Climate Change, Environmental threats and Cybersecurity in the European High North

Cassotta, Sandra; Sidortsov, Roman; Pursiainen, Christer; Pettersson, Maria; Goodsite, Michael Evan

Published in:
Enablement Besides Constraints

Publication date:
2019

Document Version
Accepted author manuscript, peer reviewed version

Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North. Synthesis Report.

Zojer, Gerald

Published: 01.01.2019

Document Version
Publisher's PDF, also known as Version of record

Citation for pulished version (APA):
Zojer, G. (2019). *Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North. Synthesis Report.* University of Lapland, Arctic Centre, the Northern Institute for Environmental and Minority Law. JURIDICA LAPPONICA, No. 47

JURIDICA LAPPONICA 47

Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North

Synthesis Report

Gerald Zojer (editor)

Juridica Lapponica 47

Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North.

Synthesis Report.

Gerald Zojer (editor)
Northern Institute for Environmental and Minority Law,
Arctic Centre, University of Lapland

ARCTIC CENTRE
University of Lapland

Rovaniemi 2019

Cover layout:
Gerald Zojer / KaamosCreations

ECoHuCy logo:
Zuza Banaś

Print by: University of Lapland Printing Centre, Rovaniemi 2019

Juridica Lapponica 47
ISSN 0783-4144, nro 47

ISBN 978-952-337-182-8 (printed work)
ISBN 978-952-337-183-5 (PDF)
http://urn.fi/URN:ISBN:978-952-337-183-5

Executive Summary

This synthesis report sums up the findings of the three year long research project: ***E****nablement besides* ***Co****nstraints:* ***Hu****man Security and a* ***Cy****ber Multi-Disciplinary Framework in the European High North* (ECoHuCy). The aim of the project was to design a multidisciplinary research framework to address human security questions related to digitalisation and the increasing importance of cybersecurity. It re-conceptualises cybersecurity by shifting the focus from technical infrastructure to safeguarding human wellbeing. Digitalisation affects the population of regions differently, depending on the regional peculiarities. This project focused on the northernmost areas of Finland, Norway and Sweden – the European High North.

Key Findings

A human security perspective on cybersecurity

- Current cybersecurity frameworks are state-centric and focus on securing information and information infrastructure. They aim to safeguard the benefits of digitalisation at the national level.

- Current cybersecurity frameworks fail to acknowledge that digitalisation may create new insecurities for people in their everyday life and lack to address the impacts of digitalisation in region-specific contexts.
- Utilising human security approaches can supplement current cybersecurity understanding and make it more inclusive to people's interests and concerns.
- A human-centred cybersecurity approach can be used to address the issues and challenges people experience from digitalisation in everyday life and in region-specific contexts. It can therefore be used as a policy-making tool to advance human wellbeing.

Citizen and civil society perspectives on cyberspace

- Cyberspace has not profoundly changed society in terms of the relative power that one type of civil society has over another type of civil society. Our framework for analysis further illustrates this finding. Basic norms, culture, interests, and goals of civil society organizations have not significantly been changed.
- Digitalisation has had a transformative, generally positive impact in the way communication happens, internally and externally, between local communities, authorities and civil society organizations in northern Norway. It has particularly helped to overcome past constraints linked to geographical distance or remoteness.
- Transnational contacts and cooperation between civil society organizations in the EHN were fostered, made

possible and enhanced by the emergence of cyberspace and digitalization.

- At the citizen and civil society level, our findings identified that citizens experience everyday cyber insecurity and wish for more effective ways to reduce or prevent the dangers inherent to it. Concerns particularly associated to personal information security, democracy and critical infrastructure emerged as important matters deserving attention.
- Community-wise, our findings call attention to the need for creating strategies to reduce and prevent the negative effects of digitalisation in local communities. Our case study in Lofoten illustrates that these negative effects can significantly alter the nature, environment and local economy. Thus, diverse communal strategies that take into account the voice of different stakeholders are suggested to minimize the negative impact and enhance the positive changes brought by digitalisation.

ICT access and use among elderly people

- Many people think digitalisation especially benefits peripheral areas such as the EHN. The internet has been described as an equaliser, and participants provided a number of examples of how digital technologies enable them to live, study and work in the EHN.
- Participants distinguished between different types of ICT use. For example, they pointed out that many elderly can competently use social media platforms like Facebook

while lacking the skills and knowledge to use services such as online banking.

- Younger family members are an important resource to many elderly people when using digital technologies. Sometimes, this involves a younger family member buying and setting up equipment. Other times, this goes as far as the older family member 'relinquishing' control over their own finances so that a family member can access online banking on their behalf.
- Full accessibility for people with disabilities, especially visual impairments, is still a challenge. Providing services in Sámi languages has also been under-prioritised.

Climate change, environmental threats and cybersecurity

- There is an important linkage between environmental governance and cybersecurity of CIs in the energy sector in the EHN, which has prompted legal scholars and policymakers to rethink their agenda based on reconceptualisation as well as a shift to sustainable cybersecurity incorporating the notion of human security.
- Cyberattacks to CIs in the EHN are sometimes subject to environmental threats due to climatic conditions as a consequence of climate change, which warrants labelling them exceptionally critical infrastructure conditions (ECICs), which require both an ad hoc and stronger regulatory frameworks.
- Because ECICs are present in the EHN, digitalisation must be viewed as a mean to achieving economic and social

development and increasing environmental protection. Likewise, protection against cyberthreats must ensure the ability of future generations to meet their own needs.

- In the EHN, there is a need for future agreements applicable to CIs and cybersecurity that link environmental governance and resilience to cybersecurity and incorporate the notion of human security. This can be designed by combining different sources of law and policy from international, regional and domestic levels.
- Many aspects of the cybersecurity regime are highly fragmented, resulting in gaps in international law and policy, which is why drawing a parallel between the environmental (liability) regime and the nascent cybersecurity regime in a global-local approach is important in order to identify ways to improve the cybersecurity regime in the EHN.

The results of this research project suggest that by utilising a human security approach the cybersecurity framework becomes more comprehensive. Instead of focusing on technical infrastructure, a comprehensive cybersecurity approach focuses on safeguarding human wellbeing. Such a human-centred cybersecurity approach can be applied as a tool in order to create meaningful and targeted policies that address both the positive and negative impacts of digitalisation, while at the same time allowing the flexibility to consider regional peculiarities.

Preface

The completion of this book is an outcome of the research that was conducted as part of the three-year-long international research project: ***E****nablement besides* ***Co****nstraints:* ***Hu****man Security and a* ***Cy****ber Multi-Disciplinary Framework in the European High North* (ECoHuCy). The project is a part of the "society, integrity and cyber-security" theme of the Nordic Societal Security Programme run by NordForsk – an organisation under the Nordic Council of Ministers that promotes Nordic cooperation on research and its infrastructure. The project was hosted at the Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland (Rovaniemi, Finland). Project partners were the University of Tromsø – the Arctic University of Norway, Swansea University (United Kingdom) and the Institute for Security and Development Policy (Sweden). The project was carried out from January 2017 to December 2019. This book represents a synthesis report of the research conducted during the project. As some of the empirical research work is still being analysed, and some outcomes have not yet been published, parts of the book contain preliminary findings or refer to articles or books that will be published soon.

Gerald Zojer
December 2019

Table of Contents

1 Introduction

Gerald Zojer

Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland

In the 21st century, the concept of cybersecurity has risen on the agendas of state administrations, (trans/inter)national organisations and corporations. This is due to rapidly advancing digitalisation, which is the process of the digital transformation of our societies. Business, public administration and societal functions are increasingly handled through digital technologies and information and communication technologies (ICTs), which are interconnected in cyberspace. At the same time, the process of digitalisation has advanced to an extent that a functioning society has become dependent on undisrupted cyberspace and ICTs. However, digital technologies are vulnerable, and technical failures, connectivity problems, human abuse or error can cause interruption of services. In order to address such challenges, information security and cybersecurity frameworks have been developed. When the infrastructure of an entire society is threatened, the question of security shifts from the individual or organisational level to the state level. Consequently, most countries have developed cybersecurity strategies to safeguard their cyber infrastructure. The concept of cybersecurity has remarkable visibility in contemporary security literature. Much of it addresses negative security: threats to be mitigated by applying specific measures, such as to protect critical infrastructure from cybercrime,

cyberwarfare, hacktivism or espionage. At the individual level, cybersecurity deals with data protection or privacy. However, the everyday life experiences of individuals or communities interacting with digitalisation also leads to new insecurities and challenges, such as the creation of social exclusion, disappearance of physical services or impacts on local culture. Mainstream approaches to cybersecurity fail to address these security challenges at the individual or community level. Moreover, they tend to treat society at the national level somewhat homogeneously, ignoring the differences and peculiarities between regions within states.

The impacts of digitalisation can also be observed in the northernmost parts of Finland (Lapland), Norway (Troms and Finnmark) and Sweden (Norbotten) – or the European High North (EHN). In the European Commission's 2019 Digital Economic and Society Index, Finland, Norway and Sweden ranked in the top five performing countries. However, the way digitalisation impacts societal development differs depending on the region. The socio-economic and environmental peculiarities of the EHN makes the region distinct from the more southern parts of these countries. The EHN is a peripheral region with a low population density, less developed infrastructure and harsh climate with long and dark winters, and in the rural areas especially, it is shaped by traditional economic activities, such as reindeer herding or fishing. Moreover, the EHN is also the homeland of the Sámi, an Indigenous people consisting of several small language groups. These particularities create a set of features that make the impact of digitalisation in the region distinct.

This book represents a synthesis of the work conducted within the three-year research project ***E****nablement besides* ***Co****nstraints:* ***Hu****man Security and*

*a **Cy**ber Multi-Disciplinary Framework in the European High North* (ECoHuCy). The aim was to design a multidisciplinary, comparative research framework to address human security questions related to the dis-/integrating effects of digitalisation and the increasing importance of cybersecurity. It constructs a research agenda suited for the purposes of policy makers, regulators and academia alike, as well as giving the citizens and communities of the EHN a voice in matters related to cybersecurity. It questions the mainstream conceptualisation of cybersecurity and instead reconstructs it with the human as the referent object of security. By utilising the human security concept, the project establishes a human-centred cybersecurity framework. This theoretical work has been accompanied and supported by several empirical case studies.

In order to develop this novel framework, the project work was divided into four substantial work packages. This book summarises these work packages, with each chapter representing the results of one project work package. It is worth noting that due to the interdisciplinary approach to the overarching theme, many deliverables of the project fit into more than one work package.

Chapter 2, 'Theorizing Security: Human Security Perspective on Cyber Security', summarises the theoretical framework that was developed during the project. It concentrates on the theoretical development of a human security perspective on cybersecurity. It begins with an analysis of the national cybersecurity discourse as established in the countries of the EHN. Then, it discusses the commonalities and shortcomings of these strategies, before elaborating the human security discourse and how it is related to digitalisation in the EHN. The chapter closes with a deconstruction of the

mainstream cybersecurity discourse and presents a human-centred cybersecurity perspective based on the human security concept.

Chapter 3, ‘Citizen and Civil Society Perspectives on Cyberspace in the European High North’, draws attention to the effects cyberspace and ICTs have on citizens in the EHN, with a particular focus on Northern Norway. It brings forth empirical evidence of the benefits and constraints arising from digitalisation for non-profit civil society organisations. It suggests that digitalisation has significant impacts on civil society, but that it neither enhances nor constrains civil society.

Chapter 4, ‘ICT Access and Use Among Elderly People in the European High North’, presents empirical findings on how digitalisation and access to ICTs affects elderly people in the EHN. It shows the dichotomy of how digitalisation can increase access to services for some but create new accessibility challenges for other community members, for example, due to a lack of digital skills, physical impairments or absence of services in local languages. The chapter furthermore discusses how younger family members have become an important resource for elderly members when using digital services.

Chapter 5, ‘Climate Change, Environmental Threats and Cybersecurity in the European High North’, establishes the interconnection between global environmental governance and cybersecurity as well as between the environmental liability regime and the cybersecurity regime. It elaborates how the climatic conditions in the EHN create extra criticality to infrastructure. The chapter examines the interactions, pros and cons of

different categories of regulatory instrument mixes and how they are connected to collateral governance issues and human security.

2 Theorising security: A human security perspective on cybersecurity

Gerald Zojer

Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland

Executive Summary

Rapidly advancing digitalisation is promoted in the northernmost areas of Finland, Norway and Sweden – the European High North (EHN). This peripheral region is characterised by a sparse population density, less developed infrastructure and harsh climate. It is also the homeland of the Sámi, an Indigenous people with several small language groups. Acknowledging the importance of information and communications technologies for the functioning of contemporary societies, the EHN states have endorsed information and/or cybersecurity strategies. These strategies aim to safeguard information and information infrastructure to encourage business development and allow society to benefit from digitalisation. Yet, these strategies fail to fully recognise the challenges and threats that people experience in everyday life from increasingly digitalised services or to acknowledge regional peculiarities within the states. Utilising a human-centred security approach to digitalisation can supplement the current cybersecurity frameworks. Such a comprehensive framework can be built on the human security approach. While acknowledging the concerns already addressed by cybersecurity, such a broadened approach extends the existing framework by including challenges at the individual and sub-state community levels. A human-centred cybersecurity approach can therefore contribute to the development of meaningful and targeted policies that move human wellbeing into the focus of cybersecurity.

2.1 Introduction

Digitalisation is advancing quickly, especially in the countries of the European High North (EHN). This is not at last due to the states' policies regarding digitalisation. In the European Commission's 2019 Digital Economic and Society Index (DESI), Finland, Norway and Sweden were among the top five performing countries. For instance, the country reports for the EHN stated that 99% of Finnish, 94% of Norwegian and 96% of Swedish households have access to the 4G network (European Commission, 2019), which is currently the fastest implementation of mobile cellular network technology available for end users.[1] Finland, moreover, was the first country to make access to broadband a basic right (Ministry of Transport and Communications, 2010). Also, the digitalisation of public services, such as education, health and public administration, is progressing quickly in the EHN. From a governmental viewpoint, the move to increasingly digitise services is often justified by gains in (cost) efficiency, especially in areas with diminishing populations, such as the EHN. However, growing digitalisation also creates new dependencies and reinforces social exclusion (see also Gulbrandsen & Sheehan, forthcoming). States have responded to the increasing importance of digital infrastructure for societal functioning by endorsing cybersecurity strategies, which aim to protect critical infrastructure. Yet, these strategies fall short of addressing new challenges that people experience in their everyday lives due to digitalisation (Hossain, Salminen, & Zojer, forthcoming; Salminen, 2019; Salminen & Hossain, 2018; Zojer, 2019b). This chapter discusses a widened

1 The fifth generation (5G) is still in its early roll-out phase and not yet available for wide public use.

security approach to the challenges created by digitalisation in the EHN. In order to do so, it utilises human security approaches to promote a bottom-up security approach. Such a comprehensive cybersecurity understanding is better suited to capture the challenges originating from digitalisation in everyday life situations for individuals and communities at the sub-state level and can be applied as a tool to identify and asses challenges in a region-specific context.

