Scientific Research Publishing

Beijing Law Review, 2019, 10, 616-642
http://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example

Sandra Cassotta[1,2,3,4,5*], Maria Pettersson[6]

[1]Department of Law, Aalborg University and Centre of Cybercrime and Cybersecurity, Aalborg, Denmark
[2]Institute for Security and Development Policy, Stockholm, Sweden
[3]Sustainable College Bruges (SCB), Bruges, Belgium
[4]The International Panel on Climate Change (IPCC) from 2017-19, United Nations Environmental Law Programme UNEP, Geneva, Switzerland
[5]School of Law, Western Sydney University (WSU), Sydney, Australia
[6]Department of Business Administration, Technology and Social Sciences, Luleå University of Technology, Luleå, Sweden
Email: *sac@law.aau.dk

How to cite this paper: Cassotta, S., & Pettersson, M. (2019). Climate Change, Environmental Threats and Cyber-Threats to Critical Infrastructures in Multi-Regulatory Sustainable Global Approach with Sweden as an Example. *Beijing Law Review, 10,* 616-642.
https://doi.org/10.4236/blr.2019.103035

Received: May 5, 2019
Accepted: June 24, 2019
Published: June 27, 2019

Abstract

This article explores and analyzes the nexus between climate change, environmental threats, and cyber-threats in a multi-regulatory contextual sustainable global approach with Sweden as an example. Research and collection of material have been conducted with the precise aim to draw a parallel between environmental regulations and the cyberspace and cybersecurity systems. Many aspects of the cyber-security system are not known and are highly fragmented. Selected points of the study of the Swedish cyber strategy are being developed in parallel to the environmental regime in order to better understand how to improve the effectiveness of the cyber complex regime from a contextual perspective. One way to better understand the cybersecurity system is to make an interdisciplinary study of how best to coordinate these systems, thus making both cyber law and policy more effective. This leads to bringing evidence on how to take inspiration from a regime system (environmental law or, more concretely, the environmental liability framework) and using it as source of inspiration to understand and shape the formation of another system in another area, namely cybersecurity. The method of this ongoing research consists of choosing and applying key aspects of environmental law (such as concepts and principles) and comparing them with comparable selected cybersecurity key aspects, which are selected because they present strong similarities with their "equivalent" focal points pertaining

to the environmental system. When conducting this comparison, multi-level governance is applied too, which means analysis of the sources of law and policy existing at Global/Regional/National (local) levels in order to understand the interactions between different levels. The analytical task of the research consists of choosing some focal points from the environmental liability system that are very similar and comparable to those of the cyber regime.

Keywords

Climate Change and Cybersecurity, Environmental Liability Regime, Environmental Threat and Critical Infrastructure, Swedish Cyber Law, Sustainable Cybersecurity

1. Introduction

Global climate change and cyber threats are two major future global challenges in terms of regulation and management. Even though variables affecting climate change, cyberspace and cybersecurity are different, they present similar characteristics from a regulatory and management perspective as they are associated with risks of anthropogenic nature affecting critical equities, including key sectors of critical infrastructures, such as the energy sector. The potential for cross-pollination in order to improve the effectiveness and enforcement of the law can enhance the common regulatory protection system against cyber-threats to the energy sector, for example. This article draws a parallel between environmental and cyber regulatory problems on typical focal points pertaining to both regimes in the case of critical infrastructures in the energy sector in order to improve cyber law which looks extremely fragmented and uncertain in the way to regulate and manage risks (Radzwill, 2015; Hathaway et al., 2012; Schmitt, 2017; Tsagourias & Buchan 2016). The article advocates that law should look uniform and homogenous and not based on a monistic vision, but rather on a multi-regulatory pluralistic vision where sources of law and policy interact in an integrative fashion. This article connects climate and environmental law concepts and principles with cybersecurity issues, and shows how these can be used in the cyber regulatory space in order to improve the management and effectiveness of cyber law.

The aim of this study is to categorize instruments and mixes of instruments to design a sustainable, preventive and effective legal framework for protecting against cyber risks in order to enable decision makers to act preventively. The research question thus *seeks to design a model consisting of a sustainable combination of selected legal approaches and instruments to improve the effectiveness of regulation and management to prevent cyber-threats and reinforce cybersecurity*. In order to do so, we first commence to individualize the global dimension of both regimes and examine key international legal frameworks, including the possibility to apply environmental law principles to the cyber dimension. Thereafter, we analyze the regional dimension of EU cybersecurity law,

and lastly the national dimension, with Sweden as the primary object of investigation. Three factors are taken into consideration: international cooperation, risk management (liability and insurance), and who is responsible (public governmental/private). Focal points common to the two regimes, such as the notion of damage, liability, and insurance, are thus taken into consideration for cross-pollination analysis. Factors and focal points are considered in relation to stakeholders as well as the private and public sector.

2. Global Level: Cyberspace through the Prism of Environmental Law and Policy

In consideration of two of the world's most overhanging threats: climate change and cyber-threats (Radzwill, 2015; "Cybersecurity Forum", 2013-18)[1] legal scholars, policy-makers and the business sector are actively trying to understand how to manage and regulate the intractable aspects that characterize these two contemporary multilevel phenomena. The physical consequences and the estimated costs of non-action to these threats are enormous and still largely under-quantified. There is an urgent need to tackle and mitigate risks in the climate change and cybersecurity (The 2013 European Union Strategy)[2] regimes (Oran, 2012; Oberthür et al., 2012; Radzwill, 2015).[3] Both regimes can be perceived as "global collective problems" that share similar practices and concerns and interest the private sphere. The similarities of the regimes make it possible to analyze issues related to cyberspace through the prism of environmental law and policy. Both regimes deals with problems that affect the sustainability of the

[1]The term "cyber-attack", "cyber-threat" and "cyber risk" are different even though used in the same context. A "cyber-attack" is an offensive action, whereas a "cyber-threat" is the possibility that a particular attack may occur, and the cyber risk associated with the subject threat estimates the probabilities of potential losses that may result. A cyber-attack is an act of unauthorized altering, deleting, disrupting, damaging or suppressing data within targeted computerized systems or network. See for that point, Radzwill, 2015 and "*Cybersecurity Forum*", 2013-18.

[2]The technical definition of cybersecurity refers to the Internet security as a branch of computer security specifically related to Internet. Its objective is to establish rules and measures to use against attacks over Internet. The advantages of cybersecurity will defend us from critical attacks and help us to browse the safe websites. Internet security processes all the incoming and outgoing data on our computer. The term "cybersecurity" 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. See the 2013 European Union Strategy.

[3]The term "cybersecurity regime" will be used in this article referring to the definition of Oran Young as a "complex regime" because cybersecurity is not yet a consolidated regime but it is in the process to become one and in that sense, this article helps to establish the existence of a regime when referring to cybersecurity. A "regime complex" is a collection of governance arrangements that are linked together in the sense that they address matters related to a common issue area or spatially defined region but that are not hierarchically related in the sense that they all fit within some well-defined institutional architecture. The originators and theorists of this way of thinking about governance have focused on cases like the regime complex for plant genetic resource and the regime complex of climate change. Regime complexes vary dramatically along a spectrum ranging from severe fragmentation to close-knit integration. For "regime complex" see Oran, 2012. Building and International Regime Complex for the Arctic: Current Status and Next Steps, *The Polar Journal*, No. 2, pp. 391-407.

whole planet; the atmosphere for climate change, and world security for cyberspace.[4] Both regimes rely on doctrines of international (environmental) law and on the concept of sustainable development,[5] which thus links the two regimes. Sustainable development is a central concept to equitable management and regulation of the global "common pool resources", such as the environment and the cyberspace (Radzwill, 2015)[6] which are both spaces not belonging to anybody but rather considered as *res communes* and *res nullius*. Cyberspace, Internet, and the environment, are all Common Heritage of Humankind (CHM)'s concepts.[7]

2.1. The Concept of Global Commons or "Imperfect Commons"?

At an international level, the areas that do not fall within the jurisdiction of any one country are defined as "international or global commons". The notion of global commons posits that there are limits to national sovereignty in certain parts of the world and that these areas should be open to use by the international community but closed to exclusive appropriation by treaty or customs. Examples are the High Seas, Antarctica, Outer Space & the Atmosphere but also cyberspace (Redder & Hughes, 2008). Global commons are often governed by regulations at multilevel, such as at the international, regional and national regulatory levels. There is no binding legal principle to govern global commons but the closest historically used is the common heritage concept (CHM). Since cyberspace is the most recent addition in the sphere of global commons, it is worth considering how the CHM may be applied to enhance cybersecurity.

