacks., Mostly official documents speak about information security rather that cyber security, and the scope is therefore wider than merely preparing for cyber security attacks.

3.3.1. Law and Regulations

The so-called Security Law on preventive security measures from 1998 (lastly amended in 2016)[107] defines the responsibilities and rights of the Norwegian National Security Authority (NSM), established only in 2003, which is a cross-sectoral professional and supervisory authority within the protective security services in Norway, especially focusing on information security. According to the mandate, the purpose of protective security is to counter threats to the independence and security of the realm and other vital national security interests, primarily espionage, sabotage or acts of terrorism. The law also discusses information security in one article, Article 4 with several paragraphs. It defines the security grades for different type of information, the responsibility to secure the sensitive information, the authority control over the sensitive information management, including the equipment and encryption systems, monitoring the security, including the right, with consent of the function owner, for the NSM to hack the information systems in order to find vulnerabilities. The law was detailed in the Regulation on Information Security from 2001[108], including the basic security principles, management system, technical minimum requirements, and so forth.

As to the energy field in particular, the so-called preparedness regulation concerning power production from 2012 contains an article which is Article 6 on information security. It includes sections on identification of sensitive infor-

[106]Report, Cyber Security in the Energy Sector—Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector-Energy Expert Cyber Security Platform, 2017, 52.

[107]Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), LOV-1998-03-20-10, Sist endret LOV-2016-08-12-78 f, Forsvarsdepartementet 1998/2016.

[108]Forskrift om informasjonssikkerhet (av 1. juli 2001 nr. 744).

mation, which refers to information that might damage installations or affect features that affect the power supply, such as vulnerabilities and location of critical equipment. It does not include any explicit regulation concerning a cyber-attack, rather that one receive sensitive information that can be used for other type of malicious attacks.

In that sense the Norwegian model has strong potential to be used as a source of inspiration in the design of a future information sharing scheme on threats, risk and vulnerabilities for the EU level. Presently, the EU regulatory level such a scheme is not defined and designed. The EU regulatory level is also lacking a common applicable classification scheme as explained in the previous section.

3.3.2. Strategies and Actions Plans

Norway's governments third and latest "National strategy for information security' is from 2012 (preceded by and based on the first and second strategies of 2003-2006 and 2007-2010 respectively as well as the proposal for "Cyber security strategy)."[109] The 2012 strategy starts with the statement that ICT is a cross-sectoral "strategic security challenge" that "has become critical for the society to work normally", thus embedding critical or vital societal functions and respective infrastructure as well as their interactions.

While the overall coordination role is with the government, the strategy defines a hierarchy of the variety of actors and their respective roles and responsibilities. First, each function bears the main responsibility, following the Norwegian so-called *responsibility principle* explaining that the actor who has responsibility in normal conditions should also bear responsibility in a crisis situation. "In practice, this means that the responsibility lies with the owner of a function, no matter it is located in the public or private sector." Larger security measures however are prepared in cooperation of the owner of a function and respective public agencies. The specific ministries or departments are all responsible for their sector's critical infrastructure security, in terms of identifying the critical functions and infrastructures, as well as evaluating, planning on the strategic level, the prevention, preparedness and response measures, as well as monitoring cyber security in the agencies that are subordinated to them. In practice, these agencies are responsible for the respective actions as they know their functions the best. Four ministries, namely the Ministry of Justice and Preparedness, the Ministry of Government Administration, the Ministry of Defense, and the Ministry of Transport and Communications, are singled out as particularly being responsible for cyber security.

The strategy then outlines on generic level, the actions that should be taken. They include: developing a holistic and systematic approach towards cyber security; making the cyber security dimensions related to vital societal functions more robust; coordinating the cyber security measures in the public administration; developing the warning and response systems towards cyber threats; en-

[109]Nasjonal strategi for informasjonssikkerhet, Fornyings-, administrasjons-, og kirkedepartetement (on behalf of the Government of Norway (2012).

hancing the prevention measures; putting continuously resources to competence and capability building; and securing high-level national research related to cyber security.

