Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change

Klein, Joëlle; Hossain, Kamrul

Published in:
ARCTIC REVIEW ON LAW AND POLITICS

DOI:
10.23865/arctic.v11.1936

Published: 11.02.2020

Document Version
Version created as part of publication process; publisher's layout; not normally made publicly available

Citation for pulished version (APA):
Klein, J., & Hossain, K. (2020). Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change. *ARCTIC REVIEW ON LAW AND POLITICS*, *11*, 1-18. https://doi.org/10.23865/arctic.v11.1936

Arctic Review on Law and Politics
Vol. 11, 2020, pp. 1–18

Peer-reviewed article

Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change

Joëlle Klein & Kamrul Hossain*
Northern Institute for Environmental and Minority Law,
Arctic Centre, University of Lapland

Abstract
The following article revisits existing scholarship on human-centric approaches to security in cyberspace and argues that a holistic understanding of cyber security in the Arctic must include discussion of the use of cyber technology in the everyday lives of individuals and communities, addressing both the ways such tools enable and undermine human security. Simultaneously, the article contextualises the Arctic as a region undergoing rapid change as a result of climate change and increased digitalisation and seeks to understand the consequent implications for human security. In light of these considerations, the article analyses the existing constraints and possibilities that cyber security and digitalisation pose for human security and revisits them from a human-centric perspective of cyber security. It also seeks to contextualise such security influences in relation to the role of climate change and its influence on the region. Finally, several examples are discussed to underline the interdependent implications of digitalisation and climate change from a human-centric perspective of cyber security in the Arctic.

Keywords: *cyber security; digitalisation; human security; Arctic; climate change*

Responsible Editor: Nigel Bankes, University of Calgary, Canada

Received: October 2019; Accepted: January 2020; Published: February 2020

1. Introduction

In the last several decades, the use and spread of cyber technology, an inclusive system of information and communication technology, has rapidly increased across the globe. With it, discourse on cyber security is increasingly prevalent on the national and international levels. As the new frontier of cyberspace develops, efforts to regulate

*Correspondence to: Kamrul Hossain, email: khossain@ulapland.fi

Citation: Joëlle Klein & Kamrul Hossain. "Conceptualising Human-centric Cyber Security in the Arctic in Light of Digitalisation and Climate Change" Arctic Review on Law and Politics, Vol. 11, 2020, pp. 1–18.
http://dx.doi.org/10.23865/arctic.v11.1936

and protect privacy and data seek to balance with the need for open and fair use. States have begun to adopt cyber security strategies to protect their interests and securitise the cyber arena from threats leveraged by malicious actors. However, within these strategies, the technicality of cyberspace is not discussed in relation to the negative (threats) and positive (enablement) aspects of security[1] that technologies and cyberspace provide for individuals and communities *within* states. Government- and state-based understandings of cyber security are often limited to national security interests that place the state as the referent object vulnerable to the insecurity of cyber infrastructure or frameworks. The threat of hacking, or cyber influence, and control and ownership over information and intelligence is often the first imagined threat in relation to cyber security. This places the state, its infrastructure and its institutions at the centre of such threats but fails to consider the impact of cyber security on people at the individual level and their communities. National security agendas surrounding cyber security often do not conceptualise the human impact of such threats as the predominant referent of security but rather dominant institutional frameworks. Likewise, considerations of cyber security often neglect the abilities of cyber technology to enable individuals and communities to achieve security.

Cyber technology and digital tools are increasingly replacing existing physical tools, and information, services and data are migrating into the digital sphere under the current trend of digitalisation. Therefore, the state of cyber security determines how digital transformation occurs. Digitalisation has changed the medium and function of everyday societal interactions and has influenced how individuals and communities relate to each other and themselves. Cyberspace has become "cyber-physical" in the sense that everyday interactions (communications, shopping, finances, education, etc.) have become inextricably linked to the cyber world, and public goods and services are increasingly dependent on the use of online and digital technology.[2] Facebook, Instagram, Twitter and Snapchat are prime examples of how individuals present themselves and share information online. Alongside the information individuals choose to share, companies and firms are interested in the inherent data individuals create simply by entering an online space – subtle information about an individual's location, preferences, activity and usage. Human rights in cyberspace are becoming increasingly relevant and important, yet scholars[3] note that individual and community security concerns and their variance across regions and contexts are often not discussed or are inadequately reflected in cyber security research.

Ongoing discourse on cyber security contextualised in various regions is thus problematic, not only because of the state-based assumptions and preconceptions underlying our understanding of cyber security, but also in understanding the nuanced ways in which cyber security impacts local communities and individuals. This is particularly true when it comes to discourse on the Arctic. Although the region is often discussed as homogenous, it is actually a complex and intersecting network of different cultural, societal, political and geophysical realities. There are, of course, many similarities between various Arctic states in terms of cold climactic

conditions, the presence of indigenous peoples, the legacy of colonialism, dichotomies between rural and remote communities, and the shared regional governance forum of the Arctic Council.[4] However, it is important to remember that, despite shared similarities, the reality is that individuals and communities are prone great variation across the Arctic. This is also true for cyber security and digitalisation. In discussing both the Arctic and digitalisation in tandem, cyber security becomes an inherently important discussion based on the particularities presented by both.

