5 Climate change, environmental threats and cybersecurity in the European High North

Sandra Cassotta[a)*], Roman Sidortsov[b)], Christer Pursiainen[c)], Maria Pettersson[d)] and Michael Evan Goodsite[e)]

a) Department of Law, Aalborg University, Denmark; and Institute for Security and Development Policy (ISDP); Correspondence: sac@law.aau.dk

b) Department of Social Sciences, Michigan Technological University

c) Department of Technology and Safety, UiT The Arctic University of Norway

d) Department of Business Administration, Technology and Social Sciences, Luleå University of Technology

e) School of Civil, Environmental and Mining Engineering and The Institute for Mineral and Energy Resources, The University of Adelaide; and Institute for Security and Development Policy (ISDP)

Executive Summary

This chapter establishes the interconnection between existing environmental global governance systems and cyberspace/cybersecurity as well as the first ever parallel between the environmental (liability) regime and the nascent cybersecurity regime. Understanding the interconnections between these and the role of law, policies and practices in the European High North (EHN) is critical to understanding the variables affecting both climate change and cyberspace. Although climate change and cyberspace are different phenomena, the risks associated with both of them are anthropogenic and can affect the same critical equities, including key sectors such as water, food and energy infrastructures. The aim of this study

is to better grasp the development of cyberspace and its revolutionary impact on human behaviour and human security. This chapter examines and addresses four core ideas: (1) the linkage between climate change, environmental threats and cybersecurity in the EHN; (2) how the interconnectedness of environmental threats and cybersecurity can be identified, managed and regulated, including aspects of governance for cybersecurity and cyber resilience in the EHN; (3) how cyberthreats and their related risk assessments can be incorporated into regulatory frameworks in order to create proactive rather than reactive law by exploring which is the best regulatory framework (or possible combination) applicable among different areas of law; and (4) the current cyberthreats, for example, in the energy industry and specifically to critical infrastructures (CIs) of the energy system, which will advise on the need to design a future agreement incorporating the notion of human security.

5.1 Introduction

This chapter analyses the interconnection between global climate change and cyberspace by showing links and similarities between the two spheres and establishing for the first time a parallel between selected focal points of the environmental regime (in particular the environmental liability regime) and the nascent cybersecurity regime. Acknowledging and understanding these interconnections is critical for devising policies and practices in the European High North (EHN). This chapter examines the shared space of similarities between environmental regime systems (including variables affecting climate change) and cyberspace frameworks. Although the two regimes are different, they are exposed to the same risks associated with anthropogenic effects that might affect the same critical equities, including key sectors such as water, food and energy infrastructures.

The present chapter investigates how the development of cyberspace, with its revolutionary impact on human behaviour and human security, is contributing to social progress. By understanding the risks that come with cyberspace, we can secure not only the environment but also human activities and security. The latter, viewed in an untraditional way and in a broader context at the global level, is not only confined to state security and physical actions. It also includes environmental threats as a consequence of climate change impacts. By showing how risks from human activities are strictly interconnected with the use of cyberspace and related technologies, this chapter demonstrates the need to couple environmental and cybersecurity regulations in order to produce a joint regulatory response. The development and use of digital products and services depends on the functioning of infrastructures, which are under constant stress from both societal and environmental factors.

5.2 Core guiding questions and responses

This chapter examines four core guiding questions:

1. Is there a linkage between climate change, environmental threats and cybersecurity in the EHN, and if so, what is the nature of this linkage?
2. How can the interconnectedness of environmental threats and cybersecurity be identified, managed and regulated, including aspects of governance for cybersecurity and cyber resilience in the EHN?
3. How can cyberthreats and their related risk assessments be incorporated into regulatory frameworks in order to create proactive rather than reactive law? Which is the best regulatory

framework (or possible combination) applicable among different possible areas and levels of regulations?

4. What are the current cyberthreats, for example, in the energy industry and to critical infrastructures (CIs) of the energy system?

CIs and their protections against individuals, groups and foreign nations are strictly intertwined with cybersecurity and the peace of cyberspace (Fidler, 2015). CIs are strictly dependent on cyberspace and are heavily digitalised, especially in the case of the energy sector (oil, gas, electricity and nuclear), which is more exposed to environmental climate conditions/threats as well as cyberthreats. Cyberthreats and environmental threats interact with CIs in a negative synergistic way and make CIs even more vulnerable to risks. CIs in the energy sector are particularly at risk of cyberthreats and cyberattacks, especially in the EHN countries, such as Norway, Sweden and Finland. It is necessary to evaluate the risks of cyberattacks damaging CIs.