The strategy was accompanied some years later with an Action Plan on Information Security 2015-2017[110], which however covers only public administration. Information Security and related crisis management should be organized in the same way as Norway's general crisis management system, based on four principles. First, the *responsibility principle* implies that the agency who is in charge of a sector or issue in normal situation, is also responsible for handling extraordinary events. Second, *equality principle* means that the normal daily organization structure should be kept as much as possible similar also in extraordinary events. Third, the *subsidiarity principle* tells that extraordinary events should be handled at a lowest level possible. Finally, the *cooperation principle* requires that each authority, function or agency has to take its own responsibility to organize the best possible cooperation with all relevant actors in prevention, preparedness and response to extraordinary events. The Action Plan then defines basic tasks related to six areas: management and control; risk management; security in digital services; digital preparedness; national common components (instead of each sector building its own security systems); and knowledge, competence and culture.

In the substance all these elements of the Norwegian model, based on the four principles of the crisis management system contained in the Norwegian Action Plan on Information Security, are well suited to be taken into consideration as a source of inspiration to fill the EU regulatory gaps on crisis management system, exposed in the previous section.

3.3.3. Critical Infrastructure and Vital Societal Functions

Like its Nordic neighbours, Norway also chose to speak about critical or vital societal functions rather than just critical infrastructure. Already in the early Norwegian approach from 2006—called "Protection of Critical Infrastructures and Critical Societal Functions in Norway"[111]—both the concept of infrastructure and that of function were included as elements at different levels. Critical societal functions formed a more general level, being dependent on but also encompassing infrastructures. The hierarchical idea was that society's basic needs are covered by critical societal functions, which depend on infrastructures, whose criticality is assessed according to three criteria: 1) *dependability*, in that a high degree of dependability implies criticality; 2) *alternative*s, in that few or no alternatives imply criticality; and 3) *tight coupling*, in that a high degree of tight

[110]Kommunal-og moderniseringsdepartement, "*Handlingsplan for informasjonssikkerhet i statsforvaltningen* 2015-2017", Norway, Oslo (2015).

[111]Justis-og politidepartementet, *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Innstilling fra utvalgoppnevnt ved kongelig resolusjon 29. oktober 2004, Avgitt til Justis-og politidepartementet 5. april 2006, NOU Norges offentlige utredninger 2006: 6. Departementenes services enter Informasjonsforvaltning, Norway, Oslo.

coupling or linkage within a network implies criticality. This approach forms the basis for deciding whether any given infrastructure is critical or not. In practice, the approach makes it possible to limit the extent of the CI considerably, because not every part of, say, an electricity grid or a transport system is necessarily considered critical, which is the case in the EU approach at the conceptual level. Therefore, this important idea contained in the Norwegian approach turn to be extremely inspiring for the EU in order to fill the gap of the total absence of criticality in the notion of "critical infrastructure" as explained in the previous section.

In a 2017 report by the Norwegian Directorate for Civil Protection (DSB), titled "Vital functions in society, it was discussed which kind of functional capabilities must society maintain at all times.[112] The term "vital societal functions" is defined and the functions are listed and categorized. The term is reserved for "functions that society could not cope without for seven days or less without this threatening the safety and/or security of the population". The term is further divided into three broad categories: governability and sovereignty; security of the population; and societal functionality. Listed under these categories are the functional areas and assets that are usually brought up in critical infrastructure discussions, such as the government and other administrative bodies, the emergency services, essential utilities such as energy and water, and so forth. It is noteworthy that the very term "critical infrastructure" is not mentioned at all, with the term "infrastructure-based services" being used instead. In the report, cyber (or ICT) security is a horizontal concept, but there is a short section about it in particular. It is mentioned that it is important to have the ability "to detect information security incidents, limit damage and rapidly restore normal operation in registers and systems with vital societal functions and/or which include confidential personal data", and that it "is essential for every system owner to be capable of detecting unwanted incidents as soon as possible in order to limit damage and restore system functionality and security".

3.3.4. Risk Assessments

The most recent "National Risk Assessment" was prepared by the Norwegian Directorate of Civil Protection in 2014.[113] It emphasizes that attacks against SCADA systems may paralyses or destroy power production, power transmission, refineries, water supply, treatment plants, transport and oil platforms, as well as reveals a lot of sensitive and classified information for unauthorized parties. The Risk Assessment refers to plans and materialized threats specially designed to take control of SCADA systems in Norway, related to espionage, sabotage and terror. The bottlenecks include the enterprises policies, not taking the risks seriously enough, not having the needed security organization at place, and relying on outdated security technology, and all in all not introducing the proper risk-reducing measures. The National Risk Assessment discusses particularly

[112]Norwegian Directorate for Civil Protection, Vitalfunctions in society. What functional capabilities must society maintain at all times? (2017), Norway, Oslo.

