Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North

Article (Accepted Version)

Sustainable Cybersecurity? Rethinking Approaches to Protecting Energy Infrastructure in the European High North.

Sandra Cassotta, Associate Professor in International Environmental and Energy Law, Department of Law, Aalborg University and Research Fellow at the Institute for Security and Development Policy (ISDP), Stockholm, E-mail: sac@law.aau.dk

Roman Sidortsov, Assistant Professor of Energy Policy, Department of Social Science, Michigan Technological University, E-mail: sidortsov@cantab.net

Corresponding author: Sandra Cassotta, e-mail: *sac@law.aau.dk*

The work is a deliverable of the ECoHuCy Research Project (Enablement besides Constrains: Human Security and a Cyber Multi-disciplinary Framework in the European High North) supported by NORDFOSK 81030

Sustainable Cybersecurity? Rethinking Approaches to Protecting Energy Infrastructure in the European High North.

Abstract

Rapidly increasing digitization has positively contributed to economic and social development and helped increasing environmental protection. However, it also made socio-technical systems and ecosystems more vulnerable to cyber-threats. Critical infrastructure (CI) in the energy sector is particularly vulnerable to such threats. Remoteness, seasonal darkness, and severe climate that is becoming less predictable due to global climate change–the kind of conditions present in the Arctic European High North (EHN), for example–amplify the impacts of a potential cyber-attack. Although these exceptionally critical infrastructure conditions (ECIC), as we term them, pose inordinate and immense governance challenges, the existing national and international legal frameworks treat them in a fragmented manner. In this paper, we argue for rethinking the existing governance structures and propose an approach that connects cybersecurity and environmental governance. We outline the contours of a coherent and cohesive risk-based, pluralistic, and polycentric legal framework that we see as a critical part of the new ECIC governance regime. We draw upon the concept of sustainable development and the precautionary and polluter-pays principles of environmental law to propose three guiding principles for this framework.

Key words: Cybersecurity; Critical Infrastructure; Exceptionally Critical Infrastructure Conditions; Sustainable Cybersecurity; Resilience; Energy Sector, Environmental Governance

1. Introduction

In the past decade, cyber threats to critical infrastructure (CI) have become one of the most discussed topics in the energy policy and scholarly domains. The reason for the increased prevalence is rather simple – as energy systems become more digitized, they become more susceptible to frequent and devastating cyber-attacks (World Energy, 2016; EECSP, 2017; Skotnes, 2015). Yet despite impressive progress by researchers and policy-makers, several gaps remain. One such gap is the amplifying effect of the rapidly changing climate on the CI located in remote regions with severe climate conditions—the Arctic European High North (EHN), for example. As we argue in this paper, the possibility of a cyber-attack on CI subject to such conditions warrants elevating them to the level of *exceptionally critical* or, as we term them, exceptionally critical infrastructure conditions (ECIC).

To place the ECIC in the context of a past hostile cyber-intrusion, we refer to the 23 December 2015 attack on the electrical grid in Ukraine's capital Kiev. The attack, which was allegedly perpetrated by the Russian hacker group Sandworm, resulted in a six-hour blackout that affected hundreds of thousands of Ukrainians (Sullivan and Kamensky, 2017). If a similar attack were successfully launched in the Norwegian EHN, it would probably not immediately affect as many people as the 2015 attack in Kiev – after all, the Arctic is sparsely populated. However, ECIC such as remoteness, lack of daylight, oil and gas infrastructure interdependence, and severe weather conditions would

have made the impact more severe and the response more difficult. The rapidly changing climate – the Arctic is warming at a rate twice as fast as the rest of the world – would have amplified these conditions due to the elevated uncertainty (NOAA, 2014) (IPCC, 2007). For instance, emergency services would have been responding to something for which they were not fully prepared. In addition, it is likely that the impact would have extended beyond residential houses, hospitals, and schools. The Arctic and EHN in particular is home to CI that is instrumental to economies and national security of many countries, the oil and gas and mining sectors, for example. CI in the energy sector are particular vulnerable to climate change and environmental threat conditions (White House, 2015; Report Fireeye Threat Intelligence, 2015; Pursiainen, 2008; Rüle, 2012; Insight Forum, 2016; BC3 Basque Centre for Climate Change, 2010; Colbert, 2016; Cortekar and Groth, 2015; US. Energy Sector Report, 2013). Therefore, ECIC are also characterized by the *cascading effect* (McGee, 2015; Arvidsson, 2015; Kopylec *et al* 2007) a condition that increases dependencies among CI that could trigger cascading failures and multi-sectorial collapses (Van Eeten, 2011). Cascading effects belong to the category of events with low probability and high consequences. In addition, causal links to state and non-state actors are difficult to ascertain, often leading to erratic and ineffective responses to such events. One does not need to have a vivid imagination to envisage a host of ripple effects from an extended blackout, such as a petroleum spill, multiple vessels and installations in distress, and search and rescue operations impeded by a lack of weather and ice movement data.