As such, the regional and local contexts of individuals and communities become important factors in determining the roles of technology and individual relationships in cyberspace. In particular, individuals' access to cyber technologies and connectivity are dependent on their locations and surrounding circumstances. In the Arctic, people's access to the internet and cyber technology vary depending on their location and the local geography. Communities located in the northernmost regions of Finland, Sweden and Norway – also referred to as the European High North (EHN) – have fairly good connectivity and access to digital services and cyber technologies, whereas the more remote, rural areas of Russia, Canada and Alaska may face more significant difficulties in accessing information and communication technologies (ICTs) and sustaining reliable connectivity.[5] In addition, Arctic communities face rapid, visible and significant impacts as a result of climate change, resulting in a shared narrative between communities and environmental justice advocates in the region. A large portion of this activism has been conducted online and popularised through social media and online communication tools. Moreover, the impacts of climate change in the Arctic may disproportionately affect digitally operated physical infrastructures, so-called "critical infrastructures," (CI) due to, for example, unexpected, unpredictable extreme conditions that prevail in the Arctic as a result of climate change. Any disruption or malfunctioning of such infrastructures would harm communities in the region. For this reason, the Arctic serves as a diverse context in which to consider the varying human security aspects linked to cyber security and climate change. The concept of human security offers an opportunity to re-centralise individuals and their communities into existing discourses in the cyber security framework. By considering cyber security through the lens of human security, the analysis shifts to a focus on both the threats and the opportunities that cyber technology affords for the security of individuals and communities. In doing so, it opens discussion on how the cybersecurity framework may both exacerbate the vulnerabilities and threats posed by climate change and increase opportunities to enable resilience of individuals and communities in the Arctic.

2. The cybersecurity framework in the context of Arctic climate change

A "cybersecurity framework" refers to a system of standards, guidelines and practices that protect and fortify information systems, networks and supporting infrastructures from unauthorised access and in critical conditions. Analyses of cybersecurity frameworks include digital infrastructures, thereby creating a connection with

cybersecurity, given that the smooth functioning of digital infrastructures is heavily dependent on the security of cyberspace. At first glance, it may seem unpersuasive to establish a link between cybersecurity and climate change; however, climate change in the Arctic can affect, for example, digitally operated physical infrastructures with the high possibility of critically disrupting their systems, affecting various dimensions of human security. To offer an understanding of human-centric cybersecurity (as discussed in part 3), this section refers to an interconnection between climate change in the Arctic and the cybersecurity framework. While part 4 elaborates on this link with concrete examples, the following discussion presents a brief introduction to the challenges and opportunities illuminated by their interconnection with reference to the Arctic.

The Arctic region can be defined differently depending on its geographic, political and bio-ecological characteristics. Politically speaking, the Arctic can be defined in international terms as the eight Arctic states comprising the Arctic Council: Finland, Norway, Sweden, Russia, Canada, the United States, Iceland and Greenland (via Denmark). A more nuanced political delineation would include further definition as the northernmost regions of several of these states. The Arctic is a geographically large region, home to diverse cultures and abundant ecosystems. It is also home to over four million people, with the northernmost areas of the region characterised by mostly rural, sparsely populated centres.[6] One defining characteristic of the Arctic is its history of colonialism, as it is the ancestral home of diverse indigenous peoples in all its constituent countries except Iceland. Nature-based livelihoods and traditional economies are vitally important to the region. Over the years, discussions on the Arctic have increasingly mentioned climate change because of its impending and current impacts, which are only accelerating.[7] The Arctic Council's Arctic Monitoring and Assessment Program (AMAP) underscores the significance of climate change in driving geographic and ecosystem changes to the permafrost, sea ice cover and duration, and glacier thickness. Accelerated positive feedback loops related to climate change also drive impacts on terrestrial vegetation, coastal erosion, freshwater balance and marine productivity.[8] According to the Arctic Climate Impact Assessment (ACIA), shifting vegetation zones, changes in animal species diversity and distribution, increased storms, the thawing of the permafrost, easy access to the region because of sea ice melt, and ultra-violet radiation all produce adverse consequences for Arctic populations.[9] The most recent Intergovernmental Panel on Climate Change (IPCC) report on the impact of global warming of 1.5 °C identifies the Arctic ecosystem as a region facing a "disproportionately higher risk of adverse consequences."[10] Environmental security concerns are therefore crucial in the Arctic, a region where several human security concerns intersect, such as climate change, natural resource extraction, and changes in socio-cultural and demographic dynamics as well as changes in the diverse economic interests of various actors, including local and indigenous populations.[11]

New economic activities, such as resource extraction, infrastructure development and tourism across the Arctic region, lead to changes in environments, economies

and societies,[12] all of which are increasingly integrated with the cybersecurity framework and where different interest groups emerge and interact both positively and negatively.[13] The human and community impacts of such developments are likely to cause both immediate and long-term effects that will change existing cultures, livelihoods and relationships with the planet. In this way, human security in the Arctic is intimately related to climate change. The indigenous populations of the Arctic are most vulnerable to these sorts of changes,[14] which often deprive them of sources of sustenance as well as political participation. However, the integration of new lifestyles and cultures driven by both demographic changes and technological advancements has brought both negative and positive incentives for the populations of the region.