[113]National Risk Analysis (2014). The Norwegian Directorate for Civil Protection (DSB), Norway, Oslo, 183-202.

two malicious attack scenarios under the concept of "cyber space". These are Cyber Attack on Financial Infrastructure and Cyber Attack on Electronic Communications Infrastructure. These scenarios are discussed in rather detailed way on the axis of likelihood, on the one hand, and consequences, on the other hand. In the first scenario, the likelihood is estimated as "low" while the average consequences would be "large", the second worst score. When it comes to specially the consequence sub-group of "societal stability", including social unrest and effects on daily life of the population, the consequences would be "very large. As to the second scenario, the treatment differentiates risks similarly within different consequence fields, such as power, roads, air, sea, civil protection and so forth.

When it comes to power, the risk is considered lower than in many other fields due "the power plants" own closed process and communications network", however, while there would follow "delayed repair of local outages due to external communication problems with customers and suppliers". The overall assessment is again estimated as "low" in terms of the likelihood and "large" in terms of consequences, however, the latter scoring most dramatic in the fields of economic losses and social stability. The Government's official report on Digital vulnerability from 2015[114] adds to this analysis. This is a rather detailed report of over 300 pages, covering most issues discussed above. When it comes to securing critical infrastructure, the report discusses this under the subissue of "robustness of infrastructure", where the answer to the threat is basically redundancy of the vital infrastructure services and their distribution routes. When it comes to power production and distribution, the report follows the DSB evaluation and considers that the risk from the electronic communication sector to power sector is rather low due to the closed and redundant networks that this sector utilizes.

National Security Authority (NSM) in turn published in 2016 its second Holistic Risk Picture[115], focusing on information and communication technology. This document classifies the threats and vulnerabilities, and builds a risk picture on that basis, and then proposes the needed counter actions. The report however is very generic in spirit, more typological than data-analysis based risk assessment. As to critical societal functions and infrastructure, one can find the following statement about the source of threat: "Attack against societal functions seem to be linked to potential conflict situations with foreign states."[116]

3.3.5. The Norwegian Arctic and Cyber-Threats

Moving to the Arctic conditions, most of the threat pictures in the national risk assessments are valid. However, some specific issues might make the critical infrastructure in the Arctic area more vulnerable, most notably the long distances and in some places harsh winter conditions. Let us use Svalbard as an example. Svalbard is a Norwegian archipelago in the Arctic Ocean situated about midway between continental Norway and the North Pole, with a population not more

[114]Departementenessikkerhets-og serviceorganisasjon, Digital sårbarhet sikkert samfunn. Beskytte enkeltmennesker og samfunn i endigitalisert verden, NOU (2015),1, Norway, Oslo.
[115]Nasjonalsikkerhetsmyndighet (NSM). (2016),Helhetlig IKT-risikobilde, Norway, Oslo.
[116]Ibid, p. 31.

than under 3 000. Most of them live in the town Long year by en.

Following the regulations for local actors in Norway, also Svalbard prepares regularly risk assessment, the latest being from 2013.[117] It includes a section for critical infrastructure and vital societal functions, including treatments for energy, heating, drinking water, tele communication and data, as well as food supply.

Of these, tele communication and data, comprising basically of cable network in Svalbard and the undersea communication cable to the mainland, is left off the official, published report as including too vulnerable information.

The energy supply of Longyearbyen is dependent on the town's power plant, which in turn is dependent on the coal supply from the local mining facility. If the coal storage is emptied, diesel generators can be used as a reserve, but sooner or later the fuel is also ending without further supply. While in the risk assessment the likelihood of the worst case, total disruption of energy supply, is considered low, the consequences are considered as severe. Depending on the time of the year, the population would have to be evacuated to the mainland, and also the other infrastructure would be damaged without electricity and related heating. Some diesel aggregates in critical places such as the airport could however provide some time. When it comes to central heating, the most serious vulnerability is if the primary network would be damaged or its function would be disrupted; as a result, in most harsh winter times (even if in Svalbard the temperature rarely goes lower than about −15 Celsius in winter time), the town would be frozen and its infrastructure would be damaged. Electricity disruption in wintertime would also sooner or later result in the damage and disruption of the drinking water network. As to the food supply, the main food shop chain has a reserve for four months for most needed products, though some would be vulnerable to electricity disruption.