ECIC raise the need for reconceptualization of cybersecurity to reflect environmental, social, and human security considerations (Shackelford, 2016). The overarching objective of this paper is to explore the legal aspect of this reconceptualization through assessing the need for a coherent and cohesive legal framework governing prevention and response to threats to CI. We argue in this paper that the concepts of environmental protection and sustainability provide a pathway to such a framework that accounts for interdependences, complexities, and uncertainties.

This is not to say that there are no legal frameworks, international and national, that might apply and address some implications in connection with ECIC. However, they treat ECIC the same way they treat other CI in the context of cyber-threats—in a highly fragmented manner (Radzziwill, 2007, Tsoagourias, et al, 2016, Hathaway, 2012, Schmitt, 2017). Thus, the applicable international law and policy instruments do not expressly address cyber-attacks to CI. This is due to the fact that the underlying legal regimes were formed before the emergence of cyber-security concerns let alone cyber-attacks on CI. This fragmentation further complicates multi-level cyber-security governance thereby necessitating integration of national, regional and international legal and policy instruments (Hathaway, 2012; Saalman, 2018). International treaties and regional agreements governing environmental protection and sustainable development, including those applicable to the Arctic, are also silent on cybersecurity and ECIC. Similarly, legal scholars are yet to connect cybersecurity to environmental governance in a meaningful manner. Meanwhile, such linkage might signal a paradigm shift from cybersecurity towards "sustainable cybersecurity" bringing about changes in the composition of actors, mechanisms, and technologies that are used to handle cybersecurity risks and design, implement, and enforce environmental policies.

We begin this paper with placing cybersecurity governance in the context of sustainable development, as well as the precautionary and polluter-pays principles, and suggest guiding principles for developing a legal framework for governing ECIC. We continue with exploring the concept of resilience as an entry point for cybersecurity actors, mechanisms, and technologies to link with

sustainability and environmental law principles. We conclude with a discussion of developing the aforementioned framework whilst emphasizing the importance of legal practices and standards.

2. Links between Sustainability, Environmental Law Principles, and ECIC

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" (UN Brundtland Report, 1987)).). Currently, sustainable development as a concept in international law is premised on three pillars: economic development, social development, and environmental protection (Birnie et al, 2009; Cassotta, 2011)). Practices and doctrines from international law on sustainable development are applicable to cyberspace (Shackelford, 2016). Important principles of environmental law linked to the concept of sustainable development in this context include the precautionary principle and the polluter-pays principle. The precautionary principle aims to provide guidance in the development and application of international environmental law as reflected in Principle 15 of the Rio Declaration of 1992 of the United Nations Conference on the Human Environment: "*where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation*" (Rio Declaration, 1992). This principle also reflects the eternal dilemma of how best to establish a "balance" between economic growth and protection of the environment. The polluter-pays principle requires the costs of pollution to be borne by persons responsible for causing pollution. Accepted as customary law in the European Union (EU), the Organization for Economic Cooperation and Development (OECD), and the United Nations Economic Commission for Europe (UNECE), the polluter-pays principle is closely related to the rules governing civil and state liability for environmental damage. Both the concept of sustainable development and the environmental law principles offer a starting point for development of the suggested framework.

Digitization has helped to accelerate economic development, contributed to social development, and enabled many technological tools used in environmental protection. However, digitization is only a *means* to creating efficient economies, prosperous human lives, and a cleaner environment. Therefore, digitization and the security of the hardware and software that powers it should be treated as *means* to an *end* – achieving economic and social development and ensuring environmental protection. The same rationale should apply not only to present cyber-threats but also to those of the future, meaning that at times economic efficiency should yield to system redundancy, and automation to manual controls. Both proved to be critical for minimizing the damage and restoring service in Ukraine in 2015 (Sullivan and Kamensky, 2017). This should not mean halting technological progress; rather, its constructive prowess must be balanced with the potential for devastation that the progress inevitably brings. Thus, our *first* guiding principle states, "When ECIC are present, digitization must be viewed as means to achieving economic and social development and increasing environmental protection whereas protection against cyber threats must ensure the ability of future generations to meet their own needs."