Climate change compounds some of the Arctic's unique characteristics: volatile conditions, harsh environments, exposure to unpredictable natural disasters, long winters, sparse populations, outmigration and vast distances between human settlements.[15] Given these special characteristics and the ongoing societal transformations the region faces, the functioning of Arctic society has become gradually dependent on digital infrastructures, which replace, for example, traditional physical infrastructures. Online platforms become the media through which people perform their everyday activities, their day-to-day interactions and communications, and even their livelihoods.[16] Perhaps more importantly, public services such as education, health care and financial services are increasingly administered on online platforms. While this transformation has been taking place all over the world, the uniqueness of the Arctic lies in its special characteristics, which offer both challenges and opportunities to its people as they digitise.

These challenges do not only arise from cyber-attacks on digital infrastructure; they can also arise from climate change–induced natural catastrophes. For example, natural disasters may disrupt communication networks and thus halt digital services, such as health care, education, everyday financing, etc. Moreover, critical infrastructures, such as energy supply, run through digital infrastructure; disrupting these would cause drastic human suffering. The stable functioning of these systems requires resilient infrastructures. However, in the Arctic, such infrastructure is not adequately resilient because of uncertainties posed by climate change. Even in case of a breakdown of existing infrastructures due to, for example, climate change–induced threats, replacing or fixing them under Arctic conditions is extremely difficult because of its remoteness, poor physical infrastructure and fragile infrastructure support systems. Even when repairs are possible, they involve high costs and longer periods of time. Such disruptions clearly cause human suffering that amount to human security threats.[17]

On the other hand, the stable functioning of digital infrastructures in the Arctic would promote human security, as it would enable people to access services such as education, health care and others that are delivered through digital platforms, thereby promoting greater social inclusion.[18] Additionally, as services are replaced

by digital infrastructures, people would need to travel less,[19] since services would be attainable through well-connected internet networks. Less travelling means less use of motorised vehicles and consequently decreased greenhouse gas emissions and greater efficiency of climate change mitigation, which would advance greater environmental sustainability in the Arctic by realising a number of human security issues.

3. Human security as it applies to the cybersecurity framework

This section introduces the concept of human security and contextualises its application regarding cyber security and increased digitalisation. It builds on the previous section to elaborate on the current discourse around cyber security and the need to reconceptualise the security dialogue generally. It also discusses the inclusion of the cybersecurity framework as an emerging avenue for discussion within the human security paradigm.

In traditional conceptions of security, the referent object has been the state and its interests – essentially, national security. However, this fails to consider internal security or the well-being of individuals and communities as objects of security. Alongside this dominant discourse, the concept of human security was developed to re-focus the object of security away from the state and onto individuals and their communities. The notion of "human security" was popularised within the framework of the United Nations (UN) Development Programme in 1994 and based on achieving "freedom from fear" and "freedom from want."[20] The concept now also includes the "freedom to live in dignity."[21] In order to do so, human security proposes a bottom-up approach to understanding well-being as security centred on individuals and their communities as sites of freedom from fear, want, indignity and vulnerability. Human security re-centralises the referent object of security away from the state to individuals and their communities, and in doing so, it requires a more nuanced view of threats and opportunities for societal well-being that transcends the concept of "threats" as viewed through a national security paradigm. The function of human security, as stated in the UN General Assembly resolution 66/290, "is an approach to assist Member States in identifying and addressing widespread and cross-cutting challenges to the survival, livelihood and dignity of their people."[22] At its foundation, the concept promotes "people-centred, comprehensive, context-specific and prevention-oriented responses that strengthen the protection and empowerment of all people."[23] Furthermore, the concept has been expanded to encompass not only threats to individuals and their communities (survival) but also to promote security as a means of enabling individuals and their communities (survival plus).[24] In this way, human security deals both with the constraints that particular threats place on communities and individuals as well as opportunities for them to enable their own resilience and well-being. In this sense, human security can also be described as including positive and negative security elements that both protect well-being and promote its development at the level of communities and individuals.[25]

In addition, human security relies on an understanding of security that is disaggregated by interrelated, dependent features, as elaborated in the UN Human Development Report in 1994, including health, food and communal, personal, environmental, economic and political security. These features are non-exhaustive, and the concept is adaptable to suit emerging security concerns and societal changes. At the core of human security lies human well-being through the reinforcement of human rights and development. To that degree, threats related to civil safety (such as emergency and disaster preparedness) are also integral to the concept of human security.[26] The continuous functioning of critical infrastructures on which individuals and communities rely for daily existence also remains relevant. Given the broad conceptualisation of human security as a means to promote well-being by addressing issues that affect individuals and communities in their everyday lives in both positive and negative senses, digitalisation has increasingly been discussed within this framework. Recently, the concept of human security has also incorporated aspects of well-being associated with the present "yet invisible" reality under post-human security.[27] Post-human security addresses threats to well-being in light of the increasing trend towards critical functions or work previously carried out by humans being performed by machines. In such a machine-dependent era, disruptions or failures of critical functions could have serious consequences for the everyday lives of humans.