There is not yet agreement on a common and established definition of CHM but according to Jennifer Frakes (Frakes, 2003) the CHM can be defined by five following elements: 1) there can be no private or public appropriation; no one legally owns common heritage spaces; 2) representative of all nations must work together to manage global commons pool resources; 3) nations must actively share the benefits acquired from the exploitation of resources from the common heritage region; 4) there can be no weaponry or military installations established in common heritage areas as, they should be used for peaceful purposes; and 5) the commons must be preserved for future generations.

It is however as difficult to delimit cyberspace as it is to control the use of the atmosphere to prevent climate change. If not controlled, perpetrating cyber-threats can destabilize cybersecurity or even the peace of the cyberspace. Here it is important to discuss the implication of how we perceive cyberspace: it is a "commons" or is it an ensemble of physical infrastructures composed by

[4]The term cyberspace refers to the virtual realm (also called "Cyber-Realm") created as a result of the use of information technology. Nowadays the term cyberspace is characterized as the "fifth domain of war" by some academics, states, as well as the North Atlantic Treaty Organization (NATO).

[5]The concept of sustainable development will be treated in the next section.

[6]The term cyber-space can be interchanged here with the term cyber-realm. They are both virtual realm created as a result of the use of information technology. See for that point, Radzwill, 2015.

[7]The concept of CHM will be treated in the next section both in the environmental climate law and cybersecurity spheres.

cables, hardware, fiber optics, tubes or Internet. The fact that several Internet infrastructures are owned and operated by private firms and subject to multilevel governance presumes that cyberspace is an atypical or "imperfect commons" controlled by both public and private entities and subject to a mix of different private and/public tools and as well as policy strategies.

2.2. Relevance of Critical Infrastructures between Environmental Threats and Cyber-Threats

Critical infrastructures (CI) (European Commission COM, 2004; Tsagouring, & Buchan, 2015).[8] and their protection against private individual or groups or foreign nations, are strictly intertwined with cybersecurity or the peace of the cyberspace (Fidler, 2015). CI are also strictly dependent on cyberspace as well as heavily digitalized, not least in the energy sector,[9] which—although more exposed to environmental climate conditions and environmental threats—is also subject to cyber-threats. In addition, cyber-threats and environmental threats interact in a way that increases the risks for CI. This is particularly true in the energy sector, especially in the European High North (EHN) areas, such as Norway, Sweden and Finland where there is a need to improve resilience (Pursiainen, 2018). Given the lack of treaties both at global and regional level regulating cyber-threats and cyber-attacks, especially to CI and under environmental threats, it is up to the national level, and more specifically to the private sector to manage cyber-threats. Even if cybersecurity, or better "cyber insecurity", is a global and regional problem, like climate change, initiatives for sustainability are still driven "bottom-up" and in the private sector. At the same time, the Paris Agreement (The Paris Agreement, 2016)[10] signed under United Nations Convention on Climate Change (UNFCCC) (The United Nations Convention on Climate Change, 1994),[11] outlines, for the first time in the governance of the atmospheric pollution, an "integrated" top-down and bottom-up approach, as

[8]Critical infrastructures linked to cybersecurity is relevant because cyber-attacks to critical infrastructures permit to evaluate the risk-assessment of damaging capabilities of cyber-attacks. It is worth noticing that there is no precise and agreed definition on the term critical infrastructure. However, the precise definition of what this definition should include in the concept is not the same in all countries. The EU defines critical infrastructures 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*". See for that point, European Commission COM (2004) 702 of 20 October 2004. Also, 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). See for that point, Tsagouring, & Buchan, 2015.

[9]The energy sector is considered composed in this article by: oil, gas, electricity and nuclear.

[10]The Paris Agreement, signed on the 22 April 2016, entered into force on the 12 December 2016 and deals with greenhouse-gas-emissions, mitigation, adaptation and finance.

[11]The UNFCCC is an international environmental treaty that became effective in 1994 with the objective of stabilizing greenhouse gas concentrations in the atmosphere at a level that would prevent dangerous anthropogenic interferences with the climate system. The framework sets no binding limits on greenhouse gas emissions and contains no binding mechanisms. Instead, international treaties (called "protocol" or "agreements") may be negotiated to specific further action towards the objective of the UNFCCC.

opposed to the clear top-down approach in its predecessor, the Kyoto Protocol (The Kyoto Protocol, 2005).[12]

2.3. The Tragedy of the Commons: Climate Change, Environmental Threats and Cyber-Threats

In the same way as for cyberspace, the climatic atmosphere is not inexhaustible. The amount of clean air on earth is, for example, not without limit. The tragedy of the commons predicts a gradual overexploitation of common pool resources, including oceanic and atmospheric resources (Hardin, 1968). The question is if the tragedy of the commons is a possible scenario also in case of cyber-threats: can the Internet space be overused, as the pasture in Hardin's example? (Hardin, 1968).[13] Both the atmosphere and cyberspace are affected by millions of actors and thus face similar problems in terms of potential overuse of resources. The presence of the "free-riders" (Nordhaus, 2015; Hansel, 2013)[14] is also common in these contexts. No one knows how many cyber-attacks are needed to push the world into a collective dilemma, we only know that if cyberspace is treated as a "commons"—i.e. unregulated and unguarded—there is a risk that its resources will be overexploited and eventually exhausted. Common pool resources are often managed thought property regimes that can be difficult to enforce, and it can also be difficult to get rid of free-riders. To conclude, it is unknown how many of

[12]The Kyoto Protocol is an international treaty under the UNFCCC that commits parties to reduce GHG-emissions, based on the distribution of responsibility outlined in the Annexes established in the UNFCCC. The Kyoto Protocol was adopted in Kyoto, Japan on 11 December 1997 and entered into force on 16 February 2005.

[13]Hardin describes the tragedy of the commons in this way: "Picture a pasture open to all. It is to be expected that each herdsman will try to keep as many cattle as possible on the commons. Such an arrangement may work reasonably satisfactorily for centuries because tribal wars, poaching, and disease keep the numbers of both man and beast well below the carrying capacity of the land. Finally, however, comes the day of reckoning, that is, the day when the long-desired goal of social stability becomes a reality. At this point, the inherent logic of the commons remorselessly generates tragedy. As a rational being, each herdsman seeks to maximize his gain. Explicitly or implicitly, more or less consciously, he asks, "What is the utility to me of adding one more animal to my herd?" This utility has one negative and one positive component. 1) The positive component is a function of the increment of one animal. Since the herdsman receives all the proceeds from the sale of the additional animal, the positive utility is nearly +1. 2) The negative component is a function of the additional overgrazing created by one more animal. Since, however, the effects of overgrazing are shared by all the herdsmen, the negative utility for any particular decision-making herdsman is only a fraction of −1. Adding together the component partial utilities, the rational herdsman concludes that the only sensible course for him to pursue is to add another animal to his herd. And another; and another… But this is the conclusion reached by each and every rational herdsman sharing a commons. Therein is the tragedy." Hardin, 1968.

[14]Free-riders" refers to the "free-riding" phenomenon, which occurs when a party receives the benefits of a public good without contributing to the costs. In the case of international climate change policy, countries have an incentive to rely on the emission reduction of others without taking proportionate domestic abatements. The failure of the Kyoto Protocol, and the difficulty of establishing and effective follow-up regime, is largely due to the free-riders. See, Nordhaus, 2015. Similar, to the climate change regime, the free-riding problem also exists in cybersecurity governance. However, cybersecurity is not a pure public good. A state who invests in its cyber defense first improves the security of its own goods, public and private networking. Yet to a certain degree it also benefits other states' cybersecurity. See Hansel, 2013.

climate change's impacts and cyber-attacks it will take to reach a "tipping point"[15] pushing the world, in both cases, into a collective dilemma, and what actions and responses in terms of governance could be applicable. The *scale* of the problem is thus similar for climate- and cyber-threats. In the long run, no one knows, for example, if the Internet can theoretically survive a nuclear war.