The precautionary principle is closely related to the principle of prevention and serves to safeguard against the risks of environmental damage and human security disruption, where human security here

is conceived in an untraditional perspective in a broader context at global level, not only confined to state security and to physical actions It draws upon the concept of sustainable development that elevates environmental concerns due to the importance of natural resource availability for future generations. The precautionary principle can guide digitizing the existing CI and/or siting and permitting new CI facilities. This means that under certain circumstances, manual controls and analogue technologies could be preferred over digitization or an energy facility in ECIC is not built at all. Accordingly, our *second* principle posits: "If the effects of cyber-attacks under ECIC are unknown, redundancy, analogue and/or manual controls, and 'zero option' alternatives must be used."

Unlike the precautionary principle, the main purpose of which is to safeguard against the risks of environmental damage and human security disruption, the polluter-pays principle can be used for allocating damage due to a cyber-attack. Such damage can include environmental as well as economic and social harm and to offset the costs of dealing with "cyber-pollution" – a persistent activity aimed at overwhelming CI that is yet to manifest in a full-scale cyber-attack. Thus, our *third* guiding principle states, "A state or non-state actor that launched a cyber-attack is responsible for all the economic, social, and environmental damages that occurred as a result of the attack, including the cost of lost opportunities to achieve economic and social development and increase environmental protection."

3. Linking Environmental Governance and Cybersecurity through Resilience

It would be naïve to expect government energy planners, corporate cybersecurity experts, emergency responders, military commanders, and many other professionals tasked to handle the destructive side of digitalization to accept sustainable development and environmental law principles as the basis for their day-to-day operations. Fragmentation of the applicable legal frameworks is both the cause and effect of tribalization that tends to lock people working on cybersecurity issues in their disciplinary and professional silos. Yet the proposed linking is not impossible. There is a plethora of instances in which actors whose interests typically do not align collaborate to solve a shared problem, often by pursuing the same goal. As we explore below, resilience can become common ground for cybersecurity and environmental governance.

Resilience enables people and ecosystems to cope with changes – shocks and stresses – and to adapt and even transform themselves as needed. However, some changes are so substantial or abrupt that they fundamentally alter the system, pushing it beyond an ecological tipping point. This phenomenon has been defined by scientists as "system shifts" or "paradigm shifts." (Arctic Resilience Report – ARR, 2016). The concept of resilience is not only pertinent to changes in natural and human environments, it also extends to socio-technical systems, societal formations, organizational structures, and political and transnational regimes.

A cyber-attack to CI in the energy sector under ECIC can be compared to extreme climatic events, because of the unpredictability, rapidity, and vulnerability of the area touched with the consequences of a profound black out, in an environment with less resilience. In such an environment, the time needed to recover would certainly be longer. The threats are also changing rapidly and it is impossible to predict what these changes will look like, even in a short period of time, making it very difficult to muster sufficient political will and align legal instruments and mechanisms to design, implement, and enforce mitigation strategies.

Risk-based approaches to resilience dominate in the EHN with a focus on reducing severity and uncertainty, as well as improving risk management. They are critical for protecting CI against cyber-threats, as they inform policy-makers about the vulnerabilities and risks to which CI is exposed, including the risk of the cascading effect, and identify and develop strategies to protect CI. These approaches have been effective, in terms of results and costs, at protecting system components from known threats (Van Eaten, 2011) However, unknown and hybrid threats pose a particular set of challenges that the existing risk-based approaches might not be able to handle. This is where the precautionary principle, detested by some in the risk analysis community, might prove to be the only available option (Sunstein, 2003). This is especially the case when in the quest for maximizing business efficiency, some actors do not take necessary precautionary measures to prevent attacks that may exploit vulnerabilities if the costs of cyber- attacks are not internalized (Van Eaten, 2011; Schackelford, 2014; Pursiainen, 2018)