As such, one emerging aspect of security that has been increasingly discussed by scholars includes digital security, which focusses on the role of digitalisation in the security of individuals and communities.[28] Essentially, digital security incorporates the foundational framework of human security as a frame of analysis in the interactions between human well-being regarding increased digitalisation.[29] Scholars have already been active in discussing the need for re-inserting the human impact or perspective back into the discourse around cyber security. At the foundational level, Diebert underlines the importance of a human-centric approach to cyber security: "In today's highly networked societies, in which an individual's personal data are widely distributed across numerous platforms, securing privacy requires a comprehensive approach in which individuals are empowered to control what happens to their data no matter where they are located, and governments and companies should have legal obligations to treat data in ways that protect the privacy of all users and citizens – thus promoting human security."[30] Cavelty expands on the need to move beyond state-based security approaches that re-militarise and increase insecurity for human beings. She emphasises moving towards policies that consider privacy and data protection, which are inherently linked to a human rights perspective, as well as understanding cyber security as a social practice and an extension of social knowledge.[31] In this way, the concept of human security is also broadly applicable to digitalisation and the evolution of cyber-based functions and their impacts on the everyday lives of individuals and communities. Human security serves as a broad framework within which the impacts of emerging trends, developments and phenomena related

to the well-being of individuals and communities can be assessed, contrasting with the existing traditional security discourse outlined below.

First and foremost, the tendency in traditional security discourse is to view cyber security as a purely technical concept in which the integrity of a network or computer system is the referent of security. This becomes clear when analysing existing national security policies as well as specific cyber security–related policy documents and supporting research. For example, the European Union Agency for Network and Information Security (ENISA)'s Threat Landscape Report for 2018 highlighted the following as threats: malware; web-based attacks; web application attacks; phishing; denial of service; spam; botnets; data breaches; insider threat; physical manipulation/damage/theft/loss; information leakage; identity theft; cryptojacking; ransomware; and cyber espionage.[32] Although all these inherently impact individuals (e.g. identity theft and information leakage), the predominant object of security is still the network, system or online tool itself,[33] while individuals and their communities are merely implied. Although this focus is still important and increasingly relevant as technology develops further, especially with emerging artificial intelligence technology and autonomous systems, there is another aspect of security that is marginalised when cyber security is presented as a predominantly technical security concept: the real-life impact of societal digitalisation for the security and well-being of individuals and communities.

Furthermore, discussions of the broadening of security within a technology or cyber context are fixated on human behaviour and societal interaction as secondary impacts of digitalisation rather than starting points. While valuable, this perspective does not inherently include an understanding of the interrelated risks and opportunities that may be promoted or threatened in an increasingly digitalised world. The dominance of internet giants and their establishment in market economies, for example, if unchecked by states, may undermine individual rights to privacy, freedom of expression and freedom of thought.[34] The concept of internet and digital rights is quickly emerging as an important aspect of existing human rights regimes[35] and deserves a more dominant focus in existing cyber security debates. For example, in ENISA's recent analysis of research and development (R&D) priorities in cyber security, the inherent role of the individual or community in guiding cyber security processes was underscored in its section on capacity-building as an educational challenge. Within this, the report notes that, "Unless cyber security experts learn, either individually or in groups, to be experts across disciplines (i.e. technical, human behaviour, organisational and regulatory), the ability to build a socially inclusive, secure future for ICT will be lacking."[36] To this end, perspectives that centralise the human within cyber security are relevant to the development of systems that are secure for individuals and communities.

Digital divides, often referred to as "gaps" between demographics and regions in the use of digital technologies in terms of access, training, knowhow and skills, also play a role in understanding the impact of dependence on technology for individuals

and communities. The simple use of technological services and goods requires certain skills and knowledge to navigate and function in such a system. Furthermore, the development of algorithms and functional tools in a cyber context are limited to those with specific skills and education, which can create closed, inaccessible arenas. The digitalisation of critical infrastructure also creates a new variable to consider in the nexus of cyber security conceptualisation. As an increasing number of public goods and services migrate to digital spaces, so do their relationships to societal and human behaviour and their security. However, this also has consequences for individuals and communities in a more direct, tangible way, as vulnerabilities that may have existed in the physical realm are now also present in the digital. The increasing interconnectivity of critical infrastructures, such as electricity, water and energy resource management systems with cyber technology means that societal security and functions depend on the security of the cyber network.[37] In rural regions, including those in the Arctic, digital divides are also experienced along cultural and gender lines, and the presence of opportunities surrounding community-based digital development or innovation are concentrated in larger cities.[38] To this end, individuals and communities seeking to engage in increasing digitalisation in a meaningful way may need to leave their communities to do so, with consequences for the identities and cultural integrities of individuals and communities.