2.2 Digitalisation and cybersecurity

In policy documents and development strategies of all the EHN countries and regions, the advancement of digitalisation plays an important role in promoting the efficiency of public services as well as (new) business opportunities. With increasing digitalisation, the functioning of society becomes more and more reliant on undisrupted information and communication technologies (ICTs). At the same time, physically available services, such as public administration or health services, are not only being replaced by digital services but are decaying or being dismantled. Further, ICTs and digital technologies are vulnerable, for example, due to connectivity problems, technical failures, human abuse of vulnerabilities and human error. Such challenges have been addressed by information security and cybersecurity frameworks.[2] When entire societies' ICT infrastructures are challenged, the question of security shifts from the individual or organisational level to the state level. Thus, most states have endorsed cybersecurity strategies in order to bring attention to questions of

2 At the organisational level, the terms information security and cybersecurity are often used synonymously.

information security at the state level. The difference, therefore, is that the state carries out the responsibility for the production of security (Salminen, 2019; Salminen, Zojer, & Hossain, forthcoming; Zojer, 2019b).

2.2.1 Current cybersecurity approach in the European High North

Generally, cybersecurity refers to securing the digital ecosystem that constantly interacts with operations in the physical environment (Limnéll, Majewski, & Salminen, 2015). When cybersecurity is conceptualised at the national level, it usually focuses on threats to infrastructure critical for the functioning of the states' society. It references threats originating from cybercrime, cyberwarfare, hacktivism or espionage and is concerned about the defence of cyberspace from cyberattacks (Kostopoulos, 2013; Kramer, Starr, & Wentz, 2009; Zojer, 2019a, p. 175). Yet, in the absence of an univocal or unanimous definition of cybersecurity, this chapter utilises the national approaches of the EHN states.

Finland's 2019 cybersecurity strategy is scarce in its definitions, but the preceding strategy from 2013 stated that cybersecurity 'means the desired end state in which the cyber domain is reliable and in which its functioning is ensured' (Secretariat of the Security Committee, 2013, p. 1). The 2019 strategy aims at safeguarding vital societal functions that depend on the cyber domain as well as supporting the availability of reliable digital services and business development. The guidelines of the strategy are based on three pillars: a) to develop international cooperation in order to protect the cyber environment without borders; b) better coordination of cybersecurity management, entailing planning and preparedness; and c) the

development of cyber competence by increasing everyday skills and top skills as a means of safeguarding cybersecurity (Secretariat of the Security Committee, 2019). The Swedish cybersecurity strategy aims at managing risks inherent to digitalisation that impact prosperity and security. Cybersecurity ‘concerns the whole society’ and everyone ‘needs to take responsibility for cyber security issues’ (Ministry of Justice, 2017, p. 3). The objectives are to protect the lives and health of the population, the functioning of society and the capacity to uphold fundamental values, including democracy, the rule of law, human rights and freedoms as well as national growth and competitiveness, by ‘a set of security measures to preserve the confidentiality, integrity and availability of information’ (Ministry of Justice, 2017, p. 4). The Norwegian strategy defines cybersecurity as the protection ‘of data and systems connected to the Internet’ (Ministry of Government Administration, Reform and Church Affairs, 2013, p. 28). The goal of the strategy is to create robust and secure ICT infrastructure, tackle adverse ICT events and increase the level of competence and security awareness.

2.2.2 Commonalities and shortcomings

The three cybersecurity strategies are similar in that there is only a limited role allocated to individuals and their everyday experiences with digital technologies. The wellbeing of the people is considered to be dependent on ICTs, but people can also cause problems through negligence or malevolence. In all these strategies, it is the cyber domain – information, data and systems – that is constructed as the referent object of cybersecurity rather than the people. Instead, human individuals are treated as threats,

weak links, victims, or as factors who pose a potential risk to information security (Salminen, 2018; 2019; Salminen & Hossain, 2018; Salminen et al., forthcoming; Zojer, 2019a; 2019b). This approach to cybersecurity can therefore be compared with a traditional security approach, wherein the state's interests are the referent object of security. However, such a state-centric approach runs the risk of failing to address the challenges and threats originating from digitalisation in everyday life and in a sub-national or regional context. The complex interrelation between digitalisation and societal development requires a more comprehensive approach to these multifaceted challenges in order to facilitate human development and prosperity (Collins, forthcoming; Salminen, 2018; Salminen & Hossain, 2018; Salminen et al., forthcoming; Zojer, 2019b). A human-centred security approach enables individuals and communities to vocalise their fears and challenges and empowers them to address issues that originate from state actions and that might be detrimental to societal integrity at the sub-state level (Hoogensen Gjørv, 2012; Hossain, Zojer, Greaves, Roncero, & Sheehan, 2017). Finally, states' measures to provide cybersecurity may in fact pose new challenges and risks to information security at the individual level (Dunn Cavelty, 2014). Therefore, this chapter argues that a human-centred approach to cybersecurity can help to reveal the challenges digitalisation brings to people's everyday lives while also considering region-specific peculiarities.

2.3 The human security discourse

Within the academic field of international relations, traditional approaches to security studies have dealt with threats to sovereign states (for example,

Mearsheimer, 2014; Waltz, 2010). Towards the end of the 20th century, and especially during the end of the Cold War in the 1980s, the scope of security studies broadened to also include sectors such as the environment or societies at the sub-state level (for example, Buzan, Wæver, & de Wilde, 1998; Heininen, 2013; Hoogensen Gjørv, Bazely, Goloviznina, & Tanentzap, 2014; McSweeney, 1999). These new approaches to security changed the scope and nature of security threats, which were recognised as being socially constructed. Such critical security theories led to questioning of the ontological and epistemological basis of security studies as a field. This led to the development of more complex and comprehensive concepts of security, with human security gaining prominence and popularity within the global political discourse, resulting in numerous state and multilateral policies (Gulbrandsen & Sheehan, forthcoming), such as the Millennium Development Goals or the Sustainable Development Goals. Instead of state sovereignty, these widened security approaches focused on the wellbeing of individuals and communities at the sub-state level and thus centred around threats to human wellbeing. The human security concept became popularised through the publication of the United Nations Development Programme's (1994) Human Development Report (HDR). Together with the emergence of critical approaches to security, these developments enabled and accelerated the move towards multiple sectors of security and the adoption of human individuals and sub-state communities as referent objects of security (Gulbrandsen & Sheehan, forthcoming), which has been claimed to be a new paradigm of security (Commission on Human Security, 2003).

2.3.1 Defining human security

There is no universally accepted definition of human security. Some scholars have discussed human security in a rather narrow sense, delimiting its meaning to the protection of communities or individuals from physical violence (for example, Human Security Centre, 2005). Using such a narrow understanding, the concept might even be applied to legitimise military interventions as a political tool, such as through the responsibility to protect (R2P) commitment, which allows the international community to intervene in states that fail to protect their own people from genocide, war crimes, ethnic cleansing or crimes against humanity (Zojer, 2019b, p. 300). Yet, the most common understanding of human security expands the concept 'beyond physical violence as the only relevant threat/vector; and beyond physical harm as the only relevant damage' (Gasper, 2014, p. 32). The Commission on Human Security (2003, p. 4), defined human security as 'the protection of the vital core of all human lives in ways that enhance human freedoms and human fulfilment', including 'processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity'. This people-centred approach to security focuses on what people need in order to live in freedom from fear and freedom from want. Human security thus 'sits on interstices of human rights, human development and security discourses' (Martin & Owen, 2014, p. 1) and conceptualises culture, identity and human progress as needing to be protected.

Using such a broad understanding, the human security approach acknowledges that security threats not only originate from physical violence

(freedom from fear) but that societal security also depends on the absence of threats to ideational or material freedoms (freedom from want). To apply such a broad and human-centred security approach, many have built their definition on the concept established in the 1994 HDR, which identified seven key areas of human security: economic, food, health, environmental, personal, community and political security. All of these aspects are considered individually important, yet they are also interconnected and sometimes even conflicting. For instance, a sound environment is important for providing healthy and nutritious food, but environmental integrity may at the same time be challenged by economic development. Because of the complex interrelation of the different sectors and in the absence of a unanimous or univocal definition, the concept has also been exposed to criticism. Paris (2001, p. 91), for instance, argued that if 'human security means almost anything, then it effectively means nothing'. Krause (2004, p. 367) warned that in order to be a useful concept, human security must avoid becoming 'a loose synonym for "bad things that can happen"'. However, when human security is not reduced to a predetermined list of issues or to a narrow definition, it is 'flexible enough to allow for a deeper understanding of the root of insecurities and capacities to address them' (Tadjbakhsh, 2014, p. 54). The Nobel prize laureate Amartya Sen (2014, p. 22) pointed out that 'the very lack of a general theory allows an openness that is important for this kind of work'. Consequently, a broad and flexible application of the human security approach creates a framework that allows for the assessment of security threats at the individual and sub-state levels in a region- and issue-specific context (Hossain et al., 2017; Zojer, 2019b).

2.3.2 The interconnectedness of digitalisation and human security in the European High North

Due to the rapid process of digitalisation and the wide diffusion of personal computers and other electronic devices (such as smartphones, the Internet of Things, etc.), ICTs have become one of the most significant areas of technological progress and are interdependent with societal development. ICTs can thus play an important role in safeguarding human security 'since they are among the major sources of strengths in improving the quality of living across the world' (Sen, 2014, p. 24). For instance, acknowledging the importance of the internet, the international community has identified the intentional disruption or prevention of dissemination of or access to information from the internet as a violation of human rights (General Assembly resolution 32/13). However, the interconnectedness of digitalisation and societal development is related to regional particularities, which bring with them a new set of challenges. The EHN can be characterised as peripheral within the EHN states; having a sparse population density with long distances to reach certain services (health, education, public administration, etc.); having a harsh climate with long, cold and dark winters; being shaped by an economy wherein traditional activities and subsistence, such as reindeer herding or fishing, still play an important role for many individuals and communities; and having a less developed infrastructure, such as health care or ICTs, than in the southern parts of the EHN countries. Furthermore, the EHN is also the homeland for the Sámi, an Indigenous people with several small language groups. Thus, digitalisation creates new opportunities as well as challenges that are specific to the region. Zojer (2019b) pointed out that all seven key areas of

human security are affected by digitalisation in a region-specific context. For example, utilising telemedicine allows medical professionals to offer services in remote areas, improving health and decreasing the need to travel long distances, therefore mitigating environmental impacts related to traffic. However, as Gulbrandsen and Sheehan point out in this volume (chapter 4), the increasing digitalisation of health services can also be interpreted as thinning out the welfare state and decreasing access to physical contact with health professionals. As highlighted by regional and national digitalisation and development strategies, the increased use of ICTs may bring new economic opportunities by enabling local businesses to access global markets; however, online shopping also challenges existing retailers. Digital devices, such as global positioning system trackers, may increase the efficiency of traditional activities such as reindeer herding and can furthermore be used for planning land use with different stakeholders (Zojer, 2019b, pp. 311–314), but they also have the potential to disrupt traditional knowledge, which is crucial for the sustenance of cultural integrity, especially for the Indigenous population. Digital technologies can be used to store traditional knowledge and make it accessible; however, due to the interoperability of modern technologies with the nature of traditional knowledge, this is not an easy task (Pettersen, 2011). The internet and social media can be used to keep in touch with members of (language) minority groups, thereby contributing to maintaining culture and language, but it can also lead to digital exclusion, challenge local culture through the influence of global culture or be used for harassment or hate speech, which can create additional burdens for members of marginalised or already vulnerable groups. ICTs can also be used to increase participation possibilities in

political processes or environmental impact assessments, whereas the same technologies can be abused for state oppression (Dymet, 2019; Hossain, 2019; Zojer, 2019b, pp. 315–317; Zojer & Hossain, 2017, p. 45).

2.4 Deconstructing the mainstream conceptualisations and re-constructing cybersecurity as human centred

The countries and regions of the EHN promote digitalisation because it provides opportunities. Not only does it create a technological foundation for new ways of doing things, it can also help to reduce costs and increase efficiency. At the same time, it generates friction and dissatisfaction because it creates new types of vulnerabilities, problems or exclusion. While cybersecurity is aimed at safeguarding the opportunities that come with digitalisation, it does not perform well in capturing or responding to the challenges that people face in everyday life (Salminen et al., forthcoming). Moreover, the current national cybersecurity frameworks focus on threats at the national level but fall short of capturing the specific challenges digitalisation generates in a local context, such as in the EHN. However, in the end, the aim of cybersecurity frameworks is to safeguard societal integrity and to promote human development. To do so, a meaningful cybersecurity framework needs to be comprehensive. First, it needs to understand that human wellbeing cannot be delimited to financial wealth but that it also includes non-material values such as spirituality or cultural integrity. The very purpose of the HDRs has been to challenge the common narratives of national and international development politics to shift

attention from a pecuniary focus and to highlight a multidimensional understanding of human development that focuses on people's wellbeing (Haq, 1995). Second, the techno-determinist narrative of cybersecurity needs to be overcome. Technology is not a neutral object but rather it embeds culture and politics and is thus socially constructed (Bijker, Hughes, & Pinch, 2012; Latour, 2004; MacKenzie & Wajcman, 1999; Winner, 1980). Third, the impacts of technological progress, such as digitalisation, differ depending on the cultural, socio-economic and environmental peculiarities of a region. Since national strategies and policies are usually made in the states' capitals (far south of the EHN regions), there is danger that policy makers are not fully aware of the particularities of the northernmost parts of their countries.

The concept of human security as a security approach has the breadth and flexibility that is necessary to analyse the complex and multifaceted interrelations between digitalisation and societal dynamics at the sub-state level, thus allowing for the focus of security concerns to be shifted to human wellbeing. The human security approach can be applied to particular issues that are of interest in order to raise awareness of and motivate response to these issues (Gómez & Gasper, n.d.). It can be used to identify existential threats to individuals and communities and therefore it can be used as a policy-making tool (Floyd, 2007). It empowers people by listening to their fears and challenges and also can unveil threats that people perceive as originating from states' actions. It makes people into securitising actors, hence contributing to building their capacity (Hoogensen Gjørv, 2012). Consequently, the human security approach offers a tool set that can supplement the current cybersecurity framework to become more sensitive

to the impacts of digitalisation in people's everyday lives in a region-specific context. It therefore could serve to create new understandings and insights into specific vulnerabilities. The current cybersecurity frameworks do address issues that are important for the inhabitants of the EHN, as a fully operational cyber infrastructure is necessary to maintain the functioning of digitalised societies. However, the human security approach also includes difficult and traditional security concerns. Thus, applying a human security approach could close the gap between traditional cybersecurity issues and a human-centred agenda, allowing countries to respond to the many opportunities and challenges related to digitalisation. Similar to the widening of the traditional security approach in international relations, a multidimensional and comprehensive cybersecurity approach is better suited to address the challenges digitalisation creates. Applying such a human-centred cybersecurity framework can therefore contribute to the development of meaningful and targeted cyber policies and advance human wellbeing in a society that is being rapidly transformed through digitalisation.