2.4. Overuse of Resources

Millions of actors can evidently affect the atmosphere and cyberspace, and thus the climate and cybersecurity. Cyberspace and the atmosphere share the potential problem of overuse of resources, difficulties of enforcement, and both spaces are subject to the inactions of free-riders. As previously noted, the nature of the problem in both contexts is intrinsically linked to the governance of commons, which exists both at the domestic and global, regulatory levels. Common pool resources are typically not inexhaustible. The areas where common pool resources are located are often managed through property regimes that can be difficult to enforce and in some cases it can also be difficult to exclude actors, for instance if they belong to a "defined user pool". Free-riders can thus exist also here.

Examples of resources contained in common pool resources are fish, forests, lakes, and village pastures. Both cyberspace and the atmospheric climatic space thus share the difficulties to establish and enforce norms to control the actors' behavior. In the case of environmental pollution it can be difficult to see to it that emissions limitations are in fact adhered to (monitoring), or on a less developed level even to control the use of the environment by requiring permit for environmentally hazardous activities. In the case of cyberspace, similar problems arise in the form of information and computer network and the use of the space on the Internet, as will be explained in the next section. This kind of uncertainty regarding what actions and responses, e.g. in terms of governance, that could be applicable, calls for effective intervention to promote the uses of both spaces in a more sustainable manner by promoting a "sustainable cyber security", preferably based on the Precautionary principle.[16]

2.5. Cooperation

Cooperation on cybersecurity and environmental protection requires different forms of relationships, for example among governments and their law enforcement agencies or stakeholders. These different forms of cooperation can be in the form of bilateral cooperation, such as Multilateral Legal Assistance Agreements (MLTAs),[17] informal bilateral cooperation, such as individual police con-

[15]The "tipping point" are composed by elements of the climate that may pass a critical threshold, or "tipping point," after which a tiny change can completely alter the state of the system. Moving past tipping points may incite catastrophes ranging from widespread drought to overwhelming sea level rise.

[16]The Precautionary principle will be treated in section 3.3.1.

[17]Mutual Legal Assistance Treaties (MLTAs) are agreements between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public or criminal laws.

tacts, or formal multilateral cooperation, such as the Council of Europe with the European Cyber Crime Convention (better known as the "Budapest Convention") (The European Convention on Cybercrime, Council of Europe, July 2004).

In the case of regional cooperation on cybersecurity for CI in the energy sector, the aim is to control and make secure any disclosure of vulnerabilities and incidents affecting the energy sector. This also includes cooperation among stakeholders. The difficulties lie in establishing an acceptable level of protection and cooperation. In both the cybersecurity—and the environmental protection regime, the duty to cooperate—as a general principle of international environmental law—applies, especially when dealing with global commons. A practical example of such a (hard law) multilateral agreement is the United Nations Convention on the Law of the Sea (UNCLOS), in which the duty to cooperate is stated in Art. 197.[18]

In the case of cyber activities, nations must solve their disputes peacefully, without any resort to illegal force, and they have duties of due diligence to monitor their networks in order to prevent them from being used to cause harm to other nations and in some cases to non-state actors and stakeholders (Jensen, 2014). In addition to matters of peace and security, the duty to cooperate applies to the solving of international problems of economic, social, cultural and humanitarian character, especially in respect to Antarctica, Outer space and the Seabed. An example of a hard law in the field of cybersecurity is the previously mentioned Budapest Convention that refers to cooperation in Art. 23.[19] While the standard for the level of cooperation is not agreed in any of the regimes, there is consensus that states must exercise good faith when fulfilling the duty of cooperation, and that this is fully interconnected with a stakeholder approach, and relates to global commons subject to both public and private regulations.

2.5.1. The Paris Agreement, the Kyoto Protocol and the Montréal Protocol

Climate change and cyber-security can both be addressed in a multi-regulatory governance system. It will however not be enough to solve problems related to effectiveness and enforcement; bottom-up action and the activities of civil society at national level will still be crucial. Vertical implementation of international law via regional law (i.e. EU law) would improve and contribute to the communication of information and details regarding implementation of key policies and targets, both regarding climate change policies and cyber-policies. Also horizontal implementation of the regional law (i.e. EU law) at national level, e.g. by

[18]Article 197 of the UNCLOS Convention states "States shall cooperate on a global basis and, as appropriate, on a regional basis, directly or through competent international organizations, in formulating and elaborating international rules, standards and recommended practices and procedures… for the protection and preservation of the marine environment, taking into account characteristic regional features."

[19]Art. 23 of the European Cybercrime Convention states, "The Parties shall cooperate with each other, and provide mutual assistance, particularly with respect to investigations of cyber incidents".

providing information on activity plans and strategies to be implemented at national level in both realms, is important. The governance of cybersecurity and climate issues cannot rely on one level of regulation, or on one dimension (i.e. only vertical implementation) but rather requires a combination of the two dimensions (vertical and horizontal), with strong emphasis on the role of civil society to ensure both top-down and bottom-up implementation. The role of civil society is, for example, highly relevant for the implementation of the Paris Agreement to minimize the free-rider problem and thus contribute to enhance international cooperation to combat climate change. Under the Paris Agreement, even if individual countries' plans are voluntary, the legal requirements that they publicly monitor, verify and report, as well as the practice to publicly put forth updated plans, are designed to create a "name-and-shame" system aiming to prevent international laggards of free-riders. This is in contrast to the previous treaty that the Paris Agreement replaces, the Kyoto Protocol. While the Kyoto Protocol was successful in terms of ratification and the setting of binding emission reduction targets, it did not enforce sustainable development, not least since only the developed countries were bound by the targets, despite the fact that large emissions also came from the developing countries.

It took a long time for the Kyoto Protocol to come into force[20] and thus have an impact on global climate policy. The "Montréal Protocol" (The Montréal Protocol on Substances that Deplete the Ozone Layer to the Vienna Convention for the Protection of the Ozone Layer of 1987),[21] on the other hand, is considered as an example of a successful model of cooperation to address global problems, in this case the depletion of the ozone layer (Baush & Mehling, 2013). Although climate change can be considered a greater challenge than the depletion of the ozone layer, not least because of the timescale of the problem, the implementation of the Montréal Protocol can serve as a model for specialists, treaty drafters, and planners in the field of cybersecurity.

When discussing models for cybersecurity governance it is important to be aware of the complexities related to the tipping point.[22] It is thus highly relevant to understand how many and which kind of cyber-attacks it will take to reach a tipping point and put the world to take collective action.

2.5.2. The Council of Europe, the Tallinn Manual and the Multilateral Legal Assistance Treaties (MLAT)

Drawing a parallel between environmental regulations and the cyber space and cybersecurity systems can be an inspiring exercise for the governance of both re-

[20]The implementation of the Kyoto Protocol was delayed mainly due to the US withdrawal from the protocol that seriously jeopardized its entry into force. Although it was adopted already in 1997, it wasn't until Russia signed it, in 2004, that it came into force.

[21]Protocol on Substances that Deplete the Ozone Layer (Montréal Protocol) of September 16 of 1987 to the Vienna Convention for the Protection of the Ozone layer is an international environmental agreement designated to protect the ozone layer by phasing out the production of numerous substances that are responsible for the ozone depletion.

[22]The concept of tipping point is explained in Section 2.3.

gimes. Several aspects of the cybersecurity are however highly fragmented and/or unknown. One way to increase the understanding of both the cybersecurity system and the environmental law regime, and thus to contribute to their development and formation, is to highlight the parallels of the regimes and how one system can serve as a source of inspiration for the other, with the aim of increasing the effectiveness of both. As noted earlier, an example of a cybersecurity treaty is the Budapest Convention under which the parties cooperate to combat cybercrime. Contrary to the climate agreements, the Budapest convention however allows for reservations, which permits states to opt out from specific provisions, thus potentially weakening the regime (although aiming to expand participation and speed entry into force).