4. The cybersecurity framework and climate change – security examples in the Arctic

The last two sections provided a foundation on which to understand the link between human security, cyber technology and digitalisation and their relevance in the context of a climate-changed Arctic. To demonstrate the interrelated nature of climate change and cyber security for individuals and communities in the Arctic, the following section highlights several examples that underscore and contextualise such security issues.

As discussed above, human security in the Arctic can be assessed by defining both opportunities for enablement (positive security) as well as threats to individuals and communities (negative security). At the regional level, several such assessments have been made in the form of examining digitalisation and telecommunications infrastructure in the Arctic.[39] While this infrastructure may not seem overtly related to cyber security, it is in fact intimately linked, as a connection to the cyber world would not be possible without it. Contextualising cyber security in the framework of human security in the Arctic, scholars have actively addressed the positionality of digitalisation and cyber security from the perspective of human security, developing a human-centric perspective of cyber security more specifically in the EHN. Although this only represents one part of the Arctic, the concept itself does not lose applicability on a larger scale. The defining features of a human-centric perspective of cyber security are also relevant in other Arctic regions, which face similar regional impacts

of climate change, with implications for digitalisation in rural, sparsely populated areas.[40] Zojer and Hossain, for instance, demonstrate the multi-dimensional aspects and impacts of human security in the Barents Region.[41] Zojer further discusses various elements of human security as they relate to digitalisation in the EHN, contextualising human security in the digital arena in a more localised context.[42] Salminen demonstrates the specific link between cyber security policies and their impacts on human security in the EHN in a case study of digitalisation and the social health system in Northern Finland.[43] Dymet demonstrates the link between digitalisation and an increasingly cyber-based sphere of interaction with its impact on societal and individual cultural participation through language in the EHN.[44] Casotta and Sidortsov also underline the vulnerability of critical infrastructure and argue that a new approach to the impact of digitalisation and climate change on the integrity of energy management systems is of vital importance for different states in the EHN.[45]

Rather than considering cyber security solely within a framework of securing a physical object, this article considers cyber security through the lens of "*techne* and *logos*," as suggested by Cavelty in reference to contextualising Bijker's three types of technology into modern understandings of cyber security.[46] In this understanding of cyber security, technology becomes as much a social practice as societal knowledge and therefore re-centres the human into equations about the well-being or integrity of a cyber system. In foregrounding social practice and knowledge regarding cyber technology in discussions of human security, opportunities for enablement emerge from the ways that individuals and communities use social media and the internet generally to participate in larger society. In the same way, threats to human security regarding cyber security can be characterised as the valued aspects of social practice or knowledge that are either no longer accessible via cyber development or have become vulnerable upon their advent in cyber space. Therefore, cyber security viewed through the lens of human security can be perceived as both the enabling and threatening of social practice and knowledge by cyber systems. This view is increasingly relevant when considering advancing digitalisation in the Arctic: "Telecommunication services are seen as improving the quality of life, but the current strategies do not address the potential fears or challenges local inhabitants and communities may experience through the advancement of digitalisation."[47] Furthermore, as climate change is an urgent concern in the northern regions, the Arctic faces yet another wave of digitalisation to measure and mitigate these changes, which must also be reconciled with local communities; contextualising cyber security in the Arctic is thus ever more relevant to discussions on human security.

Digitalisation and climate change are thus phenomena that are rapidly changing societal interactions and consequently have direct influences on the security of individuals and communities in the Arctic. Under a "survival plus"[48] or broader understanding of human security,[49] the impacts of these phenomena are analysed both for their negative security implications (threats and constraints) and their positive security implications (opportunities and enablement). Such analysis must be guided

by the underlying principles of human security, which require the identification of security elements to be made and prioritised by communities themselves. Therefore, this article does not attempt to define or directly implicate specific security concerns for particular communities in the Arctic. Although some scholars have already carried out research in precisely such a framework,[50] such studies remain sparse, and further research is required to meaningfully understand the security connections between climate change, on the one hand, and digitalisation and cyber security, on the other, in the Arctic. This article instead focusses on bringing to light the intimate connections between cyber security and climate change in the Arctic. In doing so, it casts a wide net in the hope that it may spur subsequent studies at a more local, contextual level by various and diverse Arctic communities.