2.5 Conclusions

Digitalisation in the EHN is progressing rapidly and affects people's everyday lives in many regards. States' and regional policies towards digitalisation highlight the benefits and opportunities it brings forth and focus on securing cyber infrastructure in order to safeguard its positive effects. At the national level, the EHN countries have endorsed cybersecurity strategies for this purpose. However, these strategies mainly

refer to safeguarding infrastructure rather than human wellbeing and fail to address challenges in a region-specific context.

This chapter suggests that utilising the human security framework can bring additional value to identifying the needs, fears and challenges created by digitalisation. Its breadth and flexibility are responsive to a region-specific context and allow individuals and communities to raise their voices and express the challenges they perceive. It uses a people-centred perspective by making the human individual the referent object of security. Utilising a human-centred cybersecurity approach can therefore contribute to developing meaningful and targeted policies addressing the needs and challenges of the local population, thus improving human wellbeing.

References

Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). (2012). *The social construction of technological systems: New directions in the sociology and history of technology* (Anniversary ed). Cambridge, MA: MIT Press.

Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner Pub.

Collins, A. (forthcoming). Critical human security and cyberspace: Enablement besides constraint. In K. Hossain, M. Salminen, & G. Zojer (Eds.), *Digitalisation and human security—A multi-disciplinary approach to cybersecurity in the European High North*. Cham: Palgrave Macmillan.

Commission on Human Security. (2003). *Human security now*. New York, NY: United Nations.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*, 701–715. https://doi.org/10.1007/s11948-014-9551-y

Dymet, M. (2019). Digital language divide in the European High North: The level of online presence of minority languages from Northern Finland, Norway and Sweden. *The Yearbook of Polar Law Online, 10(1)*, 245–274. https://doi.org/10.1163/22116427_010010012

European Commission. (2019, September 4). *The digital economy and society index (DESI)*. Retrieved from European Commission website: https://ec.europa.eu/digital-single-market/en/desi

Floyd, R. (2007). Human security and the Copenhagen School's securitization approach. *Human Security Journal, 5*, 38–49.

Gasper, D. (2014). Human security: From definitions to investigating a discourse. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 28–42). London, United Kingdom: Routledge.

General Assembly resolution 32/13, The promotion, protection and enjoyment of human rights on the Internet, A /HRC/RES/32/13 (18 July 2016), available from https://undocs.org/en/A/HRC/RES/32/13

Gómez, O. A., & Gasper, D. (n.d.). *Human security guidance note: A thematic guidance note for regional and national human development report teams*. Retrieved from United Nations Development Programme website: http://hdr.undp.org/sites/default/files/human_security_guidance_note_r-nhdrs.pdf

Gulbrandsen, K. S., & Sheehan, M. (forthcoming). Social exclusion as human insecurity: A human-cybersecurity framework applied to the European High North. In K. Hossain, M. Salminen, & G. Zojer (Eds.), *Digitalisation and human security—A multi-disciplinary approach to cybersecurity in the European High North*. Cham: Palgrave Macmillan.

Haq, M. ul. (1995). *Reflections on human development: How the focus of development economics shifted from national income accounting to people-centred policies, told by one of the chief architects of the new paradigm*. New York, NY: Oxford University Press.

Heininen, L. (2013). 'Politicization' of the environment, and environmental politics and security in the Circumpolar North. In B. S. Zellen (Ed.), *The fast-changing Arctic: Rethinking Arctic security for a warmer world* (pp. 35–55). Calgary, Canada: University of Calgary Press.

Hoogensen Gjørv, G. (2012). Security by any other name: Negative security, positive security, and a multi-actor security approach. *Review of International Studies*, *38*, 835–859. https://doi.org/10.1017/S0260210511000751

Hoogensen Gjørv, G., Bazely, D. R., Goloviznina, M., & Tanentzap, A. J. (Eds.). (2014). *Environmental and human security in the Arctic*. London, United Kingdom: Earthscan.

Hossain, K. (2019). The evolving information-based society and its influence on traditional culture: Framing community culture and human security of the Sámi in the European High North. *Yearbook of Polar Law Online*, *10(1)*, 275–296. https://doi.org/10.1163/22116427_010010013

Hossain, K., Salminen, M., & Zojer, G. (Eds.). (forthcoming). *Digitalisation and human security—A multi-disciplinary approach to cybersecurity in the European High North.* Cham: Palgrave Macmillan.

Hossain, K., Zojer, G., Greaves, W., Roncero, J. M., & Sheehan, M. (2017). Constructing Arctic security: An inter-disciplinary approach to understanding security in the Barents region. *Polar Record*, *53*(1), 52–66. https://doi.org/10.1017/S0032247416000693

Human Security Centre (Ed.). (2005). *Human security report 2005: War and peace in the 21st century*. New York, NY: Oxford University Press.

Kostopoulos, G. K. (2013). *Cyberspace and cybersecurity*. Boca Raton, FL: CRC Press.

Kramer, F. D., Starr, S. H., & Wentz, L. K. (Eds.). (2009). *Cyberpower and national security*. Washington, DC: National Defense University Press.

Krause, K. (2004). The key to a powerful agenda, if properly delimited. *Security Dialogue*, *35*, 367–368. https://doi.org/10.1177/096701060403500324

Latour, B. (2004). *Politics of nature: How to bring the sciences into democracy*. Cambridge, MA: Harvard University Press.

Limnéll, J., Majewski, K., & Salminen, M. (2015). *Cyber security for decision makers*. Jyväskylä, Finland: Docendo.

MacKenzie, D. A., & Wajcman, J. (Eds.). (1999). *The social shaping of technology* (2nd ed.). Buckingham, United Kingdom: Open University Press.

Martin, M., & Owen, T. (2014). Introduction. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 1–14). London, United Kingdom: Routledge.

McSweeney, B. (1999). *Security, identity, and interests: A sociology of international relations*. Cambridge, United Kingdom: Cambridge University Press.

Mearsheimer, J. J. (2014). *The tragedy of great power politics* (Updated edition). New York, NY: W.W. Norton & Company.

Ministry of Government Administration, Reform and Church Affairs. (2013). *Cyber security strategy for Norway*. Norwegian Government Administration Services.

Ministry of Justice. (2017). *A national cyber security strategy* (No. Skr. 2016/17:213). Stockholm, Sweden: Ministry of Justice.

Ministry of Transport and Communications. (2010, June 29). 1 Mbit Internet access a universal service in Finland from the beginning of July. Retrieved from https://www.lvm.fi/-/1-mbit-internet-access-a-universal-service-in-finland-from-the-beginning-of-july-782612

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security*, *26*(2), 87–102. https://doi.org/10.1162/016228801753191141

Pettersen, B. (2011). Mind the digital gap: Questions and possible solutions for design of databases and information systems for Sami traditional knowledge. *Diedut*, *1*, 163–192.

Salminen, M. (2018). Digital security in the Barents region. In K. Hossain & D. Cambou (Eds.), *Society, environment and human security in the Arctic Barents region* (pp. 187–204). London, United Kingdom: Routledge.

Salminen, M. (2019). Refocusing and redefining cybersecurity: Individual security in the digitalising European High North. *Yearbook of Polar Law Online*, *10(1)*, 321–356. https://doi.org/10.1163/22116427_010010015

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High

North. *Polar Record, 54(2)*, 1–11. https://doi.org/10.1017/S0032247418000268

Salminen, M., Zojer, G., & Hossain, K. (forthcoming). Comprehensive cybersecurity and human rights in the digitalising European High North. In K. Hossain, M. Salminen, & G. Zojer (Eds.), *Digitalisation and human security—A multi-disciplinary approach to cybersecurity in the European High North*. Cham: Palgrave Macmillan.

Secretariat of the Security Committee. (2013). *Finland's cyber security strategy*. Retrieved from Security Committee website: www.yhteiskunnanturvallisuus.fi/en

Secretariat of the Security Committee. (2019). *Finland's cyber security strategy 2019*. Retrieved from Security Committee website: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Sen, A. (2014). Birth of a discourse. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 17–27). London, United Kingdom: Routledge.

Tadjbakhsh, S. (2014). In defense of the broad view of human security. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 43–57). London, United Kingdom: Routledge.

United Nations Development Programme. (1994). *Human development report 1994*. New York, NY: Oxford University Press.

Waltz, K. N. (2010). *Theory of international politics* (Reissued). Long Grove, IL: Waveland Press.

Winner, L. (1980). Do artifacts have politics? *Daedalus, 109*(1), 121–136.

Zojer, G. (2019a). Free and open source software as a contribution to digital security in the Arctic. *Arctic Yearbook, 2019*, 173–188.

Zojer, G. (2019b). The interconnectedness of digitalisation and human security in the European High North: Cybersecurity conceptualised through the human security lens. *Yearbook of Polar Law, 10*(1), 297–320. https://doi.org/10.1163/22116427_010010014

Zojer, G., & Hossain, K. (2017). *Rethinking multifaceted human security threats in the Barents Region: A multilevel approach to societal security*. Rovaniemi, Finland: University of Lapland Printing Centre.

3 Citizen and civil society perspectives on cyberspace in the European High North

Johana Evelyn Montalvan Castilla[a)] and Christer Henrik Pursiainen[a)]

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

Executive Summary

This chapter draws attention to the effects that cyberspace and the use of information and communication technologies (ICTs) have on citizens and civil society organisations in the European High North (EHN). We particularly examine the benefits and constraints arising from digitalisation in Northern Norway. This is further explored from a community, regional and cross-border perspective. The qualitative methods of analysis used include structured and semi-structured interviews. The interviews were conducted at five different non-profit civil society organisations. Additionally, a workshop using semi-structured questions was conducted with local inhabitants of Tromsø.

The results of our work include a framework of analysis that can be used as a tool to understand and study civil society in light of the changes brought by digitalisation and ICTs. Moreover, preliminary findings and observations on the perceived integrating and disintegrating effects of digitalisation on civil society in Northern Norway are presented. Civil society in the EHN is both the subject and object of multiple digital and cybersecurity policies. In this regard, our future research will focus on cybersecurity and civil society

developments in Northern Norway and will include other case studies, a larger study sample and the application of mixed research methods.

3.1 Introduction

The emergence of cyberspace, the widespread use of information and communication technologies (ICTs) and the digitalisation of important societal services have transformed the way of life for individuals, communities and societies. It is therefore important to move from a mere technological understanding of cyberspace and ICTs to a more profound understanding of the effects of ICTs on democratic politics, societal processes, changes and emancipation.

This chapter examines the beneficial effects as well as the downsides and risks arising from digitalisation and its implications for citizens and especially civil society in Northern Norway. Civil society can be seen as a major component of the society–state relationship, and this relation is essential in defining the socio-political system of any modern state.

As with other communities in the European High North (EHN), local communities in Norway are objects and subjects of a diverse array of digital policies. On the one hand, this means that they have a decisive role in co-defining post-modern cyber reality. On the other hand, it means that they are vulnerable to the pressures of globalisation and nation-state policies.

We identified a lack of research and case studies on the effects of cyberspace on citizens and civil society in the EHN. Our task was to first develop a generic framework of analysis to make sense of digitalisation/civil society interaction that is applicable in this region and

beyond and to second use this tool to understand and empirically analyse civil society in light of changes brought about by the emergence of cyberspace.

Our research addresses human security questions in Northern Norway to give a voice to citizens, local communities and civil society. It particularly focuses on economic, social, political and environmental dimensions from the perspective of individual citizens/inhabitants and civil society organisations. Although there are always several causal factors affecting the formation of societies, our task leads us to focus especially on cyberspace-related phenomena, such as the internet, social media, ICTs and so forth.

3.2 Cyberspace and civil society

Our initial research sought to illustrate and analyse some of the effects of cyberspace on civil society. In order to do so, a framework for analysis was created. This was used in conjunction with small-scale observations conducted at civil society organisations. We then mainly focused on themes such as self-organisation, participatory democracy, participation in governance, immigration issues and cross-border cooperation. Additionally, our work has pinpointed some of the threats and risks created by cyberspace.

Our work also highlights cyber-dependent infrastructures and vital societal functions in the context of long distances, limited accessibility and harsh environmental and climatological conditions. Challenges and threats arising from social phenomena such as cross-border organised crime, terrorism, jihadism, xenophobic groupings and radicalisation are also addressed.

We started with an extensive literature review in order to identify the research problems and gaps in the aforementioned research areas. Methodologically, relevant statistics and data such as qualitative interviews and social media outputs were collected. The initial data collection took place in Tromsø and Oslo. The selected and detailed case studies allowed us to address the issues mentioned under the two blocks.

Although the main geographic focus is on Northern Norway, our research also includes some comparative perspectives between Northern Norway, Norway at large, other Nordic countries and beyond. A complementary, comparative approach is useful to gain understanding of whether location makes a difference in cyberspace, and if so, to understand the mechanisms through which this has developed.

3.2.1 Research questions

The research questions addressed in this study include:

- What effect has the emergence of cyberspace and ICTs had on civil society (citizens) and civil society organisations in the Norwegian High North?
- What advantages/benefits (social, economic, organisational, etc.) do civil society organisations in the Norwegian High North experience or have experienced over the last years? due to the use of the internet and ICTs?
- Regarding cyberspace and the use of ICTs, what constraints or disadvantages do such organisations experience?
- How have particular organisations changed and if so, through which mechanisms?

- Has a transnational dimension enhanced the emergence of cyberspace? If so, how or through which mechanisms?
- Have ICTs enhanced political participation and contact with authorities? If so, how?
- Has cyberspace enhanced or decreased social phenomena such as radicalisation, extremism or xenophobia? If so, what have been the effects?
- Have cyberspace and ICTs helped further cross-border communication and the presence of organisations? If so, how?

3.2.2 An analysis of cyberspace and its effects on civil society

Numerous societal and organisational changes have appeared as a result of the emergence of cyberspace and digitalisation. In order to analyse the areas in which such changes have taken place, a framework for analysis was created to classify and understand the nature of these changes.

Our first publication on the subject (in Montalvan Castilla and Pursiainen, 2019) is an exploratory study that examined the effects of cyberspace on one part of a democratic society, namely civil society.

Civil society is a major component of society–state relations, and these relations can be understood as the main ingredient in defining the socio-political system of any post-modern state. Thus, in order to argue that the emergence of cyberspace is constitutive as to the nature and characteristics of civil society, we must move from a mere technological understanding of cyberspace to a more profound understanding that considers democratic politics and emancipation.

Civil society is a very complex issue, and the concept has been the focus of political philosophers in the past two centuries. Although the issues at stake amount to a veritable battlefield of different conceptions, we have simplified the issue by dividing the understandings of civil society into four categories: apolitical, political, transnational and 'uncivic' (for example, the mafia) civil societies.

Consequently, we are concerned with the question of what kinds of civil society cyberspace enables or enhances and what kinds it limits or constrains. This framework for analysis is presented in Table 1.