A comparison between the cybersecurity- and the climate regime reveals that a substantial amount of regulations, including the necessary multi-regulatory dimensions, applicable to global commons exists within the respective frameworks. Nevertheless, the current governance is not sufficient to cover the gaps in cybersecurity. For example, in the case of a cyber-attack on a CI, there is total absence of binding international cyber law below the armed-attack threshold. The armed-attack threshold is the line at which the law of war is activated. The problem of the armed-attack threshold has not been solved by the Tallinn Manual 2.0 of 2017, an otherwise valuable tool to understand and assess the international law applicable to cyber-threats (Schmitt, 2017).[23] Several bilateral and multilateral agreements are applicable in order to secure cyberspace. In addition to the Budapest Convention, there are dozens of MLTAs that can be applied to seek criminal prosecution of cyber-attacks and that specifically mention Internet Law (IT) and which are broad enough to cover all law enforcement investigations. What is missing in these cybersecurity agreements are the enforcement provisions, the verification mechanisms, the sharing information systems, and compliance dispute settlement' mechanisms. Although the Paris Agreement does not contain enforcement mechanisms or dispute settlement mechanisms, the lack of right of reservation, the verification mechanisms and the bottom-up approach enclosed in the Agreement implies that it can still serve as a source of inspiration for the international law responses regarding cybersecurity. On the other hand, the information sharing mechanisms and the increasing number of ratifications typical of the cybersecurity treaties, such as in the case of the MLTAs and the Budapest Convention, could certainly inspire the climate regime and end up reinforcing cooperation and increasing the number of ratifying states, a number that in the case of the Budapest Convention has been considerably increasing. The information sharing mechanisms and verification mechanisms are also crucial to avoid the problem of free-riders and to help prevent the

[23]See Schmitt, 2017. This 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 possible application of international laws related to cyber uses of forces and armed conflicts involving cyber operations.

overuse of resources and the tragedy of the commons, thus enhancing international cooperation and effectiveness.

3. Confronting, Comparing and Coordinating Environmental Law and Policy to Cyberspace, Cybersecurity and Cyber-Threats

Drawing a parallel between the environmental law regime and the cybersecurity regime is also fruitful to understand the gaps in the cybersecurity realm. As noted above, several aspects of the cybersecurity regime are still unknown and highly fragmented. This section therefore explores how the environmental law regime, and in particular the environmental liability framework, can be coordinated with the cybersecurity regime. This is done by analyzing key aspects of environmental law, primarily concepts and principles, which are then compared to corresponding aspects of cybersecurity. For the comparison, a multilevel governance perspective is applied; sources of law and policy existing at global, regional and national levels are analyzed in order to understand the interactions between different levels on the focal points of each regime.

3.1. Environmental Damage and Damage from Cyber-Threats

One example of crucial focal points from the environmental liability regime is the problem of the identification of the author of the damage or the potential polluter. The identification of the author of the environmental damage (i.e. pollution due to climate change) is often very difficult because it is difficult to identify the source of pollution. The same can be said for cyber-damages, as it is often impossible to identify the source and the author of the cyber-threat or cyber-attack. Both regimes present anomalies compared to other regimes. In the environmental law context, these anomalies exist because ordinary rules targeted at the causality link do not achieve positive results, primarily because the logic behind the traditional vision of the causality link, i.e. the link between the author of the damage and the event that is necessary to attribute liability, is a mechanical logic (Cassotta, 2012).

In environmental law there is no such mechanical logic and it is often impossible to identify the author of the damage, for instance in the case of acid rains or remoteness of the damage or cumulative emissions.

Also in the case of cyber-threats or cyber-attacks, the identification of the author of the damage and the source and origin of cyber-attacks is extremely complex (Lalou et al., 2017). This is a fundamental problem in cybersecurity digital forensics. It is often extremely difficult to definitively name a perpetrator after a cyber attack (Newman, 2018). Hackers have a lot of technical tools to cover their tracks at their disposal and even if analysts figure out which computer a hacker used, it is still difficult to determine who used it. This is known as the "attribution problem" which makes it cumbersome to establish causation and liability as a consequence of the cyber damage. The problem of causation in environmental

and cyber damage can explain why it is difficult to apply the Polluter-Pays Principle in these regimes; if there is no polluter, there is no one to be held liable. Moreover, what it the damage and how should it be quantified? How much should be paid for compensation and how should transboundary damages be dealt with? Etc. All these are anomalies pertain to both regimes.

Analyses based on crucial focal points and solutions offered by the environmental law regime are applicable to the cyber regime, here among environmental concepts and principles as well as aspects related to liability, insurance and environmental policy tools, as is explained in the following sub-sections (from 3.2 to 3.3.4).

3.2. Environmental Pollution and Cyber-Pollution

The problem of overuse thus pertains both to the realm of environmental law, specifically to air and water pollution, and cyberspace. Both regimes are potential victims of the tragedy of the commons.[24] In cyberspace, for example, "information pollution" can occur as a result of a massive amount of spam messages that consume limited bandwidth. Likewise, the destruction of the atmosphere is the result of many individuals (companies, industries etc.) "maximizing their own utility" without regard for the consequences as these are carried by all. In cybersecurity, information pollution can be due to distributed denial of service attacks that can cause websites that have been targeted to literally crash, which can be caused by a massive amount of requests for website access (Bray, 2008; Ophardt, 2010). It can however also occur as the result of lack of defined ownership or regulation, causing individuals to overuse "their space". Similarly, the atmosphere is highly subject to atmospheric pollution and does not have an unlimited storage capacity, which in turn calls for governance, specifically for responses that limit the open access to nature overexploitation and mitigate human anthropogenic behavior. Such limits can be materialized e.g. through privatization measures that aim for the establishment of well-defined property rights, or through the public sector, for instance through the implementation of policy instruments, such as the cap-and-trade system under the Kyoto Protocol, which also has the capacity to prevent free-riders, or through taxes or quotas.

In the case of both environmental pollution and cyber-pollution, the major challenge is to identify the polluter (environment) and the perpetrator and the source (cyberspace). Against the proliferation of cyber-attacks, there are often no governance mechanisms and regulations in place, neither to punish or to prevent damage. Nor is there an effective governance response to the problem of greenhouse gas emissions causing climate change.[25] Since both environmental pollution due to GHG emissions and cyber-pollution are by nature global phe-

[24]For an explanation of the connection between the "*tragedy of the commons*" and the two regimes (environmental and cybersecurity), see Sections 2.3-2.4.

[25]Interesting to note, one country, Thailand, however has in place a mechanism to regulate information pollution. The mechanism of regulation put into place by Thailand is the "National Broadcasting and Telecommunication Commission" ("NBTC") that has acted to reduce information pollution in Southeast Asia with regards to SMS spam and data roaming fees.

nomenon it can be adducted that even though many countries have in place regulatory frameworks that are "effective" or has the potential of being effective at least, it does not solve the problem. The way to govern cybersecurity and climate issues is to not only depend on one level of regulation, as previously mentioned in section 2.5.1.

3.3. Environmental Concepts and Environmental Law Principles Applied to Cyberspace

Environmental law principles and concepts can provide interesting insights to better understand and design cybersecurity regimes. One important concept in this regard is sustainable development. Together with the practices and doctrines forming international law, sustainable development represents important starting points applicable to cyberspace. Principles of environmental law, such as the Polluter-Pays-Principle and the Precautionary principle, offer established platforms from which cyber-security can be analyzed. Internet and cyber-security are very important tools for economic development with healthy and stable global systems. It is thus crucial that the goal also for cybersecurity is "sustainability" and stability, which in turn calls for a new type of important matrix within the concept of sustainable development, one that links environmental and economic issues with cyber-security law.

3.3.1. The Concept of Sustainable Development, the Polluter-Pays Principle and the Precautionary Principle

The Brundtland Report defines sustainable development as "*Development that meets the needs of the present without compromising the ability of future generations to meet their own needs*" (Report "Our Common Future", Brundtland, 1987).[26] Sustainable development as a concept in international law has evolved from the original into three pillars: economic and social development along with environmental protection. It has been acknowledged that practices and doctrines from international law on sustainable development are applicable to cyberspace (Shackelford, 2016). Cyber-security has to be sustainable to ensure economic and human development, as well as environmental protection. Therefore, there is an important interconnection within the concept of sustainable development that links environmental and economic issues with cybersecurity law. For example, sustainability in the context of a legal framework for governing the exposure of critical infrastructures that are very much exposed to environmental conditions to possible cyber-threats (i.e. energy sector, oil and gas, electricity or nuclear), must account not only for present cyber-threats but for those of the future. Concretely, in the case of a power outage caused by a cyber-attack, a newly built facility must withstand a flood of a higher severity that the historic highs suggest.

[26]The concept of "sustainable development" can be traced back from a United Nations (UN) ad hoc Report "*World Commission on Environment and Development*" chaired by Gro Harlem Brundtland who in 1987 produced a report titled "Our Common Future" for the UN.