There is no precise or agreed upon definition of CIs, with definitions varying between countries. The European Commission (2004, p. 3) defined CIs as ‘physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments’. CIs in the energy system are linked to environmental and climate change threats, such as rising sea levels, which also pose a threat to people living in coastal areas. Therefore, environmental threats can affect not only the ecology of an area but also human security (Cassotta, S., Sidortsov, R., Pursiainen, C., Goodsite, E., Cyber threats, harsh environment and the European High North (EHN) in a human security and multi-level regulatory dimension: Which framework

applicable to critical infrastructures under “exceptionally critical infrastructure conditions” (ECIC)? *Beijing Law Review, 2019, 10*.

This chapter addresses four key questions to frame effective regulations regarding the interconnection between environmental threats and cybersecurity and to suggest how a governance response should be structured to connect the two areas. The consequences of digital disruptions reach beyond the costs associated with clean ups, repairs and/or replacements of affected CIs to include economic, social and environmental disruptions. Thus, this chapter contributes to developing strategies for mitigating the impact of cyber-threats on the EHN, thereby acknowledging the existence of a connection between the two regimes. The integration of the key sectors and factors as well as the application of the same principles of environmental law to both regimes has been particularly fruitful in understanding how to create a safe future for the EHN, which in turn will promote human security.

From a theoretical perspective, this chapter uses and combines different parts of scientific literature drawn from theories of international regimes, including studies on the role of international relation theories, international law, transnationalism, theories of complex interdependencies and global environmental politics. These research streams in the political science literature can prove helpful in addressing the core questions of this chapter. This approach is based on Elinor Ostrom’s (2012) legal framework applied to cyberspace, which can help to conceptualise the connection between cyberspace and environmental regimes. Through this method, institutional analysis design and socio-ecological systems (Ostrom, 2012) complement legal theories based on legal pluralism and polycentrism (Petersen & Zhale,

Arnaud, 1995). This chapter is based on a theoretical framework that is operationalised through the concept of exceptionally critical infrastructure conditions (ECICs) and CIs in the energy system using a multilevel context (global and regional) without neglecting the domestic dimension of sources of law and policies in Norway and Sweden.

From a methodological perspective, this study uses process tracing; legal analysis of both hard and soft law including legal acts, treaty provisions, policy reports and diplomatic speeches; and comparative analysis between different sources of law and policies analysed with a multilevel approach as method of assessment. In addition, the approach was interdisciplinary, combining law and political science to explore which international legal framework would be most applicable to addressing cyberthreats to CIs if environmental law did not prove useful. An example is the case of cyberthreats to CIs in the energy sector of the EHN, which inspired the suggested regime formation processes to achieve effectiveness in terms of environmental protection and security goal achievements

5.3 Conceptualising and governing the linkage between environmental governance and cybersecurity

This chapter conceptualises the linkage between environmental governance and cybersecurity by addressing the core guiding questions of this research. The first two core questions address the linkage between climate change, environmental threats and cybersecurity in the EHN and how the interconnectedness of environmental threats and cybersecurity can be

identified, managed and regulated. These questions include aspects of governance for cybersecurity and cyber resilience in the EHN. This research was conducted based on 1) the concept of ECICs and the law in the EHN; 2) the nexus between climate change, environmental threats and cyberthreats in a multi-regulatory, contextual, sustainable global approach with Sweden as a case study; and 3) the most appropriate framework for addressing cyberthreats and the harsh environment in the EHN.