In general, the overall strategy of Svalbard is to identify the bottlenecks and find and enhance redundant systems to overcome natural, technological and man-made threats. While cyber security is not specifically discussed in the published report, it is however easy to imagine that some parts of the interdependent infrastructure chain, most notably related to electricity production and distribution, might be vulnerable for cyber-attacks.

To sum up, the analysis of the legal and policy framework applicable to cyber-threats and cyber-attacks in a pluralistic and polycentric approach and in a multilevel regulatory analysis denotes the existence of a complex cybersecurity regime that is not yet a consolidated regime. However, from all that proceed, it can be advocated that the cybersecurity regime including the case of cyber-threats and cyber-attacks to CIs in the EHN under ECIC conditions is in the process to be created and this section has helped to establish how to design a framework to cyber-threats and cyber-attacks by combining different levels of governance with particular emphasis on the role of Norway as a crucial source of inspiration.

[117]Svalbard. Risiko-og sårbarhetsanalyse. (2013). Offentlig version, Norway, Longyearbyen.

4. Conclusion, Recommendations and New Future Pathways

This article has demonstrated how CIs, cyber security and human security are intertwined and how this inter-linkage ends up being highly risky in terms of management in the EHN within a global multi-level context. This high level of exceptional criticality in terms of vulnerability is due the fact that in the presence of harsh climatic conditions as a consequence of climate change effects, CIs became "extra critical" from which derived the new concept coined as "Exceptionally Critical Infrastructure Conditions" (ECIC).

4.1. Conclusion

From a legal and political point of view, the interlinkage between CIs and cyber security under ECIC conditions needs special protection, in terms of resilience, management of risks and cooperation between European High North countries (EHN), which share similar problems and threats. The need to defend these CIs under attack from foreign nations, or some individual or some groups of people will arise. Most of relevant norms come from pre-cyber international law before cyber-threats appeared and constitute fundamental principles, such as the prohibition of intervention, use of force, attacks on civilian targets. A holistic assessment under the prism of human security focusing on risk assessment and management has been achieved with the aim to understand, and to improve coherency and uniformity of international and regional law. In addressing the question of research, this article has demonstrated that the law cannot solve or represent the only part of the possible puzzle to be applicable in case of cyber threats to CIs, in the EHN under ECIC conditions. Instrument mixes, such as standards, strategies, measures, tools, voluntary measures, codes as identified at global, regional and national regulatory levels, are also necessary.

4.2. Recommendations

They need to be integrated with collateral governance issues, such as environmental threats, international relations, international cooperation and coordination, the factor of human security, private and public approach. These collateral governance issues, including *standards* all operate in syntonic synergistic linkage, including the stake-holder approaches. Practitioners, policy makers and governments may be well aware that cyber threats applied to CIs under ECIC conditions cannot be covered by existing international, regional or national laws because unfitting or they do not address the event. However, this does not mean that there is a void of legislations. On the contrary, this article has assessed and analyzed the possibilities also in terms of cooperation. Some states or international organizations have even gone beyond cooperation by adopting international norms. An example of such a phenomena is the EU law, with the directive 2008/114/EC.[118] However, there is no such readily applicable framework, but a myriad of potential international law norms, coupled by the guidance produced by the valid updated analysis of the new version of the 2.0 Tallinn Manual. Still,

it is not clear how international law applies. The need for a regulatory framework applicable to CIs and cyber-security is evident. Designing a suitable programme linked to human security is urgent. This article suggests designing a possible framework by combing the potential of bits of provisions from international-regional and domestic levels of sources of law and policy, combined with relevant sources of Norwegian law and policy strategy under the human security umbrella. By validating the first assumption of this article,[119] it has been explained and proven why Norway has been selected as a case study, especially for its value on how this model could contribute both the international and regional law in designing an effective legal framework. Cyber-threats present a new kind of threat and gaps in regulatory terms that current international and regional laws are not ready to meet. The Norwegian model presents several potential aspects that could begin to fill gaps. For example, the Norwegian model has strong potential to be used as a source of inspiration to design future information sharing schemes on threats, risk and vulnerability that are not well defined at the EU level. By validating the second assumption of this article[120], it has been demonstrated how the four principles of crisis management are well suited to be incorporated in a new possible piece of international agreements in the EHN.