Another set of challenges comes from the unwillingness of different key actors to cooperate on managing the cascading effect across international borders (Van Eaten, 2011). Solutions to these challenges are currently emerging through international inter-sectoral resilience cooperation. For example, the importance of resilience and increased civil-military readiness has been recognized by the North Atlantic Treaty Organization (NATO) goal at the Warsaw Summit in 2016 because NATO's ability to provide military support is highly dependent on functioning civil infrastructure (NATO Press Release, 2016). Therefore, a cyber-attack on civil CI, alone or as part of a terrorist attack not only can threaten a member nation's security, it can disrupt a NATO response. Solutions based in resilience focus on the necessary features allowing a complex, integrated system to recover function following a disruption. Specifically, resilience-based approaches are essential for threats aimed at affecting people and infrastructure in the Arctic, where the complex and high-value critical infrastructure components held by state and non-state actors are increasingly under threat of cyber disruption. A resilience approach would empower relevant stakeholders in the EHN to better understand: (i) where vulnerabilities and risks may arise within interconnected Arctic infrastructure systems; (ii) how cyber-attack or intrusion could pose cascading risks to the safety and operation of Arctic sites; and (iii) identify strategies to secure critical infrastructure against cyber-threats, particularly against vulnerable infrastructural targets. Hence, it is worth noticing that linking environmental governance and cybersecurity through resilience is of specific interest and in line with the NATO's current approach in this regard.

4. From the Guiding Principles to a Legal Framework

As noted above, at present, a coherent and cohesive legal framework that reflects ECIC does not exist. However, this does not mean that there is a complete legal vacuum – there are international and national legal frameworks, parts of which can and have been applied to certain aspects of the issues identified above. These frameworks include telecommunication law, aviation law, space law, and law of the sea (Hathaway, 2012).

Yet the lack of coordinated effort leaves many gaps and creates many ambiguities. In addition, because of the interdisciplinary, multi-layer, and multi-sectoral nature of cybersecurity in the ECIC context, and thus the presence of a multitude of state and non-state actors, a legal framework is only one part of an overarching governance regime (Stevens, 2018; Saalman, 2018). Currently, at international, regional, and national levels, governance regimes also lack coherency and cohesiveness. This is also due to the fact that these legal frameworks were formed prior to the

emergence of cyber-attacks and are therefore not expressly aimed at regulating a cyber-attack, but appear to regulate only a small fraction of it.

A potential legal framework for governing ECIC should be uniform, coherent, and cohesive. It should be centred on the concept of risk favouring proactive approach over reactive approach. It should be designed to be a critical part of the overarching governance framework accounting for both horizontal and hierarchal structures of power (Van Asselt, M. and Renn, O., 2011). Therefore, the legal framework should be based on a pluralistic and polycentric view of sources of law rather than a monistic view. In a monistic view, the sources of law are hierarchical and not interactive. In a polycentric view, sources of law and policy in provenance from the different areas of law, both from the public and private sector, overlap and coexist. Under the uncertain conditions of climate change and associated environmental threats, law and policy tools need to be applied in a complementary manner. These tools need to draw upon available technical standards and soft law. Although this legal framework should not be excessively rigid, it nonetheless should be premised on a set of guiding principles to give it a direction and a clear purpose. The guiding principles proposed above provide a starting point. Policy-makers need to know how to face challenges or legal fragmentation, and of imperfections of international law applicable under ECIC, and be informed about the urgent need to integrate cybersecurity and sustainability design in the future legal framework.

5. Sustainability and Cybersecurity through Legal Standards and Practices

The argument for the pluralistic and polycentric foundation of the ECIC legal framework is bolstered by the prevalence of non-state actors in the cybersecurity domain and the successes they have had handling cyber-threats. In the management of cyber-threats, often not only the public sector but also the private sector is involved in representing stakeholder interests. The private sector is often faced with managing cyber-threats as part of an effort to build trust with other actors via joint ventures, mixed agreements, hybrid business practices, and corporate social responsibility (CSR) initiatives (Shackelford, S., et al., 2016). Trust here means a level of collective confidence that a computer system will behave as expected. The management of cyber-threats to CIs can be based on instilling cybersecurity's best available practices (BAP) and best available technologies (BAT) while increasing digitization. Consensus is often necessary for standard harmonization, and industry best practices provide flexible and cost-effective approaches to enhance cybersecurity measures that assist owners and operators of CIs in assessing and managing the 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.