5.3.1 Concept of ECICs and the law in the EHN

To our knowledge, no one in the field of cybersecurity and climate change has suggested that cybersecurity is an important tool for economic development, but at the same time, the target of cyberthreats to CI, which in the Arctic EHN become extra critical given the harsh environmental conditions and vast distances. Given this extra-criticality due to the environmental conditions, especially the impact of climate change (Cassotta & Sidortsov, 2019), this chapter argues that CIs under ECICs are forged by climate change (such as flooding; rising sea levels; and interruption of maritime routes, electricity and communications), especially in the energy sector due to its increased exposure to environmental threats and its connection with major military and civilian installations. This chapter uses Norway as an example, arguing that if Norway's energy assets were attacked by Russia or another country, if its communications were interrupted or if an oil spill occurred, these would be extra critical because vessels would be put in distress, communications jeopardised and rescue operations made more difficult. This implies the need to create a plan at the intersection between cyberspace and harsh environmental conditions. In this

new way of thinking, the environment, cybersecurity and CIs interact with social and human security determinants. Cybersecurity needs to be reconceptualised from a green perspective that links it to environmental considerations to ensuring sustainability regarding both environmental and human security issues as well as a healthy, stable global ecosystem (Shackelford, 2016). CIs under ECICs need special legal protections due to the cascading effect, which is an effect that increases dependencies among CIs, which could trigger cascading failures and multi-sectorial collapses (Van Eeten, 2011). Given that climate change is hitting the Arctic harder than any other region of the world, and that the effects will be reflected in the rest of our planet (Intergovernmental Panel on Climate Change, 2007), the significance of the cascading effect is amplified, especially for the category of events with low probability and high consequences. We found that although it is possible to map which legislations are potentially applicable for protecting CIs against cyberthreats,[1] many researchers feel that the applicable legislations are fragmented (Hathaway et al., 2012; Radzziwill, 2007; Schmitt, 2017; Tsoagourias & Buchan, 2016). Findings from our study have shown that no treaties or regional agreements based on sustainable protection of CIs under ECICs exist in the Arctic. Such a legal framework is necessary because CIs in the Arctic are crucial for economic, military and security issues and are strictly interconnected with the concept of human security, as explained previously.

1 Legislation applicable to protection against cyberthreats include *jus ad bellum* laws (such as the Law of Armed Conflict), the Charter of the United Nations, space law, laws of state responsibility, international humanitarian laws, international criminal laws, international laws applicable to terrorism, human rights laws, internet laws or the law of the sea (such as the United Nations Convention on the Law of the Sea).

These CIs host many data hubs, and significant energy resources depend on digitalisation, the internet and computer commands. Disruptions due to climate change impacts, such as flooding, ice, nuclear radiation or other climate disasters, require new proactive responses and methodologies. Frequent climate changes (storms, cyclones, rising sea levels, water scarcity, drought, heat waves and warmer temperatures) can threaten nuclear power plants and their infrastructure.

In addition, research has shown that sustainability fails when CIs under ECICs are not protected. Sustainable development is defined in the report Our Common Future (also known as the Brundtland Report) as ‘development that meets the needs of the present without compromising the ability of future generations to meet their own needs’ (World Commission on Environment and Development, 1983). International practices and doctrines on sustainable development are also applicable to cyberspace (Shackelford, 2016). Important principles of environmental law that are linked to the concept of sustainable development include the polluter-pays principle, the precautionary principle and the principle of prevention. Both the concept of sustainable development and environmental law principles can offer research areas in which to analyse the cybersecurity of CIs exposed to climate conditions. The connection between sustainability and cybersecurity is based on the need for social and economic progress and sustainable development in civil society.

In the management of cyberthreats, both the public and private sectors should be involved in managing the interests of stakeholders. The private sector is often faced with managing cyberthreats as part of an effort to build trust with different groups through business activities such as joint ventures,

mixed agreement, hybrid business practices or corporate social responsibility practices (Shackelford 2016). In this context, trust is defined as confidence that a computer system will behave as expected. Cyberthreats to CIs can be managed by utilising cybersecurity's best available practices and technologies while expanding internet access. Consensus standards are often necessary to harmonise an industry's best practices, for example, providing flexible and cost-effective approaches to enhancing cybersecurity measures that assist owners and operators of CIs with assessing and managing risks. In cases where sustainable business practices are equipped to deal with issues of trust, cybersecurity and cyber peace can offer business models on which to grow business practices. This chapter argues that CIs under ECICs require a new paradigm of sustainable climate cybersecurity that relies on the intention to protect CIs through environmental laws and sustainability. Sustainability fails if the linkage between CIs and ECICs is not governed through laws (Cassotta & Sidortsov, 2019).