Effects of digitalization	**Apolitical civil society**	**Political civil society**	**Transnational civil society**	**Uncivic civil society**
Enhances	Entrepreneurship (and possibly individualism) Visibility Mobilisation and recruiting Two-way and mass communication Cost reduction and efficiency	The construction of social and political consciousness Visibility Mobilisation and recruitment Two-way and mass communication Bottom-up initiatives to challenge or influence elite decision-making	Cross-border learning and exchange of ideas Cross-border concrete collaborative efforts and mobilisation Cost-reduction and efficiency	Manipulation of popular opinion Recruitment and mobilisation intolerance- or violence-based extreme right-wing, left-wing and jihadist groupings Cyber crime targeting to cyberspace assets, or using it as a tool to reach non-cyber assets

Constrains	Resource-consuming, and therefore favours larger organisations Favours organisations with younger members Digital exclusion on individual or group level Impersonalisation of communication, leading to (cultural) misunderstandings and lack of trust Fear of cyber insecurity	Political manipulation through cyberspace Authoritarian countries or large companies control the cyberspace and use it for their own benefit Overoptimism of digital power to create political change Benefits one-issue activist more than established political movements Relies largely on existing beliefs Fear of cyber insecurity	Cyber security problems (sensitive information, espionage) Ignorance of the of criticism of transnational civil society of the cyberspace campaigns Overoptimism of digital power to create political change Focus deflected away from off-line activism	Communication spaces can be infiltrated, monitored, hacked and traced back in forensic investigations by the authorities or activist groups State and public-private strategies and activities to fight cyber crime by capacity- and capability building

Table 1: Framework for Analysis (Montalvan Castilla and Pursiainen, 2019).

Through reorganising the existing research according to our framework and adding our own small-scale observations and interviews, we aimed to make sense of empirical cyberspace developments in relation to different modes of civil society activities. Although the empirical focus was on (Northern) Norway, we believe that the framework of analysis developed here can be

applied and tailored to any society. It is expected that this framework will facilitate the understanding of the societal changes created by digitalisation.

3.2.3 Methodology

We first studied the online media profiles, presence and activities of five civil society organisations. These organisations were dedicated to human rights, advocating for children's rights and protection, humanitarianism and, in two cases, the environment. Careful observations were conducted regarding a) the interactions of the organisations with general citizens and other members of the organisation, b) their capacity to influence and mediate political and civic arenas and c) their contact and/or cooperation with other civil society organisations abroad.

Secondly, we visited these organisations and conducted in-person interviews. Semi-structured interviews were chosen as a preferable qualitative research method because of their open structure. An interview guide with the main themes and questions was prepared. These themes and questions allowed participants to present their own concerns and narratives regarding the effects of cyberspace on their organisations.

In most cases, the main interviewees were the leaders of the organisations. A few other people working in such organisations also participated and responded to some of the questions. One of the organisations had a professional department for the management of social media networks. In this case, a full-length interview was conducted with the leader of this department in order to understand organisational changes, benefits and challenges that the emergence of cyberspace may have brought.

The humanitarian organisation interviewed was divided into several local departments and/or work teams that addressed different societal needs and provided community services. We primarily interviewed the search and rescue department and the department responsible for the integration of refugees in Northern Norway.

The organisations were chosen because of their active presence in Northern Norway and their transnational dimension, meaning that they continue to expand or grow and have established transnational contacts and partnerships. The literature shows that the emergence of cyberspace or networked communications have had a huge impact in the way organisations, particularly civil society ones, work, develop or are strengthened. This is mainly noticeable through international contacts, alliances or partnerships that partially and increasingly rely on digital ICTs for cooperation. In some cases, contact and joint work between civil society organisations in different countries would not have been possible without the emergence of cyberspace and ICTs.

Having formulated our tentative empirical conclusions, in the final phase of our study we summarised them into five simple multiple-choice questions used in an online survey. This survey was sent to 15 organisations to confirm our conclusions.

3.2.4 Results

Our findings illustrated that cyberspace and ICTs have contributed to significant changes in present day Norwegian civil societies. However, while these changes have been profound in fields such as internal and

external communication and interaction between members, the public at large and authorities, they are rather instrumental, not affecting the basic norms, cultures, goals and interests of the organisations.

After exploring some of these changes, it can be concluded that cyberspace has both enhanced and constrained civil society. Thus, we identified the need to analyse these enhancing and constraining effects through a comprehensive theoretical framework. In our analysis of societal changes due to the rise of cyberspace and ICTs, we identified four types of civil society: apolitical, political, transnational and uncivic.

Our research findings showed that cyberspace has opened new paths for both entrepreneurship and individualism for the apolitical civil society. Additionally, we noticed that although cyberspace presents itself as beneficial in many aspects for the transnational civil society, some constraining elements can be identified. For instance, social media platforms are resource and time demanding. This implies that organisations with more resources will have a stronger online presence and potentially attract new members. Thus, these findings shed light on the role that web technologies may play in furthering inequality.

It appears that the emergence of cyberspace has revolutionised the political civil society. Earlier studies (e.g. Howard and Hussain, 2013; Papacharissi, 2004) showed that the potential for civil discourse in cyberspace is strong and that it might promote democratic emancipation and political engagement/participation.

Thus, it appears that digital technologies facilitate the construction of social and political consciousness. In the case of Norway, the evidence suggests

that these technologies have considerably enhanced civic and political engagement. For instance, Facebook's ad hoc groups and their communicative power have the potential to raise societally and politically important issues among the public as well as initiate changes. Social media can also exert a strong effect on mobilisation. This can have a direct impact on local communities, concretising local help and development initiatives. In some instances, cyberspace appears to have become a meeting point between people and politicians.

Cyberspace has also had an impact on the transnational dimension. Data coming from researchers at the Norwegian Centre for Research on Civil Society and the Voluntary Sector (see Arnesen et al., 2016; Eimhjellen, 2013, 2014; Eimhjellen and Ljunggren, 2017) showed that some Norwegian non-governmental organizations have benefited from social media platforms, which allow them to keep in contact with other organisations. Our own findings at a humanitarian organisation in the Norwegian High North illustrated the cross-border connections that can be established through digital technologies. This organisation works, exchanges information and coordinates online with another one in Murmansk.

However, mistrust and scepticism toward the internet as an effective place for civic participation have occurred. For instance, cybersecurity issues regarding the exchange of sensitive information online have been reported.

Finally, the uncivil dimension of civil society illustrates the issues arising from openly intolerant and sometimes extremist groups that use cyberspace to communicate. We illustrate this by studying well-known groups in Norway such as Stopp islamiseringen av Norge (popularly known as

SIAN), which has thousands of members who communicate with each other and share information through the web and Facebook. Additionally, cybercrime and malicious or criminal acts have occurred in cyberspace. As a result, the National Strategy for Information Security was implemented by Norwegian authorities.

The above notwithstanding, we conclude (somewhat surprisingly given the enthusiasm for cyberspace as an ultimate game changer) that while cyberspace has contributed to some seemingly significant changes in the characteristics of Norwegian civil society, it is more a question of basically instrumental qualities rather than intrinsic transformation of the society. Cyberspace itself has not democratised or undemocratised societies by changing the balance between different types of civil society activities or the basic characteristics of society–state relations.

3.3 Citizens' perceptions on digitalisation: Benefits and challenges

The changes, enablers and constraints brought by ICTs and their effects on civil society can be better understood by approaching a combination of civil society organisations, individuals and local communities in the EHN. In this regard, a second study was designed with the aim to hear stakeholders' perspectives and opinions on the effects of digitalisation in the region on their interrelated everyday experiences.

3.3.1 Methodological considerations

The World Café methodology was applied. Also known as the Knowledge Café methodology, it consists of structured conversations taking place at different tables. The discussions took place in a comfortable local café in Tromsø. This atmosphere was chosen with the aim of helping participants relax and facilitating further discussions. The 12 participants were of different backgrounds and occupations and were recruited by previous familiarity and interest with the projects' scope, through social media and using snowball sampling. Among the participants were two local politicians and the director of an important company with a large presence in the three counties that comprise Northern Norway. Both genders were represented, and the participants' ages ranged from 23 to 60 years. Three table hosts were also present to moderate, guide, focus and balance the discussions. Their role was to ensure that everybody had a chance to speak, give their opinions and share their relevant personal experiences.

Prior to the discussion, the workshop goals and details were introduced and the ethical aspects covered. Six main themes emerged during the discussions. At the end of the sessions, the discussions were summarised.

The themes that were discussed were 1) use of ICTs in everyday life, 2) aspects of life transformed (or not) by ICTs; satisfaction, fears and desires regarding particular ICTs, 3) factors facilitating or hampering digital development and opinions on how to ensure the desired development and prevent counter-productive development, 4) fears, desires and wishes regarding digital and technological development, 5) individual power of influence on regional digital development, 6) digitalisation and the role of

the state, regional and local administration, companies, associations, communities and individuals in developing and maintaining security and trust.

3.3.2 Preliminary results

3.3.2.1 Perspectives on ICTs and their everyday use

Participants were most satisfied with transport-related digital solutions. Tromsø can experience harsh climatological conditions. Temperatures can easily reach -11°C and feel like -16°C. Cold winds and heavy snow falls are also common. The regular traffic flow can be substantially affected due to heavy snowfalls or icy roads, which cause accidents and delays. The municipality's real-time application (app) showing timetables, routes, connections and delays due to climatological conditions was thus praised. Before this app appeared, users waited much longer at bus stops or missed bus connections. The possibility to purchase bus or flight tickets through an app and the municipal parking app were also appreciated.

Regarding ICTs, the use of e-mail, social media (predominantly Facebook, Instagram and Twitter) and diverse websites was part of everyday life. Only one participant said that they avoided social media. Facebook appeared to be an important means of socialisation and organisation of work or study events, facilitating local and global interaction.

ICTs used for inclusive purposes and in the educational system were regarded as positive. Digital health services, such as health applications that allow online communication between patients and medical personnel, were seen as positive by some. However, the fact that these apps and online

patient journals keep track of the patients' medical history, concerns and communications was considered to be a risk and possible security threat. Financially, banking and financial transactions done digitally were perceived as beneficial because they increase efficiency and productivity.

Regarding digital services needed, better design tools for architects and designers were requested along with (gender-based) applications focusing on the security of women and apps to report on improvements needed in the city, particularly in relation to lighting. Online shopping opportunities were also valued. However, participants highlighted the need to reduce consumption and further sustainability. Software applications focusing on a sustainable lifestyle and guiding users towards plastic-free or ethically produced items were also requested.

3.3.2.2 Aspects of life transformed by ICTs: Satisfaction, fears, wishes and resistance regarding digital development

Parenting, family life, level and quality of social interaction, education, democracy and social and political spheres were identified as areas significantly transformed by ICTs. Moreover, the way in which we communicate has been transformed, as traditional time and place constraints have been removed, allowing for transnationalism. Regarding fears, the inability to sort out real news from fake news, propaganda and political and social manipulation through the internet and social media were regarded as concerning.

It was expressed that cyberspace had a positive effect on social interaction and social capital. This was illustrated by the experiences of participants who joined online groups. These groups (for example, those with social and

humanitarian causes, political groups and hobby groups) connected people with similar interests and goals, sometimes leading to offline meetings.

However, many reported a perceived reduction in social contact or interaction (such as fewer in-person meetings and lectures as well as fewer workers at banks, libraries, supermarkets and stores due to being replaced by automatised digital cashiers, chat bots and online assistants) due to ICTs. Some participants expressed the desire to avoid a future with decreased human contact.

Participants also pointed out that digitalisation has transformed the dynamic between students and teachers, as students could rely on a vast array of online material and depend less on lessons at the university. Satisfaction was also expressed regarding the amount of knowledge one can acquire online, such as practical skills or formal knowledge in a particular field or subject. The ability to research health issues and diseases and the possibility to share information online or communicate with others experiencing similar conditions was seen as a positive development.

Other major concerns were related to cyberspace being used as an arena for bullying and exclusion. Cybercrime, the hacking of smartphones and a potential ‘surveillance nightmare’ or totalitarian technological surveillance were feared. Participants wished to avoid a future were all personal information is under the control of the government and private companies.

At the personal level, the desire to preserve anonymity and privacy was expressed. Some participants noted that in modern society, children are exposed to society even before birth, with ultrasound pictures posted on

social media. Additionally, some participants saw as more negative than positive that children these days are tracked through smart devices.

3.3.2.3 Digital development

Participants found cyber insecurity to be the biggest factor impeding positive digital development. The use of digital health services (for example, patient journals), digital post services, financial scams and use and storage of personal information by websites were seen as potential threats to information security. Other related counterproductive factors were the negative effects of ICTs on democracy due to manipulation of information and the spreading of fake news.

According to some participants, measurements to prevent negative digital development should involve actors such as the local government and public libraries. Both institutions could provide more information and a space for discussion among the city's inhabitants on how to mitigate cyber insecurity and its societal effects.

Factors identified as hindrances to a balanced digital development were online phenomena such as harassment, hate speech, racism, extremism, xenophobia and bullying. The creation of large networks linked to child abuse, pornography and human trafficking was also seen as a negative aspect of ICTs. Actions taken by the police to monitor, prevent and stop such phenomena were thus deemed important.

Additionally, the digital divide and exclusion, particularly of elders and minorities, were seen as hindrances. It was noted that technology has a tendency to overlook or exclude minorities in society. Consequently, digital

technologies are not created to meet their needs. Some participants also argued that ICTs can reinforce class differences in society, pointing to differences between the people who produce or own the rights to diverse ICTs, those who pay for them and those who have the adequate knowledge to use them.

It was also stressed that despite the advantages offered by the digitalisation of societal services, direct physical, cognitive or mental stimulation and a greater engagement with an individual's surroundings have been substantially hampered. Participants also acknowledged a lack of focus and increasing disruptions, which occurred when participants became distracted by the internet and social media while performing specific tasks at work, home or university.

A main concern for many participants was that digitalisation may be driven by economic interests and thus not always focus on the best interests of the people. Some statements that illustrated this were: 'the technological development is enormously driven…[by] commercial and economic interests' and 'it is not technology that adapts to our needs. It is us who adapt to the technological solutions that come along'.

Participants also discussed whether telemedicine services in Northern Norway are mainly driven by economics (focused on saving money and resources) and not to the best interests of the patient. One positive aspect of telemedicine was that health services could be provided to populations living in more remote areas.

It was also noted by participants that attended so-called ‘smart city’ conferences in Norway and abroad, that these conferences often ended in companies trying to promote and sell their services or technologies.

Participants negatively viewed companies’ practice of collecting user data to target potential buyers through custom-made advertisements, predict purchase patterns or influence customers. The development of eye-tracking technology and filming to analyse users’ preferences was also seen as controversial. Equally, the imposition of smart electricity meters in Norway was perceived as a potential danger. These meters report when a person is at home as well as patterns connected to household activities.

Surveillance was perceived as a counter-productive factor for desirable ICT developments. Although video cameras connected to the internet can often be used for security, participants were concerned that widespread surveillance can lead to the loss of privacy and freedom as well as increased societal control.