4.1. Negative security (threats and constraints)

The following sub-section examines the interrelated negative security implications arising from digitalisation and climate change in an Arctic context. Negative security implications at the crossover of digitalisation and climate change in the Arctic for individuals and communities can be conceptualised in different ways. As previously discussed, the Arctic's physical environment is changing as a result of climate change. However, such implications are traditionally discussed from the perspective of national security, with cyber security being conceptualised as an extension of the integrity of the technology and infrastructure in cyberspace and in light of increasing uncertainty in the physical environment. For example, Cassotta and Sidortsov's conceptualisation of cyber security in individual countries in the EHN is based on the foundation that "Cyber-attacks against CI serving the energy sector compounded by climate change threats can lead to devastating consequences and put the national security of a state in peril."[51] Of course, this also has direct implications for communities and individuals living in the area who will bear any consequences that result from realised threats to critical infrastructure, since environmental degradation or damage may have direct impacts on physical installations or cyber systems that support critical infrastructure. Examples of critical infrastructures that are supported by cyber- and computer-based technology include health services, finances and banking, utilities and electricity, commercial services, and industries such as aviation, energy and natural resource management. In this way, the social and economic development of various sectors of society are inherently dependent on digitalised critical infrastructure.

Furthermore, both climate change and threats to cyber security vis-à-vis critical infrastructures have implications for societal well-being, given that both can impact the functioning of an electric-grid system, water system or energy supply chain.[52] As climate change triggers more extreme weather events and the possibility of natural disasters, physical infrastructures are increasingly vulnerable to damage. As noted above, much of the existing infrastructure was not built considering the consequences that could arise from either climate change or cyber security, given the lack

of evident need at the time it was put into place.[53] Indeed, new technologies were often developed and introduced at such a rapid rate that their implementation in critical infrastructures was poorly understood or constructed. Similarly, climate change as a factor of consideration in urban planning and infrastructure development was not deeply integrated in the construction of critical infrastructures, leading to the degradation and increased vulnerability of critical infrastructures, such as in Alaska, where they have been damaged due to the unexpected melting of the permafrost as a result of climate change.[54] Thawing permafrost also affects the physical structures supporting daily life, such as electricity and grid networks, utilities, and water and waste management systems. Such consequences are visible across the Arctic – climate change in the region has already begun to impact the production of hydropower and the management of water systems through changes in the amount of precipitation, and poor infrastructural conditions are putting distribution networks at risk.[55] These systems are vital, and so climate change also has direct implications for the integrity of cyber-physical infrastructures and their operational systems which support human needs in the region.[56] Furthermore, repairing, restoring or addressing any damage, malfunction or cyber-attack to the physical installations of digital critical infrastructures in the region may require complex, careful, expensive and/or time-consuming action. As such, digital critical infrastructures that are developed to be resilient and robust against possible threats from climate change are necessary in the event of increased climactic conditions in the Arctic. In other words, critical infrastructures need to be resilient both in meeting physical climactic threats and increased human vulnerability in light of cyber insecurities such as cyber-attacks.

While this is certainly an important aspect of security implications at the intersection between climate change and digitalisation, using Cavelty's approach to cyber security as social practice and societal knowledge, in light of human security, different issues arise that threaten the security of individuals and communities in the Arctic. For example, given the urgency of climate change in the region, the issue has become a narrative used to justify increased digitalisation in the hopes of reducing costs, transportation and energy consumption.[57] As such, public services are becoming increasingly digitalised, physical services are decreasing, and cultural and societal reliance on certain types of knowledge or physical services and interaction are changing. This also requires social change to occur, which can have implications for individual and community practices that may conflict with communal well-being and security in other ways. For example, Salminen discusses the discourse regarding digitalisation of the health system in the Länsi-Pohja area in Finland following disputes and efforts to restructure the system as well as the relationship of this public discourse to the personal security of the communities and individuals residing there.[58] As part of her argument, she notes that individual security concerns are also part of such changes and involve increased personal vulnerability within a more complex digitalised system. For example, managing diverse security credentials, establishing and knowing how to deal with different levels of trustworthiness of different

platforms, and intuitively understanding the necessary processes involved regarding shared, stored, managed and collected data all have implications for personal security.[59] Ultimately, she notes that, "Usually, when digitalisation and cybersecurity are discussed in the context of healthcare, the discourse does not revolve around user interfaces or people's experiences with or fears for service digitisation."[60] Furthermore, as health systems become more digitalised and move towards e-health and tele-health services to cut costs and energy consumption, they may be vulnerable to privacy breaches as information is stored digitally, and existing critical infrastructure supporting them may be compromised.[61] The combination of complexities, changing health interfaces themselves, the replacement of physical interfacing with digital in remote areas, potential digital divides, and the support infrastructure needed in Arctic climactic and geophysical conditions compounds the potential security implications for communities and individuals using and relying on such functions.

As climate change drives more digital solutions to reduce energy output and physical cost, it commensurately affects data storage and accessibility. Besides the example of stored personal health data, there are countless examples of both intimate personal data and seemingly harmless proximal data that must be contended with. Furthermore, societal knowledge, interactions and information are translated into data when they take place online (for example, Facebook), which is stored and secured for access by specific authorities. However, ownership, use, analysis and access to this data is not always in the hands of the communities and individuals that generate it. As communities begin to utilise and rely on digital technologies as tools for societal interaction and extending knowledge, they also rely on specific infrastructure and connectivity to meet such demands. As such infrastructure is relatively vulnerable in the northern Arctic regions, this has direct implications for those using technologies to extend societal interactions or practice into the digital realm. What happens if there are breakdowns in these systems? The advent of both digitalisation and climate change has direct implications for cyber security in the realms of personal security, information security, data protection and privacy for individuals and communities.