5.3.2 Nexus between climate change, environmental threats and cyberthreats in a multi-regulatory, contextual, sustainable global approach with Sweden as a case study

Studies have been conducted with the precise aim of drawing a parallel between environmental regulations, the cyberspace and cybersecurity systems. Many aspects of the cybersecurity system are unknown and highly fragmented (Hathaway, 2012; Radzziwill, 2007; Schmitt, 2017; Tsoagourias & Buchan, 2016). A study of Swedish cyber strategy in relation to the environmental regime is being conducted in order to better understand how to improve the effectiveness of the complex cyber regime from a contextual

perspective. One way to better understand cybersecurity systems is through an interdisciplinary study of how best to coordinate these systems, thus making both cyber law and policy more effective. This study will provide evidence on how to take inspiration from a regime system (environmental law or, more concretely, the environmental liability framework) and use it as a source of inspiration to understand and shape the formation of another system in another area, namely cybersecurity.

The methodology consists of choosing and applying key aspects of environmental law (such as concepts and principles) and comparing them with similar key aspects of cybersecurity. To make this comparison, multi-level governance will be applied by analysing the sources of law and policy existing at global, regional and national/local levels in order to understand the interactions between these different levels.

The analytical task for this research consists of choosing focal points from the environmental liability system that are similar and comparable to those of the cyber framework. This study has highlighted the difficulty of identifying the party responsible for environmental damage. In cases of diffuse pollution due to climate change effects, it is very difficult to identify the potential polluter and cause of the damage. The same can be said for cyber damages, as often it is impossible to identify the source of the cyber threat. This study concentrates on three focal points: 1) Who is responsible?, 2) How is risk managed? and 3) How is international cooperation organised? Other issues, such as liability, leadership and insurance (for example, whether the cyber system is encountering the same difficulties as the environmental system when it comes to the conceptualisation of insurance), has been treated.

5.3.3 Best framework for addressing cyberthreats and the harsh environment in the EHN

This study highlights that economic development opportunities in the EHN are accompanied by the danger of cyberthreats, especially to CIs. Building on this, this study will develop the concepts of ECIC and law in the EHN from the previously discussed article (Section 4.3.2). This study will build upon the previous concept of ECICs with the addition of new ideas; for example, a new condition of extra criticality should also include human security concerns to avoid human disasters. CIs pertaining to the energy sector are especially relevant in the EHN in terms of cyber threats since these CIs are more exposed to environmental threats. This sector is in large part dependent on digitalisation, the internet and demands of computers. The digitalisation of CIs can face interference from cyberthreats and climatic conditions, such as ice and natural disasters. Thus, new methodologies of assessment and effective legal frameworks are needed to protect these CIs. Through this, the concept of human security will evolve from merely physical security based on concrete impacts to virtual or intangible human security existing in cyberspace. This implies that society must be protected by rules regulating these new kinds of human security risks. Society's growing dependence on CIs and systems has resulted in a new class of security threats. Because cyberthreats can come from anywhere in the world and their sources are difficult to pinpoint, an examination of the CIs under ECICs requires a comprehensive analysis of the existing sources of law and policy at the national (including local), regional and international levels to observe how pluralistic systems of legal and political sources could apply and interact with complementary legal and

non-legal tools. In this study, Norway represents the domestic level (which includes the local dimension), the European Union (EU) represents the regional level and several selected treaties represent the international level.The concept of ECICs is based on recent definitions of criticality in Norway, especially those found in the recent Norwegian approach, which consists of a collection of reports, laws and strategies (DSB, 2014, pp. 183-202; DSB, 2017; Forsvarsdepartementet, 2016; Kommunal-og moderniseringsdepartement, 2015; The Ministry of Government Administration, Reform and Church Affairs, 2013; The Nordic Page, 24 March 2015).

Norway represents a good case study for a global-local approach and a possible source of inspiration for future agreements, strategies and management of the Arctic areas of the EHN. Svalbard has been chosen as a sub-case of the global-local approach, representing the local dimension. The reason for adopting the Norwegian model is because this model takes into account vulnerabilities and locations of CIs (particularly in relation to harsh environmental conditions). Svalbard demonstrates that most of the potential threats mentioned in the national risk assessment are valid in the Arctic. However, some specific issues can make CIs in the Arctic area more vulnerable, most notably the long distances and harsh winter conditions. In general, the overall strategy of Svalbard is to identify the bottlenecks and locate and enhance redundant systems to overcome natural, technological and man-made threats.