The Polluter-Pays Principle establishes the requirement that the costs of pollution should be borne by the persons responsible for causing the pollution (Jan, 2008). The Polluter-Pays Principle is closely related to the rules governing civil and state liability for environmental damage (De Sadeleer, 2006a, 2006b). The positive aspects in the linkage between civil liability and the Polluter-Pays Principle have been highlighted by several authors whom have defined the Polluter-Pays Principle as a good instrument operating as an incentive to lower pollution in a way in which it is not the tax-payer whom has to pay but rather the polluter (Kramer, 2007). In that sense, it is important to ensure standards and environmental liability schemes in which it is the persons who are responsible for the pollution who shall bear the costs (OECD, 1974, 1977, 1989).[27] The Polluter-Pays Principle can be used for allocating damage due to a cyber-attack, including environmental harm, as well as to offset the costs of dealing with "cyber-pollution"—persistent activity aimed at overwhelming CI that is yet to manifest in a full-scale cyber-attack. However, the applicability of the Polluter-Pays Principle to cyber pollution should also take into account some challenges in the relationship between Polluter-Pays Principle and the sphere of civil liability, *i.e.*: who the polluter is, what the damage is, or how much compensation should be paid. Also in case of cyber (potential) damage, it would be difficult to determine the causality link where by the need to develop a robust insurance market or compensation funds willing to provide coverage for the diffuse and transboundary character of these kinds of polluting activities.

The precautionary principle aims to provide guidance e.g. in the development and application of international environmental law where there is scientific evidence of uncertainty (De Sadeleer, 2007). This principle also reflects the eternal dilemma of how best to establish a balance between economic growth and protection of the environment (The World Charter for Nature adopted by the

[27]The Polluter-Pays Principle is a norm of that transitioned from a non-legal recommendation to a central principle of environmental law (Principle 16 of the Rio Declaration)—and entails that the polluter should bear the costs of carrying out the pollution prevention and control measures decided by public authorities to ensure that the environment is in an acceptable state. According to the original recommendation, the Polluter-Pays principle should not be accompanied by subsidies that would create significant distortions in international trade and investments. In 1989, the OECD Council established the implications of the Polluter-Pays Principle also in the matter of accidental pollution and concluded that "the operator of a hazardous installation should bear the costs of reasonable measures to prevent and control accidental pollution from that installation which are introduced by public authorities (…) in order to protect human health or the environment. Three years later, the principle made its way into the Rio Declaration on Environment and Development where Principle 16 contains a formulation similar to the one established by the OECD: "*National authorities should endeavor to promote the internalization of environmental costs and the use of economic instruments, taking into account the approach that the polluter should, in principle, bear the costs of pollution, with due regard to the public interest and without distorting international trade and investment*". See also several recommendations of the OEDC, specifically: OECD (1977), *Recommendation of the Council on Guiding Principles concerning International Economic Aspects of Environmental policies*, 26 May 1972-C (72) 128; OECD (1974); *Recommendation of the Council on the Implementation of the Polluter-Pays Principle*, 14 November, 1974-C (74) 223; OECD (1989); and finally, *Recommendation of the Council concerning the Application of the Polluter-Pays Principle to Accidental Pollution,* 7 July 1989-C (89) 88/FINAL.

United Nations General Assembly of 1992).[28] The precautionary principle can guide digitizing the existing CI and/or siting and permitting new CI facilities. For example, if the effects of cyber-attacks under environmental threatened climatic conditions are unknown, the CI facility should not be built. In this instance, applying the precautionary principle can serve as a safeguard against the risks of environmental damage and human security disruption. In the environmental business sector, application of the precautionary principle can be difficult if costs are not "internationalized". The concept of internationalization of externalities, e.g. pollution, implies that the potential polluter, i.e. the operator, should include, in the costs of production, also the costs for the environmental damage caused by the activity. This is similar to cyber business activities, which often do not take necessary measures against possible cyber-threats, and such externalities are not internationalized. This mirrors the difficulty in dealing with the private sector in matters of cybersecurity. They are often part of the problem because, when maximizing profits, the business sectors are not prepared to adopt the necessary precautionary measures, with the resulting risks of leaving entire sectors that are heavily digitalized, such as CI, without protection and thus exposed to attacks that can exploit vulnerabilities. The costs of the risks of cyber-attacks should therefore be internationalized in the same way as the business sector exposed to environmental pollution is practicing.

3.3.2. Best Available Practices, Best Available Technologies, ISO Certificates Applied to Critical Infrastructures

The connection between sustainability and cybersecurity is the need for our civil societies to be based on social and economic progress and sustainable development. In the management of cyber-threats, often not only the public sector, but also the private sector is involved in managing the interests of stakeholders. The private sector is often faced with managing cyber-threats as part of an effort to build "trust" with different groups of business activities, such as joint ventures, mixed agreement, hybrid business practices or corporate social responsibility (CSR) and practices (Shackelford, 2016) Trust means a level of confidence that a computer system will behave as expected. The management of cyber-threats to CI or industry sectors highly digitalized can be based on instilling cyber-security's best available practices (BAP) and best available technologies (BAT) while expanding Internet access. Consensus standards are often necessary

[28]The Precautionary principle entails that when an activity poses a risk, for example threatens to harm human health or the environment, precautionary measures must be taken. On an international level, it follows from the Rio Declaration that "(*w*)*here there are threats of serious or irreversible damage, lack of full certainty shall not be used as a reason for postponing measures to prevent environmental degradation*." Thus scientific uncertainty is not a reason for postponing measures action to avoid potentially serious or irreversible harm to the environment. Key aspects are thus anticipation, a long-term perspective and a shift of the burden of proof to the actor. In tangible terms, for example in connection with specific activities, this entails an inclusive assessment of the activity, resulting in concrete requirements for precautionary measures to prevent adverse social and environmental impacts. The precautionary principle was first recognized in 1992, in the World Charter for Nature adopted by the United Nations General Assembly and subsequently incorporated into various environmental related conventions.

to harmonize standards, and industry best practices provide flexible and cost-effective approaches to enhance cyber-security measures that assist owners and operators of CI in assessing and managing the risks. In cases where sustainable business practices are equipped to deal with issues of "trust," cyber security and cyber peace can offer business models on which to grow business practices.

This would require a new paradigm of "sustainable climate cyber security" that relies on the intention to protect business and industries that are highly digitalized, such as in the case of CI, to literally be conceived and perceived through the prism of environmental law and sustainability when linked to cybersecurity.

Sustainability fails if the linkage between highly digitalized business sectors exposed to environmental conditions and potentially polluting are not governed through laws. Other tools drawn from sustainable development beyond integrated reporting can also be applied to enhance cyber-security. For example, the private sector could also begin to develop the equivalent of Leadership in energy and Environmental Design (LEED standards), which would help identify firms with best options to achieve cyber-security. This is applied for example in green buildings where everything from building design and construction to maintenance and neighborhood development is digitalized but must be provided with a "LEED-Type certification scheme". This is a flexible and cost effective approach that enhances cybersecurity by assisting owners and operators controlling an activity in assessing and managing the cyber risks and provides a map of cybersecurity best practices.

3.3.3. Liability

Civil liability is the liability or legal obligation that anyone has, to repair a wrong (or a tort) or a breach inflicted to another where for example subject x commit a damage to y and subject x is obliged to compensate according to law or regulations which can be contained in civil codes or in jurisprudence. There are two main prerequisites for liability: 1) the existence of the causality link and 2) the existence of the subjective element of culpa. Therefore, the classical archetype that is found in all civil codes is: subject x causes damage to subject y, subject x must repair. However, problems arise when this archetype is applied to environmental damage or environmental pollution because the goods belonging to subject y (which is the environment that has been damaged) do not belong to anyone, as it may not have owners (Cassotta, 2012).

This is quite similar to the cyberspace, which is not owned by anyone, as the flow of information that constitutes its space is a virtual space. In the case of damage to the environment, or to natural resources (which includes the air), enterprises or the private sector of production-consumption activity, have to bear the costs. The enterprises have to internalize the external costs[29] in such a way

[29]The concept of internationalization of external costs relates to the activity of the potential polluter. The polluter is in this way (through the mechanism of the instrument of civil liability) forced to also include in its costs for production the costs that could emerge from environmental damage through a mechanism called "internationalization".

that it is not society that bears the costs, but solely the polluter who is forced, through the mechanism of civil liability, to pay and it that sense apply the Polluter-pays principle concretely. This is a reasoning originating from economic theories advocating that efficiency in achieving the goal of environmental protection is achieved when all the external costs are taken into account (Oates, 1992). Therefore, "internationalization" is a mechanism remedying the externalities that have to be understood as "external effects" of the production-consumption activity of individuals (Oates, 1992).