Cyber-attacks against CI serving the energy sector compounded by climate change threats can lead to devastating consequences and put the national security of a state in peril. Effective ECIC management should not only require identification of sources of security threats and public and private actor coordination, but also clearly defined severity thresholds that would trigger different responses. At the international level, there are legal uncertainties over what constitutes a cyber-attack on a sovereign state and the threshold for when a cyber-attack should be viewed as an equivalent to an armed attack (Schmitt, M., 2017a; Schmitt, M., b). Threshold-setting and classification are therefore important for defining responsibilities and assessing capabilities in relation to cyber-attacks of different levels. In addition, categorization of CI in terms of their criticality should be an ongoing process in light of technological progress and dynamic ECIC.

6. Conclusion

Energy CI is particularly vulnerable to the impacts of climate change. Due to remoteness, seasonal darkness, and severe climate, all of which are present in EHN, CI operates in "extra critical" or, as we term them, exceptionally critical infrastructure conditions. Unfortunately, the awesome challenges posed by ECIC are treated by the existing national and international legal frameworks in a fragmented manner, leaving CI, including energy CI located in EHN, vulnerable to cyber-threats. We, therefore, argue for rethinking approaches to governing cyber-threats to energy infrastructure under ECIC. We propose an approach in which cybersecurity is linked with environmental governance through the concept of sustainable development and the precautionary and polluter-pays principles of environmental law. We thus propose three guiding principles of ECIC governance. The *first* principle is: "When ECIC are present, digitization must be viewed as a means to achieving economic and social development and increasing environmental protection whereas protection against cyber threats must ensure the ability of future generations to meet their own needs." The *second* principle is: "If the effects of cyber-attacks under ECIC are unknown, redundancy, analogue and/or manual controls, and 'zero option' alternatives must be used." The *third* principle is: "A state or non-state actor that launched a cyber-attack is responsible for all the economic, social, and environmental damages that occurred as a result of the attack, including the cost of lost opportunities to achieve economic and social development and increase environmental protection." The idea of bringing environmental law into the cybersecurity realm might be foreign to many state and non-state actors currently involved in protecting CI from cyber-threats. However, shifting focus on resilience of the potentially impacted socio-technical systems and ecosystems will create a common ground for a joint effort. Therefore, a coherent and cohesive risk-based, pluralistic, and polycentric legal framework that is designed around the proposed guiding principles and is implemented through a holistic set of legal standards and practices should be a critical part of the proposed governance regime.

As noted above, the overarching objective of this paper is to start a conversation about reconceptualising ECIC governance. We do not suggest that our approach is the only pathway for increasing energy CI resilience. Nor do we suggest that the proposed guiding principles are the optimal way to connect cybersecurity and environmental governance. Our ideas and recommendations are based on our collective expertise as an international environmental legal scholar and a socio-legal energy scholar, as well as our review of relevant literature. Therefore, more transdisciplinary research is needed to move the needle in the scholarly and policy domains. However, we feel strongly about the *need* for reconceptualization and a shift to sustainable cybersecurity. As we note above, digitization is only a means of reaching an end. In contrast, sustainable development premised on environmental, social, and human security is an end in itself.

References:

Arctic Resilience Report – (ARR), 2016, Stockholm Environment Institute and the Stockholm Resilience Centre

Arvidsson, B., "*Development of a Method for Studying Cascading Effects between Critical Infrastructures*", Division of Risk Management and Societal Safety, Lund University, Sweden. Report 5004, Lund 2015.

BC3 Basque Centre for Climate Change – Klima Adketa Ikergai, "*Effects of Climate Change on the European Nuclear Power Sector*", September 2010.

Birnie, *et al*, "International Law & the Environment", 2009, Oxford University Press, pp. 115-127.

Cassotta, S, "*The Environmental Liability Directive in a More Sustainable Future: A Quest to Rejuvenate its approach after Lisbon*?" 2011, 1, *Section III – The Concept of Sustainable Development*", Revue Européenne du Droit de Law Consommation.

Colbert, E., Kott, A., "*Cyber Security of SCADA and Other Industrial Control Systems*" – Advances on Information Security 66, 2016, Springer.

Cortekar, J., and Groth M.*, "Adapting Energy Infrastructure to Climate Change – Is there a Need for Government interventions and Legal Obligations within the German "Energiewende*"?, Energy Procedia, 73, 12:17, June 2015.

European Union, EECSP Report of 2017 "*Cyber Security in the Energy Sector",* 2017.