Norway is a relevant case study area because of its focus on information security, protective security, vulnerabilities and locations of critical information systems equipment and their relation to weather conditions.

Norway can be used as a model for designing a legal framework to protect CIs in the energy sector against cyberthreats and as a source of inspiration for the drafting of future agreements in the Arctic and in the EHN area because it combines sources of law and policy in an integrative manner. This also demonstrates that the applicability of international law and regional law dealing with cyberthreats to CIs cannot be isolated from domestic and local dimensions. Interaction between different levels of governance is a must.

What is particularly interesting about the Norwegian case study is the how the country conducts risk assessments and focuses on information security. Norwegian law includes sections on identification and sensitive information (information that might damage installations or affect the power supply, such as vulnerabilities or location; Cassotta et al., 2019). The Norwegian approach is based on four principles that are relevant for this analysis: 1) the responsibility principle, which implies that an agency that is responsible for a sector or an issue under normal circumstances is also responsible for handling extraordinary events; 2) the equality principle, which states that the normal daily organisation structure should be maintained (as much as possible) during extraordinary events; 3) the subsidiarity principle, which explains that extraordinary events should be handled at a lower level if possible; and 4) the cooperation principle, wherein each authority, function or agency must take responsibility for organising the best possible cooperation with all relevant actors for the prevention of, preparedness for and response to extraordinary events.

The Norwegian approach also includes a specific and inspiring cybersecurity response framework. All these mentioned components of the

Norwegian model are lacking in other regional levels, such as at the EU and international levels. According to the Norwegian perspective, even though it could be argued that the Arctic is much less critical in terms of danger exposure to cyber threats due to its smaller population, there is less redundancy and longer distances in some areas at times cold weather that can justify this concept. While the consequences may be small in terms of the number of victims, they can be enormous in terms of severity.

The existence of ECICs is also supported by the cascading effects of CIs and general climatic cascading effects, which are not linked to cybersecurity and CIs but rather to the peculiar geographical location of the Arctic (Intergovernmental Panel on Climate Change, 2017). The authors of this study have advocated that these two types of cascading effects act cumulatively and interact.

The first cascading effect of CIs explains that increasing dependencies on CIs could trigger cascading failures and multi-sectorial collapse (Van Eeten, 2011). This cascading effect belongs to the category of events with low probability and high consequence. The potential of a domino effect is undeniable. Organisational and state involvement is not clear or easy, and states do not actually know how to deal with cascading effects (Van Eeten, 2011).

The second cascading effect of CIs is defined in this research as the climatic cascading effect of the Arctic. According to this condition of the climatic cascading effect, the Arctic is the thermic regulator for the entire planet, and thus events that occur there will not remain isolated to that region. For example, if an oil spill or nuclear explosion were to occur in this region, it

would have enormous repercussions for the rest of the planet (Cassotta & Goodsite, 2013). This is enough to justify the need for extraordinary legal and political measures to protect CIs in the Arctic.

The impact of this second cascading effect could not only affect the cultural heritage of the indigenous rural populations in this area, thus contributing to jeopardising their survival and leading to their extinction, but also the extinction of humankind in the rest of the world due to the critical position of the Arctic. This is why environmental governance and cybersecurity for CIs in the energy sector within the Arctic EHN must be linked to and incorporated with the concept of human security (Cassotta et al., 2019).

In the EHN region, the procurement of natural resources is being increasingly managed through 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 this local, regional and international network.

An examination of the laws governing cyberthreats to CIs under ECICs is also important for practical experts and policymakers in the field of international security by contributing to the concept of human security. This research has therefore mapped the legal and political framework protecting CIs in the EHN using Norway as a case study because this country is highly dependent on both cyber technology and CIs, such as offshore industries. Digitalised offshore activities are very relevant in Norway since this country is highly dependent on these operations, especially transportation, aquaculture and fish farming.

At the regional level, EU law provides significant potential for covering and protecting CIs in the EHN, denoting the existence of a complex cybersecurity regime that is not yet consolidated. However, from this analysis, it can be deduced that the current cybersecurity regime, including issues of cyberthreats and cyberattacks to CIs under ECICs in the EHN, is not yet a consolidated regime but rather a complex process that requires further development. The mapping of related legal and political frameworks in this research has helped to establish a foundation for how a framework against cyberthreats and cyberattacks to CIs under ECICs in the EHN should be developed through combining different levels of governance.