Additionally, it was suggested that for positive development to take place, state-based research should be conducted before acquiring new technologies. Likewise, personal awareness, discussions and reflection on the downsides and benefits of ICTs were viewed as necessary. It was proposed that to facilitate positive development, the state and municipality should have a clear overview of the needs, goals and wishes of the city and its inhabitants. After this is done, the government can begin outlining the pathway needed to bring about this technology. In relation to this, female participants felt that new technologies should include gender perspectives. This may increase security for women and other vulnerable groups.

3.3.2.4 Fears and desires regarding digital development

Common fears regarding digital development included an increasing digital divide, particularly for elders. A participant illustrated this issue by mentioning that several elders visit the Norwegian Labour and Welfare Administration to request assistance submitting online forms now that traditional paperwork is no longer an option.

Some participants agreed that despite fears and perceptions that digital development is purely economically oriented, the digitalisation of societal services saves time and resources in the long term. One concern was that patients who still wished to have in-person consultations might only have the choice of online consultations, as the number of health care providers has been drastically reduced. This may be counterproductive to the treatment of conditions such as depression.

Participants requested ICTs to track and prevent criminal behaviour, especially against women and children. Participants also commented on the terrorist attack in Norway by Anders Breivik, which resulted in the death of 77 people. It is known that Breivik connected with others with similar radical views online and received their support and encouragement. In Norway, operations such as the one known as ‘Dark Room’ serve men who plan to rape children and share online materials of them being abused. For some participants, these examples illustrated that cyberspace can be an arena for criminal associations.

Other desires included online apps that provide information about cultural events and local history and places. Moreover, there was a desire for the establishment of a local committee on ICTs and digital development. A

participant noted that in the Tromsø municipality, there are permanent committees for urban development, the private sector or industries, sports and the educational sector, among others. However, he stressed that the local political organisation lacks and needs a committee that will work towards positive digital development involving citizens.

3.3.2.5 Individual power of influence on (regional) digital development

Most participants expressed that in order to have some influence on the course of regional digital development, it is necessary to first contact the municipality and politicians. Similarly, they acknowledged that cyberspace per se cannot be completely controlled or constricted to local rules.

One participant (a politician) said that at the political level, citizens can influence regional digital development by actively participating in political meetings and discussions at the local and national levels. Institutions ensuring personal information security, such as the Norwegian Data Protection Authority, have resulted from discussions at the civil society and political levels.

The power civil society has to influence local development through social media and online groups was also highlighted. To illustrate this, concrete examples were given, such as online campaigns with high local engagement. These campaigns and online events later led to considerably large offline demonstrations and meetings. For example, the preservation of the Alfheim public swimming pool and building, the pride parade and activities related to LGBTQ rights and the Me Too movement have influenced decision makers.

However, it was noted that online participation does not always lead to offline meetings and active democratic participation. The Tromsø-based online group called No to Road Tolls had about 11,500 online members and followers. However, only 20 people showed up to a demonstration in front of the municipality.

Some participants further argued that digital development influences people and not the other way around. Others added that such development happens regardless of the local population's wishes.

3.3.2.6 Cybersecurity, security and trust

More than half of the participants felt that individuals were responsible for learning how to use ICTs carefully so as to maintain security. It was stressed that a person must have awareness of the risks present in cyberspace. Participants regarded Facebook as an unsafe platform, commenting on hacked accounts and the amount of user information that the site stores and sells. Particularly, the events linked to Cambridge Analytica their social and political consequences were mentioned.

Participants felt that it was the responsibility of the government and local and regional authorities to provide information and training to citizens to improve their digital security. This could be imparted through public or private classes at workplaces or organizations. The Swedish government takes this responsibility seriously, and it mailed letters to citizens discussing issues concerning societal security and vulnerabilities, resilience and cyber(in)security.

Two participants emphasised that the private sector has the responsibility to safeguard people's information. One added that companies operating in Norway should assume greater responsibility than they currently do regarding the client information that they collect and keep.

In light of the changes brought by digitalisation, it was argued that the state has an important role in guarding the personal data of citizens and their safety. For example, according to one participant:

> It is the state that must keep us safe. If it cannot keep us safe, then it is the same not to have it. This is the actual reason for what I pay taxes for…because they have a national security authority, and organisations such as the Norwegian Data Protection Authority. They [the government] have resources that are used to create order and implement the legislation and that can provide guidelines at all levels and for private companies in Norway.

Finally, to enhance trust, it was suggested that the integration or widespread use of digital solutions that render more effective and cost-efficient services was positive but not enough. Respondents felt that it was also necessary to involve the city's inhabitants and hear about their needs and wishes.

3.4 Digital development in small communities and organizations in northern Norway: a case study from the Lofoten islands.

We were interested in contributing to deepen the current understanding of the perceived impact digitalisation has had in civil society organizations located within small communities, and how these communities and their civil society organizations experience such changes.

For our study, we chose the Lofoten archipelago, considered one of the world's northernmost populated regions, located in the Arctic Circle and belonging to the county of Nordland, Norway. Nature-wise, the islands are known for their beauty and dramatic mountains and peaks. Fieldwork took place in Svolvær and in the villages and towns of Kabelvåg, Henningsvær and Leknes. During fieldwork visits carried in the spring of 2018 and the autumn of 2019, eight formal interviews were conducted and two small semi-structured 'citizen cafés' took place, as well as formal and informal conversations with local inhabitants.

The voluntary organizations that were formally interviewed include humanitarian organizations, political organizations, nature or environmental protection organizations, hobby organizations and an organization coordinating volunteering work in the region. Some preliminary observations from the field are presented below, as beneficial and constraining effects brought by the digital development in the area.

Enablements brought by digitalisation, according to citizens and organizations participating in the study include: a) search and rescue operations partially benefited upon the implementation of digital services b) ability to easily connect with other organizations, individuals and communities despite remoteness or vast geographical distances, c) local organizations gained increased support nationally and internationally to promote their environmental and political agendas, c) greater educational opportunities were facilitated by online education, d) efficiency and cost reduction at organizations was enhanced, e) the local economy benefited due to increasing tourism and higher demand of Airbnb accommodations and local services, f) communication with local authorities was enhanced.

Main constraints identified by citizens and organizations include: a) Increased tourism in the Lofoten archipelago, as a result of Instagram and Facebook posts, has caused that important natural areas are damaged or affected by littering, b) death and accidents in the local mountains were reported to be linked to tourists' search for the 'perfect selfie' or picture c) search and rescue operations in the mountains and high peaks have increased due to a greater flow of tourists, d) cyber-hate, surveillance and everyday cyber-(in) security issues were reported by organizations and citizens, e) a great number of services have been completely digitalized, some of them against the wishes of individuals (physical banks have disappeared, ATMs, fewer postal service points present, etc.), f) a sector taking part in the local economy was affected, such as the hotel branch and small businesses, as Airbnb and online shopping are on high demand.

Among the changes brought by digitalisation, it is particular to the area that, in the perception of many participants, tourism was greatly enhanced by social media. Pictures and posts shared in Instagram and Facebook, highlighting the exotic and beautiful nature in the Lofoten islands, were seen as a main factor that caused more tourists to visit the area. As reported by individuals, local help groups and search and rescue organizations, this resulted in damage to the natural landscape and littering and contamination.

These and other listed empirical findings, to be explored in-depth in our coming article, throw light on the positive, negative and challenging sides of digitalisation, experienced by citizens and civil society organizations embedded in small communities.

3.5 Preliminary conclusions

We believe that our research may be used as a starting point to illustrate and analyse some of the changes that civil society in the Norwegian High North has experienced due to the use, development and integration of ICTs. The implications of such changes may then be regionally compared and analysed. By shedding light on the constraints and benefits that cyberspace and ICTs have had on individuals, communities and organisations, further recommendations can be provided as to how to mitigate the negative effects and enhance the positive ones.

For instance, due to the digitalisation of services, citizens and organised civil society may become particularly vulnerable in instances of internet and ICT service disruptions. This is particularly true if there is limited technical resiliency and a lack of alternative ways to continue to operate and benefit from these services. It should also be noted that issues connected to privacy or data protection, cybercrime and increased societal vulnerability occur more frequently today. Thus, we hope our research can suggest ways to mitigate or prevent unwanted consequences that may hinder civil society in Northern Norway.

Our findings show that cyberspace has not profoundly changed society in terms of the relative power that one type of civil society can have over another. Digitalisation itself has neither democratized nor undemocratized societies (including the Norwegian society) by changing the balance between different types of civil society modes or altering the essential characteristics of society-state relations. Our results do not adhere to the idea of giving cyberspace the status of ‘agency’ in its own right.

Digitalisation appears, however, to have had a transformative, generally positive impact in the way communication happens between local communities and civil society organizations in northern Norway. Geographical distances were much less constraining when instant communication and coordination in cyberspace happened, also influencing the transnational level as well as communication with local authorities. Similarly, the rendering of different services (now digital) and their effectivity was seen as positive.

Another preliminary finding strongly suggests that the digital development, despite being praised by some for bringing increased effectivity in services and cost-reduction, has constraining effects. As expressed by several civil society organizations and citizens in Tromsø Lofoten, local communities appear, to some extent, to have been significantly and negatively impacted by the digital development. These findings may suggest the need for new strategies to cope with this kind of unwanted development.

At the citizen level, some of our findings point out that citizens experience enhanced, everyday cyber insecurity and wish for more effective ways to reduce or prevent them. Combined efforts from citizens, local and national authorities have been suggested by citizens and local authorities themselves to safeguard their personal data and to prevent fake news or other possible adverse effects on democracy.

By closely working and interacting with local civil society organisations and individuals, our work has sought to integrate local perspectives into the analysis of digital developments in the EHN. Building on our previous data and the proposed framework of analysis, our work will be expanded and

continued. We can then further discuss the implications our findings may have for civil society and issues such as democratic participation and transnational cooperation.

3.6 Follow Up

The civil society framework outlined in Section 2 will be followed up with a more empirical, quantitative, survey-based and indicator-based peer reviewed journal article, which is currently in progress. Over 6000 non-governmental organisations registered in Northern Norway (Troms and Finnmark regions) will be the empirical focus of that article. Empirical findings from the case study in the Lofoten islands will complement our study. The information from the World Café experiment discussed in Section 3 will be used in a comparative article of Finnish and Norwegian experiences.

References

Arnesen, D., Sivesind, K. H., and Gulbrandsen, T. (2016) *Fra medlemsbaserte organisasjoner til koordinert frivillighet? Det norske organisasjonssamfunnet fra 1980 til 2013*. Rapport 2016:5. Senter for forskning på sivilsamfunn og frivillig sektor.

Eimhjellen, I. (2013). Internet communication: does it strengthen local voluntary organizations? *Nonprofit and Voluntary Sector Quarterly* 43 (5), pp. 890-909.

Eimhjellen, I. (2014). Web technologies in practice: the integration of web technologies by environmental organizations. *Media, Culture & Society*, 36(6), 845-861.

Eimhjellen, I. and Ljunggren, J. (2017). *Kollektiv handling i digitale medier*. Bergen/Oslo: Senter for forskning på sivilsamfunn og frivillig sektor.

Howard, P.N., and Hussain., M.M. (2013). *Democracy's Fourth Wave?: Digital Media and the Arab Spring*. UK: Oxford University Press.

Montalvan Castilla, J. E., & Pursiainen, C. (2019). Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not? *Journal of Civil Society*, 15(4), 392-411. https://doi.org/10.1080/17448689.2019.1672288

Papacharissi, Z. (2004). Democracy online: civility, politeness, and the democratic potential of online political discussion groups. *New Media and Society*, April, Vol.6(2), pp. 259-283.

4 ICT access and use among elderly people in the European High North

Kristin Smette Gulbrandsen[a)] and Michael Sheehan[b)]

a) Department of Human Geography, Lund University
b) Swansea University

Executive Summary

Digitalisation is rapidly changing the availability of information and services online. This is accompanied by cutbacks to physical services in an attempt to save costs and increase efficiency. Digital skills have thus become critical to accessing and benefiting from developments in the digital age. This may have implications for social inclusion in geographically peripheral and sparsely populated areas such as the European High North (EHN). To address this, we used a modified framework of human and cybersecurity. Analysis of our fieldwork data indicated that this framework supports some of the key insights in the literature on digital divides in rural areas. Firstly, digitalisation is seen as highly beneficial to the EHN because it enables people to live, study and work in peripheral areas. Secondly, people distinguish between different uses of information and communication technologies (ICTs). Some services, such as online banking, are perceived as more beneficial but also more complex than others. Thirdly, younger family members are an important resource to many elderly people when using digital technologies. Lastly, not all services are fully accessible, especially for people with visual impairments. Additionally, the provision of services in Sámi languages is often not prioritised. Overall, our findings show that digitalisation provides new solutions and opportunities

that are crucial in remote areas like the EHN. However, unless its limitations are seriously considered, sections of the population may be excluded from its full benefits.

4.1 Introduction

Our research explores the relationship between digitalisation and social inclusion/exclusion in the European High North (EHN). Specifically, we examine social exclusion from the perspective of human security, arguing that this should be incorporated into a broader conception of cybersecurity. This means that the enabling and constraining aspects of digitalisation and digital technologies can be considered at the individual and community level in terms of protecting citizens' freedoms from fear and want. In order to gather primary data for our case studies, we conducted fieldwork in northern Finland and Norway. Both field trips involved semi-structured interviews with key informants in the region. The qualitative data generated by the interviews support some of the key insights in the literature on digital divides in rural areas.

4.2 Theoretical framework

Our theoretical framework bridges the literatures on security and social exclusion, showing how exclusion can be thought of as an element of human security and why the security of individuals and communities should be integrated into the wider cybersecurity debate. We briefly define these concepts below and integrate them into a single research framework, which is then applied to the EHN case study.

4.2.1 Security

Traditional approaches to security within international relations focussed on military threats to sovereign states (Mearsheimer, 2001; Morgenthau, 1973; Waltz, 1979). This narrow understanding of security was proposed in the 1980s during the post-Cold War period due to the emergence of a broader security agenda encapsulating additional sectors, such as environmental, economic and societal security (Barnett, 2001; Buzan, 1991; Buzan, Wæver, & de Wilde, 1998; McSweeney, 1999). This transition from a state-centric and military focussed understanding was reinforced by the subsequent emergence of critical security approaches (Booth, 2007; Holland & Jarvis, 2015; Sheehan, 2005; Wyn Jones, 2007) and by the adoption of a human security approach by the United Nations Development Program (1994). These developments made it possible to address security not simply in terms of additional sectors but, crucially, to focus on the individual human being or sub-state communities as the referent object (Booth, 2005, p. 22).

4.2.2 Cybersecurity

When the concept of cybersecurity emerged, this too was initially narrow in scope, focussing on the identification and protection of critical infrastructures. The human being was generally excluded from the pool of potential referent objects and had the status of the weakest link, threat or victim (Dunn Cavelty, 2014, pp. 703–704). By shifting the referent object of cybersecurity to the human being, it became possible to analyse cybersecurity not simply in terms of the problematic dimensions of human cyber use but in terms of its enabling and constraining effects.