Intergovernmental Panel on Climate Change (IPCC), Forth Assessment Report: Climate Change 2007, Working Group II: Impacts, Adaptation and Vulnerability.Insight Report Forum – Committed to Improving the State of the World, "The Global Risks Report of 2016", 11th Edition.

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

Kopylec J., D'Amico A., Goodall J. (2008) "*Visualizing Cascading Failures in Critical Cyber Infrastructures*". In: Goetz E., Shenoi S. (eds) Critical Infrastructure Protection. ICCIP 2007. IFIP International Federation for Information Processing, vol 253. Springer, Boston, MA.

Østgaard Skotnes, "*Challenges for safety and security management of network companies due to increased use of ICT in the electric power supply sector*," Doctoral Thesis, The Faculty of Social Science at the University of Stavanger, 2015.
Radzziwill, Y, "*Cyber-Attacks and the Exploitable Imperfections of International Law*", 2015, Brill Nijholff, Gorge, M., "*Cyberterrorism: Hype or reality?* 2007, Computer Fraud & Security.

Report, UN Document, 1983, The Bruntland Report "*Our Common Future*", 1983, Report World Commission and Development (WCED), chaired by Gro Harlem Bruntland, UN Document

Sibel, McGee, *et al,* "*Risk Relationship and Cascading Effects in Critical Infrastructures: Implications for the Hyogo Framework, The United Nations Office for Disaster Risk Reduction*", (UNISDR), Global Assessment Report on Disaster Risk Reduction, 2015, Input Paper, 17, January 2014.

NOAA, 2014. Arctic Report Card: Update for 2014. [Online] Available at: ftp://ftp.oar.noaa.gov/arctic/documents/ArcticReportCard_full_report2014.pdf [Accessed 1 May 2018].

NATO Press Release, 2016, 100, NATO, Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, Press Release 2016 (100).

Pursiainen C., "*Critical Infrastructure Resilience: A Nordic Model in the Making*? 2018, International Journal of Disaster Risk Reduction, 27, Elsevier, pp. 632-641.

Pursiainen C., *et al* "Towards a Baltic Sea Region Strategy in Critical Infrastructure Protection, 2008, Nordregio Report 2007:5

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

Report, Fireeye Threat Intelligence, "*Cyber Threats to the Nordic Region*", May 2015.

Rüle, M., "*NATO and Energy Security Challenges Division, NATO, Brussels"*, Belgium, Journal of Translatlantic Studies, Vol. 10. No. 4, December 2012, 388-395.

Saalman, l., "*Integrating Cybersecurity and Critical Infrastructure*", Stockholm International Peace Research Institute (SIPRI), March 2018.

Shackelford, S., 2016, "*On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Actions Problems*", Vanderbilt Journal of Entertainment & Technology Law", Vol. 18, N. 4

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

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

Schmitt, M., Vihul, L., "*Tallinn Manual on the International Law Applicable to Cyber Operations*" second edition, Cambridge University Press, 2017. (Schmitt "b").

Stevens, T., "*Global Cybersecurity: New Directions in Theory and Methods*", 2018, Volume 6, Issue 2, pp. 2-4.

Stoker, G. (1998). *Governance as Theory: Five Propositions.* International Social Science Journal, 50(155), pages 1–157.

Sullivan, J.E., Kamensky, D., "*How cyber-attacks in Ukraine show the vulnerability of the U.S. powergrid*" 2017, The Electricity Journal, Vol. 30 pages 30-35.

Sunstein, C. (2003). *Beyond the Precautionary Principle. University of Pennsylvania Law Review*, 151(3), pages 1003-1058.

Tsagourias N., Buchan, R., "*Cyber-Threats and International Law*", Chapter 14, in "*Security and International Law*" Edited by Footer, E. M, Schimt, J., White D. N., Bright, D. L, 2016, Oxford and Portland, Oregon.

US. Energy Sector Vulnerabilities to Climate Change and Extreme Weather – July 2013, US Department of Energy.

Van Asselt, M., & Renn, O. (2011, April). Risk Governance. Journal of Risk Research, 14(4), pages 431-449.

Van Eeten M., *et al* "*The State and the Threat of Cascading Infrastructures across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports*", Public Administration Vol. 89, No 2, 2011

World Energy Report, The Road to Resilience, 2016 at https://www.worldenergy.org/news-and-media/press-releases/new-cyber-report-energy-sector-prime-target-for-cyber-attacks/