4.3. New Future Pathways

New future pathways suggests that combination of both the policy and legal framework can give birth to a new embryonic agreement the skeleton framework of which would empower EHN to cooperate and collaborate further. Such a new regulatory framework or new agreement should require that parties pass domestic laws prohibiting cyber-attacks and harmonize laws across states. Such kinds of agreement should be based on information sharing, aspects of international, EU and Norwegian sources of laws and policies setting up additional mechanisms to include cooperation and collaboration with a human security global dimension.

Acknowledgements

This article is a deliverable of a research project granted from Nord Forsk (Grant n. 81030) entitled "*Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary framework in the European High North* (EHN)"-Working Package-WP4 "*Climate Change*, *Environmental Threats and Cybersecurity*" leaded by Sandra Cassotta. The authors of this article are very thankful to Nord Forsk.

[118]See subsection 3.2 "Regional Law and EU Law".

[119]In the first assumption, it is mooted whether the domestic Norwegian experience could represent a legal model to improve the applicability of international and regional law in designing proactive law achieving human security goals in a pluralistic context.

[120]In the second assumption of this article, it is wondered whether the Norwegian model need to be combined with a pluralistic and polycentric patchwork of instrument mix and governance issues in order to enhance the applicability of international and regional law rather than standing in an isolated way.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

(2012). *Russian Strategic Bombers Carry out North Patrols, RIA Novosti*. http://en.rian.ru/military_news/20120912/175920165.html

(2014a) *The President of Russia, All-Russia Youth Forum "Seliger"*. http://news.kremlin.ru/news/46507/print (Hereinafter, Presidential Meeting Transcript).

(2014b). *The President of Russia, Videoconference with the West Alpha Platform in the Kara Sea*. http://news.kremlin.ru/news/46421/print

Agreement on Cooperation on Marine Oil Pollution Preparedness and Response in the Arctic, Signed 2013.

American Convention on Human Rights (Pact of San José) Adopted in San José, Costa Rica on 22 November 1969.

Argomaniz, J. (2013). *The European Union Policies on the Protection of Infrastructure from Terrorist Attack: A Critical Assessment. Intelligence and National Security.* Routledge: Francis and Taylor, 264.

Arnaud, A. J. (1995). Legal Pluralism and the Building of Europe. In H. Petersen, & H. Zhale, Eds., *Legal Polycentrycity: Consequences of Pluralism in Law* (pp. 127-149). Hanover, New Hampshire: Dartmouth Publishing Company.

Barents (2012). Assessment of International Standards for Safe Exploration, Production and Transportation of Oil and Gas in the Barents Sea. *Final Report Phase, 4,* 9.

BBC (2007). *Russia Plants Flag under N Pole.* http://news.bbc.co.uk/1/hi/world/europe/6927395.stm

Beac. St Barents Regional Council (BRC) (2013). http://www.beac.st/in_English/Barents_Euro-Arctic_Council/Barents_Regional_Council.iw3

Beac. St. (2013). *The Barents Projects.* http://www.beac.st/?DeptID=25430

Beac. St. Barents Euro-Arctic Council (2013). http://www.beac.st/in_English/Barents_Euro-Arctic_Council/Barents_Euro-Arctic_Council.iw3

Bellona, Oil (2013). http://www.bellona.org/subjects/Oil

Berkam, P. A., & Vylegzhanin, A. (2010). Environmental Security in the Arctic Ocean. In *Nato Science for Peace and Security Series: C Environmental Security*. Berlin: Springer.

BP (2015). *BP, Statistical Review of World Energy 2015, Oil Reserves.* http://www.bp.com/en/global/corporate/about-bp/energy-economics/statistical-review-of-world-energy/review-by-energy-type/oil/oil-reserves.html

Brauch, H. G., et al. (2009). *Global Human and Environmental Security Handbook for the Anthropocene.* Berlin: Springer.

Braunch, H. G. (2004). Reconceptualizing Security—A Contribution for the 4th Phase of Research on Human Security and Environmental Security and Peace (HSEP). *Proceeding for the ISA Conference in Montreal*, Canada.