This therefore leads to the following research question: based on a human security focus, in the case of cyberthreats to CIs under ECICs in the EHN, what recommendations can be made to improve international and regional laws? Thus, not only does an analytical overview of the many international accords operating in different areas of law need to be undertaken, but domestic mechanisms must also be considered. Hence, our study shows that it is possible to use a human security focus in the case of cyberthreats to CIs under ECICs in the EHN, and it details how such an assessment can provide recommendations to improve international and regional law. In order to assess the possibility of refitting existing legal and non-legal instruments to fill the gap in international and regional law as well as address the research questions of the study, this research has formulated two main assumptions. The first assumption is that the Norwegian model could represent a legal and policy framework to improve the applicability of international and regional law for designing proactive legal mechanisms to achieve human security goals in a pluralistic context. The second assumption is that the

Norwegian model should be combined with a pluralistic and polycentric patchwork of governance – such as standards, strategic tools, risk assessment approaches and a backdrop of cooperation and coordination at the geopolitical level – in order to enhance the applicability of international and regional law.

The issue of cyberattacks to CIs under ECICs in the EHN is supported in this chapter by a discussion of scientific publications coauthored with specialists in these sectors (CIs and energy infrastructures), which provides an opportunity to expand the notion of human security. However, the issue of possible cyber-attacks to CIs exposed to environmental threats could also be perceived negatively as a disrupter to Arctic collaboration and coordination. This leads to the question of how this coordination can be reconciled with the activities of relevant international organisations, such as the North Atlantic Treaty Organization (NATO) and the EU. It is important to remember that two of the EHN countries, Finland and Sweden, are not part of NATO, and Norway is not a member of the EU (although it is a member of the European Economic Agreement and thus covered by EU legislation on cybersecurity).

The role of NATO is particularly interesting compared to other Arctic regional institutions with non-existent or weak roles in the enactment of legislation. These regional institutions (such as the Arctic Council, Barents Europe Arctic Council, Barents Regional Council and Nordic Council of Ministers) cannot competently deal with cybersecurity or security issues, nor can they govern the nexus between environmental governance, CIs, the energy sector and cybersecurity under ECICs. More important is that NATO is the only institution (compared to the other existing Arctic institutions)

that is dealing with the linkage between environmental governance, climate change and cybersecurity under ECICs through international cooperation. For example, one of these responses is to achieve resilience. In this context, approaches to risk assessment and resilience in the EHN (as defined by both civilian and military agencies) focus on system resilience, which is required for unknown and hybrid threats (Cassotta et al., 2019). According to NATO (2016), resilience and increased civil-military readiness are recognised as key goals for dealing with threats to digitalised CIs, including anthropogenic (cyberattacks) and environmental (space weather or other extreme weather events linked to climate change) threats.

5.4 Conclusion

Currently, at the international, EU and national levels, there is a lack of uniformity in the laws protecting CIs. There is no regional or even global approach in terms of human security. However, a theoretical, applicable, regulatory framework could be applied.

It is found that existing international legal frameworks do not directly address cyberattacks because they were formed prior to the emergence of cyberspace, but they could still be used in the instance of such attacks. A satisfactory regulatory framework integrating law and policy should be uniform and homogeneous and should include the possibility to govern freedom from risks in order to design a law based on a precautionary and proactive rather than reactive approach.

In terms of governance, such a framework should not be based on a monistic vision of the sources of law but rather on a pluralistic and

polycentric vision, wherein sources of law and policy from both the public and private sector overlap and coexist. Thus, law and policy utilising different tools (such as standards, soft law and technical expertise) would coexist in a patchwork mix of instruments.

CIs under ECICs 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. The policy design should include freedom from hazards, freedom from fear (addressing the conflict of a humanitarian agenda), freedom from want (in the context of a human development agenda) and freedom of dignity (with reference to human rights, the rule of law and good/effective governance). In light of this pluralistic and polycentric perspective, this study examined the interactions, pros and cons of different categories of regulatory instrument mixes. This study emphasised that in the context of cyber-realpolitik, this mix of instruments is connected to collateral governance issues, such as environmental climate threats, international relations, public and private approaches to human security and standards.