Sometimes regulations related to the so-called low probability-high risk industries, such as nuclear power plants are detailed and in other cases they are vague. Adding regulation would force the private sector operating under cyber-security rules and exposed to the risk of cyber threat, to invest more resources in protection or resilience of the systems they own or operate. This would not be welcomed by many operators, especially of CI, because markets are externalizing CI risks at present, whereas state regulation would mean establishing "liability rules based on the notion that organization should internalize the costs of the risks they produce and that by internalizing them, they will make wise choices about the technologies they use" (Pursiainen, 2018). According to one author (Pursiainen, 2018), this would require a well-functioning tort liability legislation that would make it easy for the consumer, both public and private, to demand compensation for losses incurred by CI failures or enterprises heavily digitalized with vulnerable holes that could be exposed to cyber-threats. In the substance, lessons learned from the environmental liability system and applied to the cyber-security regime can force the industry to pay more attention to cybersecurity, to invest more and to make the cybersecurity regime effective and to use liability as an instrument to apply sustainable development not only in the environmental area but also in the cybersecurity regime facilitating the shift toward a sustainable cyber security.

3.3.4. Insurance and Critical Infrastructures

The main task of an insurance system in the context of environmental law managing the environmental risk (Monti, 2001). The problem of how to best link insurance and civil liability in the environmental field, points to a constant and common concern at international, regional and domestic regulatory levels. The main problem in environmental insurance schemes is to make it fit into the mechanism of civil liability without the insurance coverage being transformed into a "legal certificate of pollution", thus providing the insurance system with a serious working instrument aimed at preventing environmental damage. In addition, the difficulties associated with "quantifying" the environmental damage may also turn out to be difficult for those who have draft insurance policies. The lack of information about losses and damages does not help with the problem of quantification. The same applies to cybersecurity, especially in relation to CI that seem to be particularly at risk of cyber-attacks and where calculating both the risk of an attack and the costs of cyber-attacks appears to be a very difficult task.

Businesses often suffer from a lack of information about losses and possible damages (Republican, 2011). The creation of an insurance system in the cyber-security regime raises the dilemma of how to best handle the private sector's role in cyberspace. In case of maximization of profit, some industries and business sectors do not take the necessary precautions, thereby leaving them open to attacks that exploit old vulnerabilities. This is particularly evident when the costs of cyber-attacks are not internalized. Doubts can thus be raised about the free market's ability to enhance cybersecurity and call for the necessary national regulation, even though it is not easy for a regulator to catch up with the rapidity of the changing cyber-threats matrix. A possible option for those governing the cybersecurity regime is therefore to create a risk insurance market.

To sum up this section has explored the nexus between climate change, environmental threats, and cyber-threats and the analysis has been conducted with the precise aim to draw a parallel between environmental regulations and the cyber space and cybersecurity systems. Many aspects of the cyber-security system are not known and are highly fragmented. Selected focal points have been detected and the analysis has been developed in parallel to the environmental regime in order to better understand how to improve the effectiveness of the cyber complex regime in a contextual perspective. This brings evidence on how to take inspiration from a regime system (environmental law or, more concretely, the environmental liability framework) and use it as source of inspiration to understand and shape the formation of another system in another area, namely cyber-security, as well as how to apply the analysis to other sources of law and policy in a multi-level perspective, as will be shown in the next sections.

4. EU Level

The EU level environmental law and policy is of course particularly inspiring for EU level cybersecurity and information system across the Union, especially in connection with CI, for example in terms of who is the author of the damage, or the perpetrator, and regarding which entity is responsible to take action, as well as in terms of risk and information sharing. This is visible when comparing selected focal points of the two most significant and most recent pieces of secondary legislation, the Environmental Liability Directive on the Prevention and Remedying of Environmental Damage 2004/35/EC (Environmental Liability Directive 2004/35/EC with Regards the Prevention and Remedying of Environmental Damage as Adopted by the European Parliament and of the Council of 2004),[30] and the Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (Directive 2016/1148 of the European Parliament and the Council of 6 July concerning measures for a High Common Level of Security of Network and Information

[30]Environmental Liability Directive 2004/35/EC with regards the Prevention and Remedying of Environmental Damage as adopted by the European Parliament and of the Council on the 21 April 2004, OJ, 2004, 143/56, the abbreviated version "ELD" will be used in this article.

System across the Union of 2016)[31], both of which are treated in the following. When comparing the sources of law at EU level in two different areas (environmental law and cyber law and cybersecurity) in order to grasp key aspects of both regimes, both the global and domestic dimensions are taken into consideration, as this will increase the understanding of how to improve the cybersecurity regime using a multi-regulatory perspective. As mentioned in section 2.5.1, problems related to effectiveness and enforcement often require a bottom-up approach and action. Section 4 includes an assessment of vertical implementation of international law via regional law (EU law), but also a horizontal implementation of regional law at national levels (including national strategies and activities plans involving the civil society). Understanding implementation requires observation on how regional law (EU law, see Section 4) is implemented at domestic level. In Section 5, the transposition and implementation of regional law on national level, using the Swedish legal order as an example, is observed. This enables for the detection of any room for improvement at a national level, through a global-local approach, in turn inspiring not only the domestic levels but all the levels of regulation. This case study also ascertains if the detection and identification of the key focal points at global and regional levels analyzed in the previous sections are applicable in the domestic Swedish case.

4.1. Environmental Liability Directive 2004/35/EC on the Prevention and Remedying of Environmental Damage

The overall objective of the Environmental Liability Directive (hereinafter "the ELD") is to establish a common European framework on environmental liability for environmental damage, air, water, land and protected species and natural resources applicable to all member states. The ELD has threefold goals within this framework, which are: to harmonize environmental liability by establishing common criteria to which national legislators will have to conform, to ensure the applicability of the Polluter-Pays Principle, and to eliminate situations of internal market distortion and to secure trade. The ELD has an important ambition to promote and implement the concept of sustainable development, which has to be understood as a value and ensure its applicability by launching a new pattern of environmental protection, sustaining economic growth based on the necessity to follow a new model of qualitative rather than quantitative environmental production. Therefore, the ELD becomes an instrument in applying environmentally sustainable development production by preventing environmental damage through the Polluter-Pays Principle. The Polluter-Pays Principle is connected with the Precautionary principle especially in handling risks activities or pollution by forcing operators to take measures, as they will otherwise have to pay if the damage occurs. The ELD contains a very important innovation, which carries of a strong message: it is the operator which has in *primis* the obligation

[31]Directive 2016/1148 of the European Parliament and the Council of 6 July concerning measures for a High Common Level of Security of Network and Information System across the Union, OJ, 2016, 194 R 000, the abbreviated version "NIS" will be used in this article.

to act, protect and maintain the environment and that a relationship must be established between the operator and the Polluter-Pays Principle.

The focus on the "potential responsible party", who thus must pay for the pollution, reinforces the effectiveness of the regime and facilitates implementation. On the other hand, among the problematic aspects of the ELD are the identification of the author of the damage and the time factor, for example in case of cumulative effects or in the case of acid rain where the effects of pollution reverberates at long distance and it is difficult to identify how many polluters there are. In that case the ELD does not consider joint and several liabilities and past and present pollution, which open the path toward a new liability solution which also would include damage from diffuse pollution such as the GHG-emission causing climate change (Cassotta, 2012).

Information sharing is contemplated in Art. 15 of the ELD: "*where environmental damage affects or is likely to affect several member states, those Member States shall cooperate, including through appropriate exchange of information with the view to ensuring that preventative actions, and were necessary remedial actions is taken in respect of any such environmental damage. Where environmental damage has occurred, member states in whose territory the damage originated shall provide sufficiently information to the potentially affected Member States*".