4.2.3 Human security

The 2003 report by the Commission on Human Security defined human security as:

> The protection of the vital core of all human lives in ways that enhance human freedoms and human fulfilment … [including] processes that build on people's strengths and aspirations. It means creating political, social, environmental, economic, military and cultural systems that together give people the building blocks of survival, livelihood and dignity (p. 4).

Creating a framework for human cybersecurity requires a brief unpacking of the concept of freedom. In human security, freedom from fear and want corresponds to the notions of negative and positive freedoms (Alkire, 2003). As such, freedom from fear is concerned with survival and is protected by civil and political rights. In the digital world, therefore, threats to the freedom from fear component of human cybersecurity include threats to privacy and freedom of expression as well as theft and fraud. Subsequently, freedom from want is concerned with livelihood and dignity and is realised through economic, social and cultural rights. In the digital world, this covers issues such as economic and educational opportunities as well as access to services. Defined this way, the concept of human security embraces many of the dimensions prominent in the social exclusion literature. From this view, human security can be considered 'a comprehensive approach that integrates the notion of social exclusion and links it to an extended framework that includes economic security, health, education, conflict, governance and migration perspectives' (Sokoloff & Lewis, 2005, p. 6).

4.2.4 Social exclusion

There is no generally accepted definition of social exclusion, but some of the most widely used definitions have clear commonalities. Burchardt, Le Grand and Piachaud (2002) argued that an individual is socially excluded if they do not participate in key activities in the society in which they live, though this is a rather broad definition. Sen (1999) noted that social exclusion may result from a lack of the capabilities required to participate in the experiences that lead to social inclusion. Often, the concept is associated with explicit citizenship rights (Berghman as cited in Noll, 2002, p. 56). Levitas et al. (2007) offered the following definition:

> Social exclusion is a complex and multi-dimensional process. It involves the lack or denial of resources, rights, goods and services, and the inability to participate in the normal relationships and activities, available to the majority of people in society, whether in economic, social, cultural or political arenas. It affects both the quality of life of individuals and the equity and cohesion of society as a whole (p. 9).

Byrne (1999) also emphasised the deprivation of social goods as a form of exclusion. There are thus clear similarities between the social exclusion concept and the prominent criteria in various definitions of human security.

Restricted access to opportunities and limited capabilities to capitalise on these, along with reference to the social and economic dimensions of exclusion, seem to characterise most of the above definitions. Thus, social exclusion is more than material deprivation. Rather, it is the relative lack of economic, social and cultural capital required to realise human freedoms. Social exclusion therefore hinders freedom from fear and freedom from want and as a consequence constrains the individual’s or community’s

ability to access and capitalise on opportunities and achieve security. Below, we clarify what this means from a human cyber perspective.

4.2.5 Measuring social exclusion

When studying social exclusion, it is useful to view it through a constructivist lens. This highlights that the concept is highly normative; many definitions of social exclusion refer to exclusion from activities that are normal or available to the average or majority of citizens. Because of the relative and normative nature of social exclusion, there is reason to question some of the quantitative indicators often used to measure it. For example, van Regenmortel et al. (2016, pp. 333–334) argued that the operationalisation of social exclusion varies between cases, as the experience of social exclusion is context dependent. A universal measure of social exclusion variables will not be appropriate or applicable in all cases, which is the case with existing research on social exclusion and the elderly. For example, labour market participation among older people who receive old age pensions can differ from country to country. Continuing to work after pension age may signify financial stress, but for others, it may be a result of high work satisfaction. Thus, labour market participation as an indicator of social exclusion ignores the motivation behind the participation.

By emphasising agency, the notion of social exclusion can be problematised further. For example, a study that took place in rural Northern Finland found that youth narratives contradicted and contested the dominant discourse of social exclusion. They emphasised that people choose to live there and can experience life satisfaction differently. The young people in the study wanted the researchers to recognise that ‘staying in a rural village can

indicate a successful life' (Lanas, Rautio, & Syrjala, 2013, p. 393). Similarly, a growing body of literature on elderly people's relationship to digital technologies has shown that motivation might be one of the most important reasons for little or no use (Dahlberg, 2012; Lüders & Brandtzæg, 2016; 2017; Slettemeås, 2014). Older people may not feel the need to use digital technologies, or they may choose to prioritise other activities. In this view, choosing not to engage with digital technology is not necessarily a sign of social exclusion but may instead be a deliberate choice about how to spend one's life and how to achieve individual wellbeing. Thus, while self-exclusion from opportunities only available through the use of ICTs or proximity to an urban area may lead to some forms of objective material deprivation, they do not necessarily lead to feeling socially excluded. However, as Reneland-Forsman (2018, p. 335) pointed out, the notion of agency is a difficult one from a structural point of view, 'as "choice" is clearly embedded within a social context and expectations that will shape what is often referred to as "choices"'.

4.2.6 Digital divides

During the 1990s, a new dimension of social exclusion began to be discussed; this idea of social exclusion resulted from limited access to ICTs and is referred to as the digital divide. The divide is understood in terms of access to and usage of digital technologies, or a divide between the information poor and information rich (Wresch, 1996). It is an example of social exclusion because 'digital exclusion involves the unequal access and capacity to use … [ICTs] that are seen as essential to fully participate in society' (Hope, Martin & Zubairi, 2016, p. 2). Today, the field has moved

from the exclusively access-based digital divide research to a greater focus on variations in skills and usage (Scheerder, van Deursen, & van Dijk, 2017).

As argued above, there is a clear component of relativity and self-perception in how social exclusion is experienced. This extends to digital exclusion as well; Helsper (2017) therefore adopted a relative deprivation model to digital inequality. She suggested that an individual may be relatively deprived in the objective sense but may not experience subjective (self-perceived) relative deprivation. If a person sees no value in digital technology, does not expect to adopt it in the future and does not have the abilities needed to use it, they might not feel like they are at an unjust disadvantage. This could help to explain why 71% of Norwegian elderly non-users feel that they cope just fine in their everyday lives (Slettemeås, 2014, p. 74).

As with social exclusion, digital exclusion/inclusion is mediated by an individual's economic, cultural and social capital. Selwyn (2004) therefore used the term technological capital, which includes aspects of traditional capital (Bourdieu, 1986) but also highlights their relevance to the digital world. Thus, economic capital includes the 'economic capacity to purchase ICT hardware and software', cultural capital is the 'participation in ICT education and training' and social capital encompasses 'networks of "technological contacts" and support' (Selwyn, 2004, p. 355). The technological capital of an individual influences their digital access on all levels (motivation, access, skills and usage), producing unequal outcomes which have implications for social exclusion (see Figure 1). Digital outcomes that enable participation and enhance capital can facilitate social

inclusion, whereas digital processes which essentially reproduce offline inequalities constrain human opportunity and security.

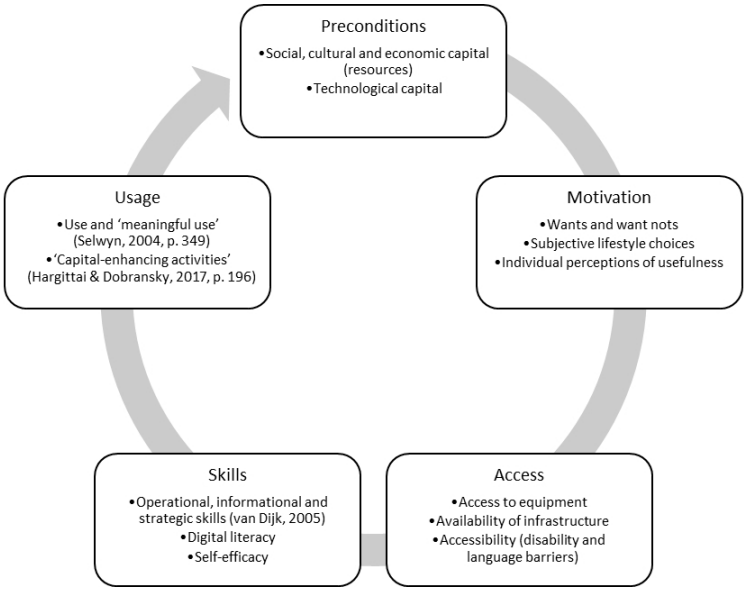

Figure 1. Levels of ICT access and its relationship to offline circumstances (van Dijk, 2005).

4.3 Case study: Elderly in the EHN

4.3.1 Background

The peripheral geographical location of the EHN represents several challenges and the potential for cumulative disadvantages. Its remote location (in comparison to its populated southern centres) and long distances mean that restricted or missing mobility can become a barrier to opportunities in general and to community inclusion specifically (Kenyon, Lyons, & Rafferty, 2002; Kilpeläinen & Seppänen, 2014). As physical

public services are withdrawn, those who cannot or will not engage online are at a greater risk of exclusion (Hodge, Carson, Carson, Newman, & Garrett, 2017; Warren, 2007). Inequality of access in terms of bandwidth, technology and literacy is a persistent problem across the Arctic (Arctic Council, 2016), yet the Nordics are generally high scoring in terms of digitalisation statistics. Moreover, the Norwegian, Swedish and Finnish national and local governments have adopted strategies to improve broadband coverage (Eskelinen, Frank, & Hirvonen, 2008; Norwegian Ministry of Local Government and Modernisation, 2016; Randall, Berlina, Teräs, & Rinne, 2018), but the general trend shows an increasing gap in digital infrastructure quality between commercially profitable (mainly urban) and unprofitable (remote) areas due to the catch-up effect (Salemink, Strijker, & Bosworth, 2017). The issue of poor internet speed is not a problem limited to the EHN, however (Statistics Norway, 2017a). It is therefore important not to overstate infrastructure problems. Yet, as the rural social exclusion literature suggests, rural populations are at a disadvantage because of long distances, sparse populations and lack of proximity to public services. Warren (2007) argued that because of this, the potential benefits of being connected are high in rural areas, as are the disadvantages of non-use. As public services become more difficult to access, internet connectivity (as well as competency) becomes more important for gaining the benefits of the ongoing digitalisation process.

4.3.2 The elderly

Elderly people are considered to be vulnerable to social exclusion and to suffering from multiple disadvantages (van Regenmortel et al., 2016). They

are also thought to be the most vulnerable to digital exclusion because they constitute the majority of non-users and weak users (Slettemeås, 2014). For elderly people facing multiple disadvantages (such as geographical location, mobility issues, poor health, old age and shrinking social networks), the total sum of experienced barriers to societal participation may lead to a higher risk of social exclusion. It is not clear whether digitalisation increases or reduces this risk. On the one hand, it is hoped that digital technologies can lessen the demographic pressures on welfare services as well as reduce the risk of social exclusion, but on the other hand, digitalisation has the potential to create unintended exclusion for weak or non-users.

4.3.3 Digital access

As outlined above, varied access to ICTs can be viewed in terms of different stages, as proposed by van Dijk (2005, p. 22). In Figure 1, we chose to illustrate this as a circle to highlight its effect in terms of producing and reproducing the preconditions for access. This model demonstrates that access consists of motivation, physical accessibility, skills and forms of use. Each form of access has implications for the utilisation of ICTs and is grounded in offline circumstances. This section evaluates the different components of access in order to shed light on the question of what problems elderly people face in their ICT use, from individual motivation and physical access to ICT skills and types of usage. This literature review serves as the theoretical starting point for an empirical investigation of digital divides in the EHN.

4.3.3.1 Motivation

Motivation determines a person's willingness to adopt and use ICTs (van Dijk, 2005, p. 27). Studies have found that many elderly people are simply not interested in using digital tools. For example, Slettemeås (2014, p. 69) reported that a perceived lack of need to use the internet and a lack of interest in it are the two main reasons why elderly Norwegians choose not to use the internet. Furthermore, Dahlberg (2012, p. 14) found that even those who have used digital tools in the past may choose not to in old age because their priorities change and digital participation is no longer seen as important to their lifestyles. Lüders and Brandtzæg (2016, p. 1) also noted a divergence in what they termed 'cultures of communication', reflecting a generational gap wherein online communication is experienced or perceived as less authentic. Some age groups, especially the elderly, might also feel that they are too old to learn how to use a computer (Nøhr, 2006, p. 85). In short, motivation is the first aspect of ICT use and necessarily affects the level of engagement a person has with digital technology.

4.3.3.2 Access

The next step to ICT use is material access. This aspect is closely associated with the traditional digital divide literature, which distinguished between computer and internet haves and have-nots (van Dijk, 2005, p. 45). The internet access gap has to a large extent been closed in the Nordics and other highly developed information societies (see European Commission, 2018), and compared to the rest of Europe, usage rates are higher in the Nordics, even among older people (Dahlberg, 2012, p. 14). While the elderly demographic is less likely to own a computer, gaps are being closed

as new tech-savvy generations begin to age. In 2014, 74% of elderly in Norway reported owning a computer with internet access in their home (Slettemeås, 2014, p. 15). However, geographically, there are some remaining urban-rural gaps in infrastructure, and demographically and socio-economically, some sections of the population are disadvantaged in terms of physical access to digital technologies.

Another dimension of material access is accessibility, by which we mean barriers to use stemming from disability. Users in this category may have the motivation, basic access and skills to use digital technologies but experience exclusion due to material barriers other than those previously mentioned. According to Slettemeås (2014, p. 10), 14% of elderly internet users with a disability feel that their disability hinders them from fully using the internet and digital equipment, and 38% feel they gain extra benefits from using the internet and digital services, showing that when accessible, people benefit from its use. Despite legislation in this area, there is still a lack of awareness about accessibility standards, and a study found that not all commonly used e-health sites, which would be of particular benefit to many groups, are fully accessible (Holthe, 2016, pp. 12–14).

However, access alone does not eliminate the inequality of digital opportunities (Tsatsou, 2011). Digital skills and how people use technology matter. Certain usages are believed to have more benefits than others, reflecting the widely reported ‘rich get richer’ effect (van Dijk, 2005, p. 126).

4.3.3.3 Competency

As more aspects of life are digitalised and more people than ever have access to ICTs, digital skills are becoming necessary for full participation in society. Using the internet has in fact become a critical competency in Norway due to high levels of access and use (Staksrud, 2011). Likewise, in Sweden there has been a 'shift in rhetoric from "access" to citizens' skilful "use" of digital resources' in government agendas (Reneland-Forsman, 2018, p. 336). Digital skills, which can be broadly divided into operational, informational and strategic skills, are therefore an important part of the ICT puzzle (van Dijk, 2005, p. 73).

Some early literature on digital divides adhered to a narrative of digital natives and digital immigrants, in other words, those born in the digital age and those who entered it as adults (Prensky, 2001). This suggests that young people today acquired a high level of digital competency from a young age. There is some truth to this. As Lüders and Brandtzæg (2016, p. 2) noted, using digital media technologies requires a combination of cognitive, sensory and motor skills as well as the knowledge of cultural and social norms and practices that are attached to these technologies. Reported barriers for older people were that computer language is difficult to understand (36%), they are dependent on guidance from others (23%) or they are afraid of making mistakes (22%; Slettemeås, 2014, p. 10).