Buzan, B., & Wæver, O. (1999). *Slippery? Contradictory? Sociologically Untenable? The Copenhagen School Replies, Review of International Studies.*

Cassotta, S., et al. (2016). Climate Change and Human Security in a Multi-Level and Multidisciplinary Dimension: The Case of the Arctic Environmental Ocean. In *Climate*

Change Management. Berlin: Springer.

Civil Aviation Convention of 1944.

Civil Aviation Convention of 1963.

Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, (Montreal Convention) 1971.

Convention on Cyber Crime (Council of Europe), CETS, No. 185, 23 November 2001, Entered into Force on 1 July 2004.

Czarny, R. M, (2015). The High North. *Springer International Publishing, 2,* 7-41.

Departementenessikkerhets-og serviceorganisasjon, Digital sårbarhet-sikkert samfunn. Beskytte enkeltmennesker og samfunn i endigitalisert verden, NOU (2015), 1, Norway, Oslo.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. Official Journal of the European Union, L 194/1, 19.7.2016.

EU Cybersecurity Strategy (2013). *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.* Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Brussels, 7.2.2013, JOIN (2013), 1 Final, 12.

European Blackout (2006). http://en.wikipedia.org/wiki/2006European_blackout

European Commission Staff Working Document on the Review of the EPCIP, Brussels, 22.6.2012. SWD (2012). 190 Final, 8.

European Convention on Human Rights (ECHR) (Formally the Convention for the Protection of Human Rights and Fundamental Freedoms) of 1950 Entered into Force on 3 September 1953.

European Union Agency for Network and Information Security—ENISA (2017). *Communication Network Dependencies for ICS/SCADA Systems.* https://www.enisa.europa.eu/publications/ics-scada-dependencies

Forskrift om informasjonssikkerhet (av 1. juli 2001 nr. 744).

Goodman, S. (2008). *Critical Information Infrastructures Protection: Responses to Cyber-Terrorism, Centre of Excellence Defense against Terrorism.* Ankara: Turkey Editions, IOS Press, 32.

Hakon, S. (2011). How to Establish Cross-Border Business and Become a Part of the Existing Supply Chain. In M. Frode, & V. Sergey [hereinafter Skretting], Eds., *Perspectives on Norwegian*. Russian Energy Cooperation.

Hathaway, O., et al. (2012). *The Law of Cyber Attack.* Yale Law School, California Law Review, 817-885.

International Convention on the Suppression of Terrorist Bombing on 15 December 1997.

International Covenant on Civil and Political Rights (ICCPR), Doc. E, 95-2 (1978), 999 U.N.T.S, Entered into Force on March 25, 1976.

International Organization of Standardization, ISO 2700.

Interview Conducted by Javier Argomaniz with Council Secretariat Official (2006). *DG I Civil Protection Unit.*

Kommunal-og moderniseringsdepartement (2015). *Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015-2017, Norway, Oslo.*

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), LOV-1998-03-20-10, Sist

endret LOV-2016-08-12-78 f, Forsvarsdepartementet 1998/2016.

Nasjonal strategi for informasjonssikkerhet, Fornyings-, administrasjons-, ogkirkedepartetement (on Behalf of the Government of Norway) (2012).

National Risk Analysis (2014). *The Norwegian Directorate for Civil Protection (DSB).* Norway, Oslo, 183-202.

Norway Intelligence Claims Russian Intelligence Intensifies Monitoring Norwegian Energy Activities. The Nordic Page. (24 March 2015).

Norway-Russia Treaty, Ann. II.

Norwegian Barents Secretariat, Barents Indigenous People's Office, Economic Development in the Indigenous North (2013). http://www.barentsindigenous.org/economic-development-in-the-indigenous-north.5143491.html

Norwegian Directorate for Civil Protection, Vitalfunctions in Society. What Functional Capabilities Must Society Maintain at All Times? (2017). Norway, Oslo.

O'Dwyer, G. (2015). *Join Cyber Training New Nordic Priority.* White Paper: Global Defense Perspectives. http://www.defensenews.com/story/defense

Optiz, C. (2015). *Potential for Nordic Baltic Security Cooperation—Shared Threat Perceptions Strengthens Regional Collaboration.* German Institute for International and Security Affairs.