4.2. Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union

With Directive 2016/1148 (hereinafter the NIS Directive), the EU establishes its normative system concerning measures for a high common level of security of network and information system across the Union. The Directive regulates the information system security for two types of entities, which are the "operators" of "essential services" (i.e. critical infrastructure operators) and digital services providers. The term is defined in the directive as an entity that provides a service that 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. 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. The Directive contemplates

the need to raise the level of protection of the CI against cyber-threats, the global and transboundary nature of the cyber-threats to some CI that do not have only national character but rather global nature, (i.e. oil pipes, internet cables but also airlines, traffic control networks, or satellite constellations). This has been the object of discussion of the European Commission before and after the NIS Directive and even before starting any joint initiatives in Cyber Defence involving European Defence Agency (EDA) and within the Permanent Structured Cooperation on Security and Defence (PESCO) context within the context of the NIS Directive. The NIS Directive recognizes the need of strong cooperation in order to align standard and most importantly to share information on systems, protocols and technologies and recognizes the high degree of interdependencies and interconnection between CI, i.e. between energy, oil and gas, electricity, transportation, nuclear etc. and this interconnection is not only across national borders but also transnational. The Directive also recognizes the need to tackle risks and vulnerabilities and the problem of identification of the perpetrator by enhancing resilience, information sharing and by recognizing the costs required to build security and resilience as part of the company's governance.

Enhancing cooperation and individualizing the entity responsible to act and take measures during cyber-threats is of importance, as stated in Art. 5.3 "…*where an entity provides a service as referred to in point (a) of paragraph 2 in two or more Member States, those Member States shall engage in consultation with each other*…" and that, as stated in Art. 17.3, "…*if a digital service provider has its main establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, the competent authority of the Member State of the main establishment or of the representative and competent authorities of those other Member States shall cooperate and assist each other as necessary*". Such assistance and cooperation may cover information exchanges between competent authorities concerned and requests to take the supervisory measures.

5. Elements of Environmental Law and Policy Applied to Cyber-Threats in Sweden

In June 2017, the Swedish government launched a national strategy for cyber security, in part to comply with the NIS Directive. There is no deadline for the implementation of the strategy; rather, the rapid developments in the area are expected to require flexibility for quick adaptation to international and EU policy and legal developments. In order to create the necessary long-term conditions for all stakeholders to effectively address cybersecurity, the strategy outlines six priority areas:

- Securing a systematic and comprehensive approach in cyber security efforts, e.g. by developing a model for risk assessment;
- Enhancing network, product and system security without compromising confidentiality, correctness and access;
- Enhancing the capability to prevent, detect and manage cyber attacks and

other IT incidents;

- Increasing the possibility of preventing and combating cybercrime;
- Increasing knowledge and promoting expertise, e.g. through education and research; and
- Enhancing international cooperation, for example by applying international law principle to the cyber security domain.

In general, the knowledge gap—or potential for development—regarding information—and cyber security in Sweden is considered large. One objective is therefore to increase the knowledge about the most urgent vulnerabilities and needs for security measures both for society as a whole and for individual users of such technology. A systematic and coherent approach to information- and cyber security is expected to contribute to more uniform assessments of threats, risks and necessary security measures. With a coherent information system, different actors are expected to be more likely to reach the same security level. Most importantly, a national model is expected to raise the minimum level of security, first of all for authorities, but also for other actors in both the public and the private sector (Justitiedepartementet/Justice Department, 2017).

The strategy stresses that the work on securing society's cyber security needs long-term strategies based on core values such as the protection of privacy. Many interdisciplinary issues are considered relevant in this context; from advanced technical matters to organization culture and behavioral science. The strategy mentions, for example, the development of self-driving cars and intelligent cities, which requires consideration of both sociotechnical, legal and ethical issues directly related to cyber security (Justitiedepartementet/Justice Department, 2017). Also education and practice are considered important elements of the strategy as it increases knowledge as well as strengthens actors' and activities' resilience to IT-related incidents: "Regular exercises both nationally and internationally are a prerequisite for developing and evaluating structures for managing serious IT incidents and for identifying organizational, technical and administrative development needs." (Justitiedepartementet/Justice Department, 2017).[32]

It is pointed out that, while there is international consensus within the UN regarding the applicability of international law in the cyber area, considerable difficulties and challenges related to the interpretation and hence the implementation of the rules remain. Sweden opposes a state-controlled Internet, but supports the possibilities to apply international legal frameworks to verify, point out and demand responsibility. The need for Sweden to take an active role in this development is stressed (Justitiedepartementet/Justice Department, 2017), In relation to international trade and economic cooperation, the position of the Swedish government is that "cybersecurity must be guaranteed within the framework of the overall ambition to promote innovations, competitiveness and societal development." It is furthermore considered important to uphold free data

[32]Justitiedepartementet/Justice Department (2017), Skr. 2016/17:213. Nationell strategi för samhällets informations och cybersäkerhet/*National Strategy for Society's Information- and Cybersecurity*. P. 29.

flows and counteract digital protectionism, e.g. in the form of localization requirement that imply that data must be stored in the home country. In all, it is strongly emphasized that the strive towards cybersecurity must not interfere with, or hamper, trade relations, neither within the EU nor outside.

In 2018, *Act on information security for important and digital services* entered into force. The purpose of the act is, in keeping with the NIS Directive[33], to achieve a high level of security for networks and information systems for socially important sectors, including energy, transport, banking, financial market infrastructure, digital infrastructure, and digital services (Act, 2018:1174).[34] To ensure a level of security that is appropriate in relation to the risk, as well as the continuity of the services, suppliers of such vital public services shall: a) conduct systematic and risk-based information security work on networks and information systems; and b) take appropriate and proportionate technical and organizational measures to manage risks that threaten the security of networks and information systems, as well as prevent and minimize the effects of incidents that affect networks and information systems. Basically the same requirements and for the same reasons are imposed on suppliers of digital services: they shall take the technical and organizational measures they consider effective and proportionate to manage risks that threaten the security of networks and information systems used when providing digital services (Act, 2018:1174).[35]

The Swedish strategy thus focuses primarily on two aspects: first and foremost, the safeguarding of basic values, such as democracy, legal certainty and human rights, and secondly to implement EU legislation. Some elements of environmental law and policy can be traced here, for example that all measures must be proportionate and effective, and the emphasis on the need to balance different interests, such as the protection against cyber threats versus property rights, in the risk assessment.

6. Conclusion

By comparing the environmental regulation system with the cyber security system, interesting conclusions can be drawn; the (quite significant) parallels between the two systems allow for increased understanding of how to integrate some key aspects.

This article has demonstrated that one way to better understand the complexity of the cybersecurity system, not least in terms of the regulatory challenges facing most countries, is to try to find solutions within existing similar systems. In this article we have conducted a cross-area and interdisciplinary study involving both the cybersecurity system and the environmental regulation system. The study aims to examine how to best coordinate these systems, thus making them more effective. To this end, we have collected evidence on how characte-

[33]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.
[34]Act (2018:1174) on information security for important and digital services, s. 1.
[35]Act (2018:1174) on information security for important and digital services, s. 11-16.

ristics from one regime system, the environmental regulation system—or more specifically, the environmental liability framework, can be used as source of inspiration to understand and shape the formation of another system, namely cybersecurity. This research thus puts forward a new approach for addressing regulatory challenges. In light of a basic assumption that there are great similarities between different regulatory regimes at *system* level, key aspects of one system are analyzed and compared to corresponding aspects of another system, with the aim of improving both systems. In this article, the environmental regulation system, primarily concepts and principles, is selected as the starting point for the comparison. It seems particularly appropriate to try to profit from the sustainability perspective that permeates this regime when designing overarching solutions to increase cybersecurity. As the more recently developed regime, the cybersecurity system is thus the main recipient of the analysis, although the aim of the research is of course cross-fertilization.

When conducting the comparison, multi-level governance concepts have been applied. This entails analysis of the sources of law and policy existing at international, regional and national levels in order to understand the interactions between these interdependent levels. For example, challenges at national level, as in the case of Sweden, can be tackled in a "global-local approach" so as to improve national law in terms of effectiveness of regulation. While the Swedish model is in agreement with some focal points compared to the EU and international level, there is naturally room for improvement in a system this new. With the knowledge produced in this research, we hope to inspire legislators at all levels. The comparison could lead to a compact, unified approach. The challenges facing the cybersecurity domain cannot be met by domestic law and policy alone.