References

Cassotta, S., et al. (2019). Cyber threats, harsh environment and the European High North (EHN) in a human security and multi-level regulatory dimension: Which framework applicable to critical infrastructures under “exceptionally critical infrastructure conditions” (ECIC)? *Beijing Law Review*, Special Issue 12-Law, Policy and Globalization, March 2019.

Cassotta, S., & Goodsite, M. (2013). A regulatory multilevel and multidisciplinary contextual analysis of environmental impact assessment (EIA) relevant to Greenland: Offshore oil drilling and

the unperfected equation. *European Energy and Environmental Law Review*.

Cassotta, S., & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*, 51, 129-133.

DSB (2014). *National Risk Analysis. Oslo*: The Norwegian Directorate for Civil Protection (DSB).

DSB (2017). *Vital functions in Society. What Functional Capabilities Must Society Maintain at All Times?* Oslo: The Norwegian Directorate for Civil Protection (DSB).

Gorge, M. (2007). *Cyberterrorism: Hype or reality?* Computer Fraud & Security.

Government of Norway, Lov om forebyggende sikkerhetstjeneste, Lov-1998.03.20.10, lastly amended with endretLov-2016.08.12.78 f, Forsvarsddepartment 1998/2016; Action Plan on Information Security 2015- 2017; Norwegian Directorate for Civil Protection, Vital functions in society, What functional capabilities must society maintain all the time? Norway, Oslo 2017.

Fidler, David P., (2015). International law, cybersecurity, and critical infrastructure protection, *Georgetown Journal of Institutional Affairs*, 16 Geo, 8

Hathaway, O. A., et al. (2012). The law of cyber attack. *California Law Review*, 100, 817–885.

Intergovernmental Panel on Climate Change. (2007). *Climate change 2007: Impacts, adaptation and vulnerability. Contribution of Working Group II to the fourth assessment report of the Intergovernmental Panel on Climate Change*. Cambridge, United Kingdom: Cambridge University Press.

Kommunal-og moderniseringsdepartement (2015). Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015–2017. Oslo: Norwegian Government Administration Services.

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

The Ministry of Government Administration, Reform and Church Affairs (2013). Cyber Security Strategy for Norway. Oslo: Norwegian Government Administration Services.

DSB (2014). National Risk Analysis. Oslo: The Norwegian Directorate for Civil Protection (DSB).

European Commission (2004). *Critical Infrastructure Protection in the fight against terrorism*. COM(2004) 702, Brussels, 20 October 2004.

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

Kommunal-og moderniseringsdepartement (2015). *Handlingsplan for informasjonssikkerhet i statsforvaltningen 2015–2017*. Oslo: Norwegian Government Administration Services.

North Atlantic Treaty Organization (NATO). (2016). *Warsaw summit communiqué issued by head of state and government participating in the meeting of North Atlantic Council in Warsaw, 8-9 July 2016.*

Ostrom, E. (2012). Polycentric systems: Multilevel governance involving a diversity of organizations. In *Global environmental commons: Analytical and political challenges in building governance mechanisms*, pp. 105–117.

Petersen, Zahle, & Arnaud. (1995). *Legal polycentricity: Consequences of pluralism in law*. Dartmouth Publishing Company.

Radzziwill, Y. (2015). *Cyber-attacks and the exploitable imperfections of international law*. Brill Nijholff.

Shackelford, S. (2016). On climate change and cyber attacks: Leveraging polycentric governance to mitigate global collective actions problems. *Vanderbilt Journal of Entertainment & Technology Law*, 18(4).

Schmitt, M. N. (2017). Peacetime cyber responses and wartime cyber operations under international law: An analytical vade mecum. *Harvard National Security Journal*, 8, 245.

Schmitt, M. N., & Vihul, L. (2017). *Tallinn manual on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.

The Ministry of Government Administration, Reform and Church Affairs (2013). *Cyber Security Strategy for Norway*. Oslo: Norwegian Government Administration Services.

The Nordic Page (24 March 2015). Norway Intelligence Claims Russian Intelligence Intensifies Monitoring Norwegian Energy Activities. Retrieved from https://www.tnp.no/norway/politics/4886-norway-intelligence-claims-russian-intelligence-intensifies-monitoring-norwegian-energy-activities

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.

Van Eeten M. (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).

World Commission on Environment and Development. (1983). *Our common future*.