4.2 Positive Security (opportunities/enablement)

The following sub-section examines the interrelated positive security implications arising from digitalisation and climate change in an Arctic context. Positive conceptualisations of security implications at the crossover of digitalisation and climate change are easiest to view through the use of social media to enable engagement and participation across communities in the Arctic. Extractive industries and economic development projects tied to natural resource use in the Arctic are increasingly interesting as climate change renders much of the north more accessible to possible development. To the degree this occurs, human security for communities and individuals is inherently tied to the ability to advocate and negotiate the projects and developments that impact their daily lives. As such, narratives of environmental justice and efforts to generate awareness and activism surrounding these concerns have emerged.

Ultimately, digitalisation has offered such an avenue for participation as well as the possibility to influence the decision-making processes behind such projects.

With the advent of digitalisation, many these discussions have moved online, and social media has become the predominant forum for social interaction regarding political, social and economic developments. In the Arctic, this must also be conceptualised alongside the simultaneous phenomenon of climate change, which has impacted immediate and long-term social practice and planning regarding security. Social media has provided communities across the Arctic with the possibility to bring local issues to the global stage and to increase their participation in the development of certain activities arising from environmental or climate change–related issues in their communities. Skjervedal discusses how social media has increased the public participation of youth in forums for public participation regarding mineral and petroleum projects in Greenland.[62] A rise in such projects could occur as climate change renders more of Greenland accessible to resource use.[63] She suggests that current systems for public participation are strengthened and improved through social media as a method for public engagement and underlines the role of such technology in providing access to decision-making for youth.[64] She found that social media removes the barriers of logistics, timing and cost and motivates youth to actively participate in sharing their views and perspectives regarding extractive industry projects in Greenland.[65] As climate change generates interest in extractive industrial development in Greenland, such processes are expected to become part of societal development, with digitalisation providing a positive tool to assist in defining the security of individuals and communities impacted by such change. In this way, social media has enabled communities to define, actualise and advocate for their security and well-being. Considering cyber security as an extension of security through social practice and knowledge in relation to technology, another form of positive security includes the utility of digitalisation in bringing new tools into the social practices of individuals and communities. This includes, for example, the use of online platforms for the preservation and dissemination of social and cultural knowledge, which are of particular importance to Indigenous peoples in the Arctic.[66] For example, various online groups exist to share and disseminate Indigenous languages tools – including a Facebook group focused on learning Inupiaq[67] and a course to learn Inupiaq words on a popular language learning platform.[68] In this way, digitalisation has spurred increased interest, use and understanding of digital tools that can overcome digital divides, secure cultural and societal practices through language, and advocate for local needs and perspectives.

4. Conclusion

Ultimately, given the widespread presence of online tools, new strategies to understand and connect security in cyberspace to individuals and communities need to be addressed. As individuals and communities rely and depend more heavily on

cyber technology and climate change shifts the practices and societal functions of existing communities, the threats and opportunities implicit in such processes need to be discussed and considered on a policy level. Furthermore, cyber security must be understood from a human-centric perspective to assess its impacts on society. Simultaneously, as the urgency of climate change and its implications for society increase, a nuanced and integrated approach to understanding security in the Arctic is necessary in all aspects. Although cyber security is predominantly viewed as impacting an invisible, intangible space, it has very real implications in the physical world. As the physical world changes as a result of climate change, these two phenomena inherently interact in impacting the security of communities and individuals in the Arctic. Given the rapid pace with which these simultaneous phenomena are changing communal practices, both need to be seriously considered from the perspective of human security and made relatable to the everyday well-being and security of individuals and communities.

ACKNOWLEDGEMENTS

This work was supported by Nordforsk, under Grant number 81030, and within the framework of the research project, *Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy)*.

NOTES

1. G Hoogensen, "Security by Any Other Name: Negative Security, Positive Security, and a Multi-Security Approach," *Review of International Studies* 38 (2012): 835–859.
2. M Salminen and K Hossain, "Digitalisation and Human Security Dimensions in Cybersecurity: An Appraisal for the European High North," *Polar Record* 54, no. 275 (2018): 108–118.
3. Ibid.; Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics* 20, no. 3 (2014): 701–715; M Salminen, "Digital Security," in *Society, Environment and Human Security in the Arctic Barents Region*, eds. D Cambou and K Hossain (Abingdon, Oxon: Routledge, 2018), 187–204; G Zojer and K Hossain, "Re-thinking Multifaceted Human Security Threats in the Barents Region: A Multi-Level Approach to Societal Security," *Juridica Lapponica* (2017), 42; G Zojer, "Free and Open Source Software as a Contribution to Digital Security in the Arctic," *The Arctic Yearbook* (2019), 1–16.
4. S Mackie, "Environmental Security in the Barents Region," in *Society, Environment and Human Security in the Arctic Barents Region*, eds. D Cambou and K Hossain (Abingdon, Oxon: Routledge, 2018), 37–57.
5. Arctic Council, *Telecommunications Infrastructure in the Arctic: A Circumpolar Assessment* (2017), 17, http://hdl.handle.net/11374/1924.
6. T Heleniak and D Bogoyavlenskiy, "Arctic Populations and Migration," in *Arctic Human Development Report: Regional Processes and Global Linkages*, eds. J N Larsen and G Fondahl (2014), 53–103, http://norden.diva-portal.org/smash/get/diva2:788965/fulltext03.pdf.
7. IPCC, "Summary for Policymakers," in *Global Warming of 1.5°C: An IPCC Special Report on the Impacts of Global Warming of 1.5°C Above Pre-Industrial Levels and Related Global*