Some elements of the examined systems are "constant" at all levels in the parallel between cybersecurity and environmental regulation, including climate space: a) the need for a multilayer approach; the necessity of designing the system upon principles (e.g. of international and environmental law); the importance of international cooperation, not least regarding information sharing; interaction between public/private sectors; and the diffusion of technical knowledge, *i.e.*, the attentive consultation of risk assessment.

Given the multiple deficiencies that exist in the examined regimes, policy-makers, managers and treaty makers operating in the area of cybersecurity need to be better informed about the transition from cybersecurity towards "sustainable cybersecurity behavior" that is currently taking place. This article has suggested new perspectives on how the effectiveness of the cybersecurity regime can be improved, with practical examples on how to overcome gaps and deficiencies in a way that would reinforce the regime, amongst other: the creation of a risk insurance market; ways to avoid the problems of free-riders; and how to mitigate the tragedy of commons. The suggestions are based on inspiration from the examined regimes, both in terms of treaty making, private practices and the ways in which different interests are balanced in the risk assessment, for example regarding the protection against cyber threats through international

(environmental) law principles and tools *versus* property rights and other private interests.

Acknowledgements

This article is a deliverable of a research project granted from Nord Forsk (Grant n. 81039) 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.

Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

Act (2018:1174). *Act on Information Security for Important and Digital Services* (p. 1, pp. 11-16).

Baush, C., & Mehling, M. (2013). Alternative Venues of Climate Cooperation: An Institutional Perspective. In E. Hollo et al. (Eds.), *Climate Change and the Law* (pp. 117-119). Berlin: Springer.

Bray, D. A. (2008). Information Pollution, Knowledge Overload, Limited Attention Spans and Our Responsibilities as IS Professionals. *Global Information Technology Management Association (GITMA) World Conference*, June 2008. https://doi.org/10.2139/ssrn.962732

Cassotta, S. (2012). *Environmental Damage and Liability Problems in a Multilevel Context: The Case of the Environmental Liability Directive*. The Netherlands: Kluwer Law International.

Cybersecurity Forum (2013-18). Pivot Point Technology Corp.

De Sadeleer, N. (2006a). Polluter-Pays Precautionary Principle and Liability. In G. Betlem, & E. Brans (Eds.), *Environmental Liability. The 2004 Directive Compared with US and Member States Law*. Cameron.

De Sadeleer, N. (2006b). *Les responsabilité environmentales dans l'espace européen—Point de vue Franco-Belge*. Bruxelles: Brulant.

De Sadeleer, N. (2007). *Implementing the Precautionary Principle*. Approaches from The Nordic Countries, EU and USA, Earthscan.

Directive 2016/1148 of the European Parliament and the Council of 6 July Concerning Measures for a High Common Level of Security of Network and Information System across the Union, OJ, 2016, 194 R 000.

Environmental Liability Directive 2004/35/EC with Regards the Prevention and Remedying of Environmental Damage as Adopted by the European Parliament and of the Council on the 21 April 2004, OJ, 2004, 143/56.

European Commission COM (2004). 702 of 20 October 2004.

Fidler, D. (2015). *Whither the Web: International Law, Cybersecurity, and Critical Infrastructure Protection.* Bloomington, IN: Law Library Indiana University Press.

Frakes, J. (2003). *The Common Heritage and Mankind Principle and the Deep Seabed, Outer Space, and Antarctica: Will Developed and Developing Nations Reach a Compromise?* 21, Wis. Int'L L.J., 409.

Hansel, M. (2013). Cyber-Security Governance and the Theory of Public Goods. 27 June 2013, *E-International Relations*.

Hardin, G. (1968). The Tragedy of the Commons. *Science, 162,* 1243-1248. https://doi.org/10.1126/science.162.3859.1243

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

Jan, J. H. (2008). *European Environmental Law*. Amsterdam: European Law Publishing.

Jensen, E. T. (2014). State Obligations in Cyber Operations. In *Baltic Yearbook of International Law* (Vol. 14, No. 1). Provo, UT: Bingham Young University School of Law. https://doi.org/10.1163/22115897-90000121

Justitiedepartementet/Justice Department (2017). Skr. 2016/17:213. Nationell strategi för samhällets informations-och cybersäkerhet. *National Strategy for Society's Information- and Cybersecurity.*

Kramer, L. (2007). *EC Environmental Law*. London: Thomson-Sweet and Maxwell.

Lalou, M. et al. (2017). Identifying the Cyber Attack Origin with Partial Observation: A Linear Regression Based Approach. *2nd IEEE International Workshop on Foundations and Applications of Self Systems*, Tucson, AZ, 18-22 September 2017, 18-22. https://doi.org/10.1109/FAS-W.2017.168

Monti, A. (2001). Environmental Risks: A Comparative Law and Economics Approach to Liability and Insurance. *European Review of Private Law, No. 1,* 51-79.

Newman, L. H. (2018). Hacker Lexicon: What Is the Attribution Problem? *Security*.

Nordhaus W. (2015). Climate Clubs: Overcoming Free-Riding in International Climate Policy. *American Economic Review, 105,* 1339-1370.

Oates, W. E. (1992). Environmental Economics: A Survey. *Journal of Economic Literature, 30,* 675-740.

Oberthür, S. et al. (2012). *Managing Institutional Complex: Regime Interplay and Global Environmental Change.* Cambridge, MA: MIT Press.

OECD (1974). *Recommendation of the Council on the Implementation of the Polluter-Pays Principle*. 14 November 1974-C (74) 223.

OECD (1977). *Recommendation of the Council on Guiding Principles concerning International Economic Aspects of Environmental Policies*. 26 May 1972-C (72) 128.

OECD (1989). *Recommendation of the Council Concerning the Application of the Polluter-Pays Principle to Accidental Pollution.* 1989-C (89) 88/FINAL.

Ophardt, J. A. (2010). Cyberspace and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield. *Duke Law & Technology Review,* 1-28.

Oran, Y. (2012). Building and International Regime Complex for the Arctic: Current Status and Next Steps. *The Polar Journal, 2,* 391-407. https://doi.org/10.1080/2154896X.2012.735047

Protocol on Substances that Deplete the Ozone Layer (Montréal Protocol) of September 16 of 1987 to the Vienna Convention for the Protection of the Ozone Layer.

Pursiainen, C. (2018). Critical Infrastructure Resilience: A Nordic Model in the Making? *International Journal of Disaster Risk Reduction, 27,* 632-641. https://doi.org/10.1016/j.ijdrr.2017.08.006

Radzwill, Y. (2015). *Cyber-Attack and the Exploitable Imperfections of International Law*. Leiden, Boston: Brill Nijhoff. https://doi.org/10.1163/9789004298309

Redder, M. E., & Hughes, M. P. (2008). Global Commons and Domain Interrelationships: Time for a New Conceptual Framework? *Strategic Forum, National Defense University, SF No. 259,* 1-11.

Report "Our Common Future", Brundtland (1987). *"World Commission on Environment and Development"*, chaired by Gro Harlem Brundtland who in 1987 produced a report titled "*Our Common Future*" for the UN.

Republican, H. (2011). Cybersecurity Task Force, Conference Recommendation of the House Republican Cybersecurity. *Task Force's Recommendations*, 3, 8, 14.

Schmitt, N. M. (2017). Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum. *Harvard National Security Journal, 8,* 245.

Shackelford, S. (2016). On Climate Change and Cyber Attack: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems. *Vanderbilt Journal of Entertainment & Technology Law,* Kelley School of Business Research Paper No. 15-54. https://doi.org/10.2139/ssrn.2630333

The European Convention on Cybercrime (Council of Europe), CETS, No. 185, 23 November 2001, entered into force on the 1 July 2004.

The Kyoto Protocol adopted in Kyoto, Japan on 11 December 1997, entered into force on 16 February 2005.

The Montréal Protocol on Substances that Deplete the Ozone Layer to the Vienna Convention for the Protection of the Ozone layer, adopted in 1987 and came into force on 1 January 1989.

The Paris Agreement, signed on the 22 April 2016, entered into force on the 12 December 2016.

The United Nations Convention on Climate Change (UNFCCC) (1994). (The United Nations Convention on Climate Change, adopted on the 9 May1992, entered into force the 23 March of 1994.

Tsagourias, N., & Buchan, R. (2016). Chapter 14. Cyber-Threats and International Law. In E. M. Footer, J. Schmitt, 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 Publishing.