Ostrom, E. (2012a). Polycentrism Systems: Multilevel Governance Involving a Diversity of Organization. In E. Brousseau, et al., Eds., *Global Environmental Commons: Analytical and Political Challenges Involving a Diversity of Organization* (pp. 105-177). https://doi.org/10.1093/acprof:oso/9780199656202.003.0005

Ostrom, E. (2012b). *A General Framework for Analysing Sustainability of Social-Ecological Systems.*

Oxford Institute for Energy Studies (2014). *Reducing European Dependence on Russian Gas: Distinguishing Natural Gas Security from Geopolitics.* http://www.oxfordenergy.org/wpcms/wp-content/uploads/2014/10/NG-92.pdf

Radziwill, Y. (2015). *Cyber-Attack and the Exploitable Imperfection of International Law.* Glossary: Brill Nijhoff. https://doi.org/10.1163/9789004298309

Report Cyber Security in the Energy Sector—Recommendations for the European Commission on a European Strategic Framework and Potential Future—Legislative Acts for the Energy Sector. Energy Expert Cyber Security, Platform, 2017, 9-11, 52-53.

Report from the Norwegian National Security Authority (NSM), the Norwegian Police Security Service (PST) and the Norwegian Government's Cyber Security Strategy for Norway (2012).

Report from the White House, Washington (2015). *Findings form Selected Federal Reports: The National Security Implications of a Changing Climate—Readiness in a Changing Arctic.* 7.

Report, Fireeye Threat Intelligence (2015). *Cyber Threats to the Nordic Region.* 10, 13.

Report, Norden, NordForsk (2013). *Societal Security in the Nordic Countries.* Policy Paper, 1-6, 23-24.

Schmitt, M., & Vihul, L. (2017). *Tallinn Manual on the International Law Applicable to Cyber Operations* (2nd Edition). Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

Schmitt, N. M. (2017). Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. *Harvard National Security Journal, 8,*

245.

Shackedlford, S. J. (2014). *Managing Cyber Attacks in International Law Business, and Relations in Search of Cyberspace—An Introduction to the law of Cyber War and Peace.* Cambridge: Cambridge University Press, Vol. 6, 282-283.

Sidortsov, R. (2017a). At the Crossroads of Policy Ambitions and Political Reality: Reflections on the Prospects of LNG Development in Russia. *Oil, Gas & Energy Law Journal (OGEL), LNG Special Issue,* 15.

Sidortsov, R. (2017b). The Russian Offshore Oil and Gas Regime: When Tight Control Means Less Order. In C. Pelaudeix, & E. M. Basse, Eds., *Governance of Offshore Hydrocarbon Activities in the Arctic*. Milton Park, Abingdon-on-Thames: Taylor & Francis Group. https://doi.org/10.4324/9781315585475-8

Skotnes, R. Ø. (2015). *Challenges for Safety and Security Management of Network Companies due to Increased Use of ICT in the Electric Power Supply Sector.* Ph.D. Thesis, Stavanger: University of Stavanger.

Svalbard. Risiko-ogsårbarhetsanalyse. (2013). *Offentlig Version, Norway, Longyearbyen.*

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Entered into force on 10 October 1967.

Tsagourias, N., & Buchan, R. (2016). Cyber-Threats and International Law. In E. M. Footer, J. Schimt, D. N. White, & D. L. Bright, Eds., *Security and International Law.* Oxford and Portland: Oregon.

Tsagouring, N., & Buchan, R. (2015). *Research Handbook on International Law and Cyberspace.* Cheltenham: Edward Elgar. https://doi.org/10.4337/9781782547396

UK, House of Lords (2010). *Protecting Europe against Large-Scale Cyber-Attacks, HL Paper 68.* London: HSMO.

United Nations Convention on the Law of the Sea, Dec. 10, 1982.

Van Eeten, M., et al. (2011). The State and the Threat of Cascading Infrastructures across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Administration, 89,* 381-400. https://doi.org/10.1111/j.1467-9299.2011.01926.x

Wæver, O. (1995) *Securization and Desecurization. R.D Lipshutz Editions.* On Security, Columbia University Press, 46-87.

Wæver, O. (2008). *Globalization and Environmental Challenges: Reconceptualizing Security in the 21st Century.* Berlin, Heidelberg, New York: Springer, 99-112.

Zhang, Z. (2013). Cybersecurity Policy for the Electricity Sector: The First Step to Protecting our Critical Infrastructure from Cyber Threats. *Boston University Journal of Science and Technology Law, 19.*