However, the development of digital skills and literacy is closely related to existing offline skills and capital. In light of this, the digital native/immigrant narrative is not as empirically valid as first thought. For example, a recent study looked at the relationship between age, education

level and digital experience/skills (Fjørtoft, 2017). An interesting finding was that the relationship between age and digital skills was mitigated by education level; among people in the 55–74 age group with a high level of education, there was a larger proportion of people with good digital skills (41%) than adults in the 35–54 age group with lower levels of education (29%). This shows that people who are introduced to ICTs earlier in life do not automatically acquire higher levels of digital skills; rather, their digital competency reflects their overall educational resources. Thus, generational divides alone do not explain the gap between digital natives and immigrants (Helsper & Eynon, 2010). We must therefore avoid the simplification that young people are automatically digitally competent and instead look at the *type* of competency acquired.

Operational skills are basic digital competencies that allow the user to utilise digital equipment. Some researchers have examined the digital skills of elderly people from this perspective. For instance, Karahasanović et al. (2009, p. 662) found that older people feel less comfortable than younger people with tasks such as downloading software to their computers, creating a webpage and programming; however, they found no significant difference in terms of age regarding the use of text editor applications and spreadsheets. Similarly, of respondents in a different survey, 48% claimed to need help from family or friends to buy digital equipment, 68% to install software, 67% to choose settings on their device, 56% to connect digital equipment, 63% to solve technical problems, 45% to download programmes or apps and 50% to update virus protection (Slettemeås, 2014, p. 10).

As society becomes more digitalised, higher levels of technological competence are becoming increasingly important to actualise citizens' rights

and reap the benefits of digitalisation. These informational and strategic skills are a different set of competencies than strictly operational skills. This is not a new problem but rather an issue of traditional information inequality being applied to a new medium, ICTs (van Dijk, 2005). As a result, digital inclusion/exclusion is closely related to users' offline circumstances (Helsper, 2012). Thus, we can hypothesise that some of the apparent skill gaps between the young and elderly may be a result of different skillsets. While children today might have a high level of operational skills from a young age, this should not be mistaken for a higher level informational and strategic competency.

Lastly, digital skills are often thought of as individual attributes. The reality is that users, especially elderly people, rely on their networks of friends and family to navigate the digital world (Rasi & Kilpeläinen, 2015). These so-called proxy users may be family members or caregivers, and they often perform formal online tasks for people who cannot do so themselves (Selwyn, Johnson, Nemorin, & Knight, 2016). Thus, despite computer and internet use being widespread in Norway compared to the EU average, many elderly are dependent upon family and friends to undertake tasks such as buying products online, setting up and installing equipment and software, troubleshooting issues and choosing the right settings (Dahlberg, 2012; Slettemeås, 2014; Statistics Norway, 2017b). This also has implications for the uses of welfare technologies or telecare equipment such as sensors, pendant alarms and GPS tracking devices, as elderly people often rely on their support networks in order to incorporate these technologies in their daily life (Koivunen, 2014). As we have shown, there are different types of

ICT-related skillsets that a person can have or acquire through their social network. These skills affect how a person makes use of digital technologies.

4.3.3.4 ICT Use

Use refers to the type of usage that is made of digital technologies, for instance, whether a person uses simple or advanced applications for entertainment, communication, information and so on (van Dijk, 2005, p. 95). This is closely related to competency, and both are considered second-level digital divides (Scheerder et al., 2017).

Slettemeås (2014, p. 52) found that common reasons among elderly respondents for using the internet were staying updated and informed (73%), using services from home (65%), staying in touch with family and friends (45%), for work (28%) and for entertainment (21%). More recent data show that among Norwegian internet users aged 67 to 79, 67% use e-mail, 6% read a blog, 48% use Facebook, 12% use other social media sites, 51% search for information, 24% look at advertisements, 24% find information about restaurants or events, 48% use online banking, 7% buy tickets for travel, 2% shop online, 13% use public services, 11% use other services and 10% watch television or videos on an average day (Vaage, 2017, pp. 66–67). Elderly people also use digital media to mobilise support and maintain existing relationships (Quan-Haase, Mo, & Wellman, 2017). Some of the positive aspects of technology mentioned by elderly people were its usefulness, convenience and supportiveness, for example, by allowing them to maintain independence and making their lives easier (Mitzner et al., 2010).

The examples above only illustrate the surface of the usage issue because in reality, access does not equate to use and use does not equate to meaningful engagement. This leads to ‘inequalities of outcome’ in the short and long term in terms of social inclusion (Selwyn, 2004, p. 351). A study in the Netherlands found that people with low levels of education used the internet more than those with higher levels of education; however, people with higher educational levels used the internet for more “objectively” beneficial purposes (van Deursen & van Dijk, 2014). Thus, the researchers argued, the internet and how we use it increasingly come to reflect offline inequalities and can potentially contribute to exacerbating exclusion. A more recent study on this connection found that the level of education as well as income can predict the internet skills of elderly people, with higher levels making them more likely to undertake more beneficial (defined as capital-enhancing) activities online (Hargittai & Dobransky, 2017).

The risk, according to Winterberg (2012, p. 27), is that two classes of elderly emerge based on their ability to use computers and the internet. This creates a situation wherein those who have the motivation, access and skills benefit from being able to capitalise on digital opportunities, whereas those who do not are at risk of increased dependence, isolation and lack of access to beneficial information and services. What, then, are the actual outcomes of differentiated access, skills and use? While the divide between first (access) and second (skills and use) levels have received much attention, Scheerder et al. (2017) argued that further research is needed on third-level digital divides (outcomes) and their implications for social inequalities.

4.4 Fieldwork and findings

In order to gather primary data about the consequences of differing motivations, access, skills and use among elderly populations in the EHN, we conducted two fieldwork trips. The first trip was made in May 2018 to Inari and Rovaniemi in northern Finland. A second trip was made to Kirkenes in northern Norway in September 2018. Both field trips involved interviews with key informants in the region who were selected because they represented key digitalisation stakeholders in the areas visited. This included a variety of people (n = 16) working in social and health care, municipal offices and non-governmental organisations, including organisations representing the elderly, indigenous people and people with disabilities. The interviews were qualitative and semi-structured. This allowed for the interviewees to discuss topics important to them in depth while still broadly covering the same range of questions in all the interviews. This was important for analysing the interview data later. The interviews were all transcribed and later coded by theme using an interpretive methodology. In the case of the Norwegian interviews, which were conducted in Norwegian, the interviews were translated after the first round of analysis in order to stay as close to the original meaning as possible. The Finnish interviews were conducted in English with the exception of one, for which an interpreter was present to facilitate the interview.

In the analysis of the interview data from the fieldwork trips, some important themes emerged:

- Respondents resisted the dichotomy of digital natives and immigrants. They pointed out that not all elderly are sceptical of digital technologies and that digital literacy varies among all age groups. Personal interest and engagement matter.
- There was a feeling that digitalisation benefits peripheral areas more than urban centres. It has been described as an equaliser, and respondents referred to a number of examples of how digital technologies have enabled them to live, study and work in the periphery.
- Perceived usefulness was important for participants' decision to adopt a digital technology.
- Lack of infrastructure and poor broadband access were only experienced in certain areas. In most places, respondents were perfectly happy about their internet coverage. However, the remaining unconnected areas will be very expensive to provide access to.
- Accessibility for people with disabilities, especially visual impairments, is still a challenge. Providing services in Sámi languages has also been under-prioritised.
- Respondents confirmed that younger family members are an important resource to elderly people when using digital technologies. Sometimes, this involved buying and setting up equipment. Other times, it required the elderly family members to relinquish control over their finances so that a family member could access online banking in their name. Banks recognise this and will sometimes ask elderly people whether they have a family member who can help them with certain tasks.
- Welfare technologies can enable independence and allow people to live at home for longer. However, not all respondents agreed that this was desirable, and some viewed it as a reflection of the underfunding of welfare services. A related concern was less

physical contact in health and social care as a result of digitalisation.

- Respondents made distinctions between types of use. For example, they pointed out that many elderly people use social media sites such as Facebook but have not learned how to use online banking and struggle to access their municipality's online services.

4.5 Conclusion

By elucidating the relationship between the concepts of cybersecurity, human security and social exclusion, we have highlighted how social exclusion can be incorporated into a broader conception of human cybersecurity. This conceptualisation allows us to analyse the enabling and constraining aspects of digitalisation and digital technologies at the individual and community levels in terms of security of freedom from fear and want. Through our review of the literature, we showed how, in addition to referring to more than material deprivation, social exclusion is a highly normative and relative concept. As such, there is a high degree of self-perception involved in how social exclusion is experienced. This is also the case for digital forms of exclusion. By exploring access to digital technologies through van Dijk's (2005) multi-level framework, we illustrated how access – from motivation and physical access to digital competency and beneficial use – is mediated by an individual's technological capital (Selwyn, 2004). This alerts us to how certain digital outcomes can facilitate social inclusion, while other processes contribute to reproducing offline inequalities, thereby constraining human opportunity and security.

The elderly provide a pertinent case study of digitalisation in the EHN because they are seen as a group that is particularly vulnerable to exclusion. Together with the disadvantages associated with the peripheral geography of the EHN, there is a concern that weak and non-ICT users, who are often elderly, may not be able to make use of the opportunities provided by digital services. As such, there is simultaneously a hope that digital technologies can provide new and effective solutions and a concern that digitalisation may create exclusion where it otherwise would not exist.

Our findings point in this direction. Firstly, there is a recognition that digitalisation highly benefits peripheral areas such as the EHN. Some participants described the internet as an equaliser and gave examples of how digital technologies enable people to live, study and work in the EHN, reflecting the broader literature on digitalisation in rural areas (Warren, 2007). This, however, presupposes that everyone wants, can access and is able to use ICTs to the extent that is demanded by the public and private sector.

Secondly, interviewees made distinctions between different types of ICT use, which have also been noted in the literature (Hargittai & Dobransky, 2017; Selwyn, 2004). For example, many elderly competently use social media platforms like Facebook but struggle to use services that are perceived to be more complex or risky, such as online banking and municipal online services. This may indicate that certain groups are excluded from what some consider the most beneficial uses of ICTs, instead having to pay user fees or travel long distances to continue using non-digital alternatives.

Thirdly, younger family members (along with competent spouses and trusted friends) are an important resource for many elderly people when using digital technologies. Sometimes, this involves the more experienced family member buying and setting up equipment. Other times, it requires elderly individuals to relinquish control over their own finances so that a family member can access online banking in their name. Having family members act as proxy users is not an uncommon practice (Selwyn et al., 2016).

Lastly, we found that universal design requires further improvement regarding the accessibility of digital services, especially for people with visual impairments. The broader literature shows that despite legislation in this area, there is still a lack of awareness about accessibility standards (Holthe, 2016). Another barrier to use is that providing services in Sámi languages is often not prioritised. Our interviews revealed that under some circumstances, these barriers can lead to compound disadvantages. To conclude, our findings show that while digitalisation provides new solutions and opportunities that are crucial for areas like the EHN and are largely welcomed, the benefits of these developments will be unevenly distributed if its limitations are not taken into account.

References

Alkire, S. (2003). *A conceptual framework for human security* (CRISE Working Paper No. 2). Retrieved from Oxford University Research Archive website: https://ora.ox.ac.uk/objects/uuid:d2907237-2a9f-4ce5-a403-a6254020052d/download_file?file_format=application/pdf&safe_filename=workingpaper2.pdf&type_of_work=Working%20paper

Arctic Council. (2016). *Arctic resilience report*. M. Carson & G. Peterson (Eds.). Retrieved from Stockholm Environment Institute website: https://www.sei-international.org/mediamanager/documents/Publications/ArcticResilienceReport-2016.pdf

Barnett, J. (2001). *The meaning of environmental security: Ecological politics and policy in the new security era*. London, United Kingdom: Zed Books.

Booth, K. (2005). Introduction to part one. In K. Booth (Ed.), *Critical security studies and world politics* (pp. 21-25). London, United Kingdom: Lynne Rienner.

Booth, K. (2007). *Theory of world security*. Cambridge, United Kingdom: Cambridge University Press.

Bourdieu, P. (1986). The forms of capital. In J. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241–258). Westport, CT: Greenwood.

Burchardt, T., Le Grand, J., & Piachaud, D. (2002). Introduction. In J. Hills, J. Le Grand, & D. Piachaud (Eds.), *Understanding social exclusion* (pp. 1-12). Oxford, United Kingdom: Oxford University Press.

Buzan, B. (1991). *People, states and fear: An agenda for security analysis in the post-Cold War era* (2nd ed.). Boulder, CO: Lynne Rienner.

Buzan, B., Waever, O., De Wilde, J. (1998). *Security: A new framework for analysis*. Boulder, CO: Lynne Rienner.

Byrne, D. (1999). *Social exclusion*. Buckingham, United Kingdom: Open University Press.

Commission on Human Security. (2003). *Human security now*. Retrieved from ReflefWeb website:

https://reliefweb.int/sites/reliefweb.int/files/resources/91BAEEDBA50C6907C1256D19006A9353-chs-security-may03.pdf

Dahlberg, Å. (2012). Användning av IT-baserade tjänster i de nordiska länderna [Use of IT based services in the Nordic countries]. In Göransson, E.P. *Fokus på eldre i informasjonssamfunnet* [Focus on the elderly in information society]. (pp. 12–24). Retrieved from: http://www.diva-portal.org/smash/get/diva2:706911/FULLTEXT01.pdf

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20, 701–715.

Eskelinen, H., Frank, T., & Hirvonen, T. (2008). Does strategy matter? A comparison of broadband rollout policies in Finland and Sweden. *Telecommunications Policy*, 32, 412–421.

European Commission. (2018). *Connectivity: Broadband market developments in the EU*. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52245

Fjørtoft, T. O. (2017, June 6). Digitale ferdigheter i ulike aldersgrupper: Unge og høyt utdannede er flinkest foran PC-en [Digital skills in different age groups: The young and highly educated are best in front oft he PC]. *Statistics Norway*. Retrieved from http://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/unge-og-hoyt-utdannede-er-flinkest-foran-pc-en

Hargittai, E., & Dobransky, K. (2017). Old dogs, new clicks: Digital inequality in internet skills and uses among older adults. *Canadian Journal of Communication*, 42, 195–212.

Helsper, E. J. (2012). A corresponding fields model for the links between social and digital exclusion. *Communication Theory*, 22, 403–426.

Helsper, E. J. (2017). The social relativity of digital exclusion: Applying relative deprivation theory to digital inequalities. *Communication Theory*, 27, 223–242.

Helsper, E. J., & Eynon, R. (2010). Digital natives: Where is the evidence? *British Educational Research Journal*, 36, 503–520.

Hodge, H., Carson, D., Carson, D., Newman, L., & Garrett, J. (2017). Using internet technologies in rural communities to access services: The views of older people and service providers. *Journal of Rural Studies*, 54, 469–478.

Holland, J., & Jarvis, L. (2015). *Security: A critical introduction*. London, United Kingdom: Palgrave.

Holthe H. (2016). *Nettbaserte helsetjenester for alle. Hvordan utvikle og implementere allment tilgjengelige e-helsetjenester i Norge* [Online health services for all. How to develop and implement publicly available e-health services in Norway] (Project Report No. 3). Retrieved from Nasjonalt senter for e-helseforskning website: https://ehealthresearch.no/files/documents/Prosjektrapporter/NSE-rapport_2016-03_Nettbaserte_helsetjenester_for_alle.pdf

Hope, S., Martin, C. and Zubairi, S. S. (2016). *The role of digital exclusion in social exclusion*. (Ipsos MORI Scotland & Carnegie UK Trust report). Retrieved from: https://d1ssu070pg2v9i.cloudfront.net/pex/carnegie_uk_trust/2016/09/LOW-2697-CUKT-Digital-Participation-Report-REVISE.pdf

Karahasanović, A., Brandtzæg, P. B., Heim, J., Lüders, M., Vermeir, L., Pierson, J.,…Jans, G. (2009). Co-creation and user-generated content – Elderly people's user requirements. *Computers in Human Behavior*, 25, 655–678.

Kenyon, S., Lyons, G., & Rafferty, J. (2002). Transport and social exclusion: Investigating the possibility of promoting inclusion through virtual mobility. *Journal of Transport Geography*, 10, 207–219.

Kilpeläinen, A., & Seppänen, M. (2014). Information technology and everyday life in ageing rural villages. *Journal of Rural Studies*, 33, 1–8.

Koivunen, E. (2014). *Telecare and older people's social relations* (Working Paper No. 3). Retrieved from AKTIVE website: http://www.aktive.org.uk/downloads/AKTIVE_Paper-3.pdf

Lanas, M., Rautio, P., & Syrjala, L. (2013). Beyond educating the marginals: Recognizing life in northern rural Finland. *Scandinavian Journal of Educational Research*, 57, 385–399. https://doi.org/10.1080/00313831.2012.656283

Levitas, R., Pantazis, C., Fahmy, E., Gordon, D., Lloyd, E., & Patsios, D. (2007). The multi-dimensional analysis of social exclusion. Retrieved from IOE *Digital Education Resource Archive website*: https://dera.ioe.ac.uk/6853/1/multidimensional.pdf

Lüders, M., & Brandtzæg, P. B. (2016). Når alt sosialt blir flyktig: En kvalitativ studie av hvordan eldre opplever sosiale medier [When everything social becomes fleeting: A qualitative study of how older people experience social media]. *Norsk Medietidsskrift*, 23(2), 1–18.

Lüders, M., & Brandtzæg, P. B. (2017). 'My children tell me it's so simple': A mixed-methods approach to understand older non-users' perceptions of social networking sites. *New Media & Society*, 19, 181–198.

McSweeney, B. (1999). *Security, identity and interests: A sociology of international relations*. Cambridge, United Kingdom: Cambridge University Press.

Mearsheimer, J. (2001). *The tragedy of great power politics*. New York, NY: Norton.

Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J. … Sharit, J. (2010). Older adults talk technology: Technology usage and attitudes. *Computers in Human Behavior*, 26, 1710–1721.

Morgenthau, H. (1973). *Politics among nations: The struggle for power and peace* (5th ed.). New York, NY: Knopf.

Nøhr, Ø. N. (2006). De kompetente eldre: Aldring og digital kompetanse – konflikt eller lykke? [The competent elderly: Ageing and digital competence – conflict or happiness?] (Research Report No. 128). Retrieved from Brage Open Knowledge Archive website: https://brage.bibsys.no/xmlui/handle/11250/144887

Noll, H. H. (2002). Towards a European system of social indicators: Theoretical framework and system architecture. *Social Indicators Research*, 58, 47–87.

Norwegian Ministry of Local Government and Modernisation. (2016). *Digital agenda for Norway in brief: ICT for a simpler everyday life and increased productivity*. (Report to the Storting No. 27). Retrieved from https://www.regjeringen.no/contentassets/07b212c03fee4d0a94234b101c5b8ef0/en-gb/pdfs/digital_agenda_for_norway_in_brief.Pdf

Prensky, M. (2001). Digital natives, digital immigrants part 1. *On the Horizon*, 9(5), 1–6.

Quan-Haase, A., Mo, G. Y. and Wellman, B. (2017). Connected seniors: how older adults in East York exchange social support online and offline. Information, *Communication & Society*, 20(7), 967–983.

Randall, L., Berlina, A., Teräs, J., & Rinne, T. (2018). *Digitalisation as a tool for sustainable Nordic regional development: Preliminary literature and policy review*. Retrieved from Nordregio website: http://www.nordregio.org/wp-content/uploads/2018/03/Digitalisation_Discussion-Paper_Jan-31.pdf

Rasi, P., & Kilpeläinen, A. (2015). The digital competences and agency of older people living in rural villages in Finnish Lapland. *Seminar.net: International Journal of Media, Technology and Lifelong Learning*, 11, 149–160.

Reneland-Forsman, L. (2018). 'Borrowed access' – The struggle of older persons for digital participation. International *Journal of Lifelong Education*, 37, 333ç344.

Salemink, K., Strijker, D., & Bosworth, G. (2017). Rural development in the digital age: A systematic literature review on unequal ICT availability, adoption, and use in rural areas. *Journal of Rural Studies*, 54, 360–371.

Scheerder, A., van Deursen, A., & van Dijk, J. (2017). Determinants of internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. *Telematics and Informatics*, 34, 1607–1624.

Selwyn, N. (2004). Reconsidering political and popular understandings of the digital divide. *New Media & Society*, 6, 341–362.

Selwyn, N., Johnson, N., Nemorin, S., & Knight, E. (2016). *Going online on behalf of others: An investigation of 'proxy' internet consumers*. N. Clark (Ed.). Sydney, Australia: Australian Communications Consumer Action Network.

Sen, A. (1999). *Development as freedom*. Oxford, United Kingdom: Oxford University Press.

Sheehan, M. (2005). *International security: An analytical survey*. Boulder, CO: Lynne Rienner Publishers.

Slettemeås, D. (2014). *Eldres bruk av digitale verktøy og internett: En landsdekkende undersøkelse av mestring, støttebehov, motivasjon og hindringer [The elderly's use of digital tools and the internet: A country wide examination of mastery, need for support, motivation*

and barriers] (Report No. 5). Retrieved from the Norwegian Directorate for Children, Youth and Family Affairs website: https://bufdir.no/globalassets/global/slettemeas_2014_eldres_bruk_av_digitale_verktoy_og_internett.pdf

Sokoloff, C., & Lewis, R. (2005). *Denial of citizenship: A challenge to human security*. (Issue Paper No. 28). Retrieved from European Policy Centre website: http://www.epc.eu/documents/uploads/724318296_EPC%20Issue%20Paper%2028%20Denial%20of%20Citizenship.pdf

Staksrud, E. (2011). Norske barn på Internett: Høy risiko - liten skade? [Norwegian children on the internet: High risk – low harm?] *Nordicom Information*, 33(4), 59–70.

Statistics Norway. (2017a). Internett-målinga 20. november 2017 [The internet measurement 20. November 2017]. Retrieved from https://www.ssb.no/inet

Statistics Norway. (2017b). Ni av ti surfer på nettet hver dag. [Nine out of ten surf the web every day.] Retrieved from http://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/ni-av-ti-surfer-pa-nettet-hver-dag

Tsatsou, P. (2011). Digital divides revisited: What is new about divides and their research? *Media, Culture & Society*, 33, 317–331.

United Nations Development Program. (1994). *Human development report*. Retrieved from http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

Vaage, O. F. (2017). Norsk Mediebarometer 2016 [Norwegian Media Barometer 2016]. (Statistics Norway report). Retrieved from http://www.ssb.no/kultur-og-fritid/artikler-og-publikasjoner/_attachment/303444?_ts=15c1173e920

van Deursen, A., & van Dijk, J. (2014). The digital divide shifts to differences in usage. *New Media & Society*, 16, 507–526.

van Dijk J. (2005). *The Deepening Divide: Inequality in the Information Society*. London: Sage Publications.

van Regenmortel, S., de Donder, L., Dury, A., Smetcoren, A., de Witte, N., & Verté, D. (2016). Social exclusion in later life: A systematic review of the literature. *Population Ageing*, 9, 315–344.

Waltz, K. N. (1979). *Theory of international politics*. New York, NY: Random House.

Warren, M. (2007). The digital vicious cycle: Links between social disadvantage and digital exclusion in rural areas. *Telecommunications Policy*, 31, 374–388.

Winterberg, E. (2012). Et digitalt A- og B-hold? [A digital A and B team?] In Göransson, E.P. *Fokus på eldre i informasjonssamfunnet [Focus on the elderly in information society]*, (p. 27). Retrieved from http://www.diva-portal.org/smash/get/diva2:706911/FULLTEXT01.pdf

Wresch, W. (1996). *Disconnected: Haves and have-nots in the information age*. New Brunswick, NJ: Rutgers University Press.

Wyn Jones, R. (2007). Message in a bottle? Theory and praxis in critical security studies. In B. Buzan & L. Hansen (Eds.), *International security* (pp. 299–319). Los Angeles: SAGE Publications.

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

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

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

b) Department of Social Sciences, Michigan Technological University

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

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

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

Executive Summary

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

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

5.1 Introduction

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

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

5.2 Core guiding questions and responses

This chapter examines four core guiding questions:

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

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

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

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

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

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

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

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

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

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

5.3 Conceptualising and governing the linkage between environmental governance and cybersecurity

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

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

5.3.1 Concept of ECICs and the law in the EHN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In the EHN region, the procurement of natural resources is being increasingly managed through cyber control. Outlining the identification of a possible regulatory framework for this technology is important not only in terms of national legislation but also in view of this local, regional and international network.

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

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

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

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

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

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

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

5.4 Conclusion

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tsagourias, N., & Buchan, R. (2016). Cyber-threats and international law. In E. M. Footer, J. Schimt, D. N. White, & D. L. Bright (Eds.), *Security and international law*. Oxford.

Van Eeten M. (2011). The state and the threat of cascading infrastructures across critical infrastructures: The implications of empirical evidence from media incident reports. *Public Administration*, 89(2).

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

6 Conclusions

Gerald Zojer

Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland

Digitalisation is rapidly changing our societies, and the relatively peripheral areas of northernmost Finland, Norway and Sweden – the European High North (EHN) – have likewise been affected. This region is the homeland of the Sámi, an Indigenous people with several languages. For the EHN – which is sparsely populated, has a less developed infrastructure (health services, information and communication technologies [ICTs], etc.) than in the more southern parts of these countries and which is characterised by a harsh climate – digitalisation offers numerous benefits. As a result of the digitalisation policies of the EHN countries, digitalisation is already relatively advanced. The motif for advancing digital technologies and ICTs is to increase efficiency of existing services and activities and to promote (new) business opportunities. However, digitalisation also creates new challenges to people's everyday lives. While some of the enabling and constraining effects of digitalisation are similar to those in other regions, the peculiarities of the EHN also lead to a distinct set of opportunities and challenges.

For instance, digitalisation of public services can reduce time and resources spent on travel by making services available in remote places. However, this is often accompanied by cutbacks to physical services. Digitalisation can

allow people to live, study and work in peripheral areas such as the EHN. However, not everyone wants, can access or is able to use ICTs as required in order benefit from digital (public) services. Thus, digitalisation may create new insecurities or exclusion for some people. ICTs and cyberspace also affect citizens and civil society organisations. The adoption of these technologies has led to instrumental changes in how non-governmental and non-profit organisations operate. Yet, the emergence of cyberspace has both enhancing and constraining effects, and the use of cyberspace has not profoundly altered the terms of the relative power of one type of civil society over another. In other words, digitalisation neither democratises nor undemocratises societies. Digital technologies not only play an ever-increasing role in public administration and personal life, but other core infrastructures also depend heavily on ICTs, such as water or energy supply. The EHN climatic conditions as well as human-induced climate change pose risks to these infrastructures and cybersecurity. Uninterrupted operation of these infrastructures is necessary for human wellbeing.

Digitalisation in the EHN states has been pushed by national and regional policies, and the rapid adoption of digital technologies and ICTs has made societies more dependent on the uninterrupted supply of these services. However, ICTs are vulnerable, and their operation is challenged by connectivity problems, technical malfunctions, human abuse and error as well as hostile interests. Consequently, information security and cybersecurity frameworks have been established in order to address these challenges. When the ICT infrastructure of an entire state is challenged, the question of security is shifted to the national level. The countries of the EHN have endorsed cybersecurity strategies to address such threats. Their

aim is to protect critical infrastructure from adverse events. Indeed, the reliability of these infrastructures has become important for the functioning of contemporary societies. However, in the end these technologies should serve a prospering development of humankind. Thus, the aim of cybersecurity must first be to safeguard human wellbeing in a digitalising world. Mainstream cybersecurity approaches, however, fail to address the negative impacts of digitalisation, as these approaches are somewhat techno-determinist, assuming that digital technologies benefit society and that safeguarding their functioning automatically serves societal wellbeing. However, such an understanding fails to acknowledge that digitalisation contains both enabling and constraining effects. Mainstream cybersecurity understanding falls short of addressing challenges and threats that people experience in their everyday lives and that originate from the dispersion of digital technologies. Therefore, cybersecurity needs to be conceptualised in a more comprehensive manner that includes the societal impacts of cyberspace, ICTs and digitalisation and that also considers its effects at the individual and sub-state community levels.

The results of the ***E****nablement besides* ***Co****nstraints:* ***Hu****man Security and a* ***Cy****ber Multi-Disciplinary Framework in the European High North* (ECoHuCy) research project, which are summarised in this synthesis report, show that integrating a human security approach can be inclusive to traditional cybersecurity concerns and the everyday life experiences of people in their region-specific context. This human-centred cybersecurity approach shifts the human into the focus of security concerns and considers both the enabling and constraining effects of digitalisation. This comprehensive cybersecurity framework can be applied as a tool in order to

create meaningful and targeted policies that address both the positive and negative impacts of digitalisation while at the same time having the flexibility to consider regional peculiarities.

This book presents the synthesis of a three-year research project Enablement besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North (ECoHuCy). The aim of the project was to design a multidisciplinary research framework to address human security questions related to digitalisation and the increasing importance of cybersecurity.

In this book we introduce a research agenda suited for the purposes of policy makers, regulators and academia alike, which also gives the citizens and communities of the European High North a say in matters related to digitalisation and cybersecurity. It questions the mainstream conceptualisation of cybersecurity and reconstructs this concept with the human being as the referent object of security. By utilising the human security concept, the project establishes a human-centred cybersecurity framework.

ISBN 978-952-337-182-8