Greenhouse Gas Emission Pathways in the Context of Strengthening the Global Response to the Threat of Climate Change, Sustainable Development, and Efforts to Eradicate Poverty (2018), https://www.ipcc.ch/sr15/chapter/summary-for-policy-makers/.

8. AMAP, *Adaptation Actions for a Changing Arctic: Perspectives from the Bering-Chukchi-Beaufort Region* (December 28, 2017), https://www.amap.no/documents/doc/adaptation-actions-for-a-changing-arctic-perspectives-from-the-bering-chukchi-beaufort-region/1615.; AMAP, *Adaptation Actions for a Changing Arctic: Perspectives from the Barents Area* (October 10, 2017), https://www.amap.no/documents/doc/adaptation-actions-for-a-changing-arctic-perspectives-from-the-barents-area/1604.
9. ACIA, *Impacts of a Warming Arctic* (October 15, 2004), https://www.amap.no/documents/doc/impacts-of-a-warming-arctic-2004/786.
10. IPCC, *Global Warming of 1.5°C*, 32.
11. K Klubnikin and D Causey, "Environmental Security: Metaphor for the Millennium," *Seton Hall Journal of Diplomacy and International Relations* 2,3 (Summer/Fall) (2002), 124.
12. According to the Arctic Human Development Report, it is unlikely that Arctic societies and cultures can remain resilient in the face of all of these biophysical and societal changes. Arctic societies face an unusual combination of biophysical and socio-economic stresses, many of which can be linked to oil and gas development. See O R Young and N Einarsson, "A Human Development Agenda for the Arctic: Major Findings and Emerging Issues," in *Arctic Human Development Report*, eds. N Einarsson, J N Larsen, A Nilsson, and O R Young (Akureyri: Stefansson Arctic Institute, 2004), 230; O Langhelle and A Mikkelsen, "Framing Oil and Gas in the Arctic from a Sustainable Development Perspective," in *Arctic Oil and Gas Sustainability at Risk*, eds. A Mikkelsen and O Langhelle (Abingdon, Oxon: Routledge, 2008), 32.
13. For example, clashes between mining companies and indigenous communities. See K Hossain and A Petrétei, "Resource Development and Sámi Rights in the Sápmi Region: Integrating Human Rights Impact Assessment in Licensing Processes," *Nordic Journal of International Law* 86, no. 3 (2017), 302–340.
14. M L Parry et al., *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: Cambridge University Press, 2007), 672.
15. K Hossain, "The Question of Societal Security in the Arctic," in *Society, Environment and Human Security in the Arctic Barents Region*, eds. K Hossain and D Cambou (London: Routledge, 2019), 3–18.
16. K Hossain, "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," *The Yearbook of Polar Law* 10 (2019), 275–296.
17. K Hossain, "Human Security in Cyberspace and Climate Change: A Reflection from the European High North," *European Journal of Human Security* 2, no. 3 (2018), 55–74.
18. K S Gulbrandsen and M Sheehan, "Social Exclusion as Human Insecurity: A Human-Cybersecurity Framework Applied to the European High North (EHN)," in *Digitalisation and Human Security: A Multi-Disciplinary Approach to Cybersecurity in the EHN*, eds. Mirva Salminen, Gerald Zojer, and Kamrul Hossain (Palgrave, 2020).
19. Salminen and Hossain, "Digitalisation," 108–118.
20. UNDP, *Human Development Report* (New York, 1994).
21. UNTFHS, *Human Security Handbook* (New York: UN Human Security Unit, 2016).
22. UNGA, Resolution Adopted on 10 September 2012, 66th Session, Agenda Items 14 and 117, A/RES/66/290 (New York, 2012).
23. UNTFHS, *Human Security Handbook*.
24. K Booth, *Theory of World Security* (Cambridge: Cambridge University Press, 2007).

25. Hoogensen, "Security by Any Other Name," 853–859.
26. Hossain, "Human Security," 55–74.
27. J P Burgess, "Posthuman Security," *European Journal of Human Security* (2017), 63–73.
28. Salminen, "Digital Security," 187–204.
29. Ibid.
30. R Diebert, "Towards a Human-Centric Approach to Cyber Security," *Ethics and International Affairs* 32, no. 4 (2018), 411–418.
31. Cavelty, "Breaking the Cyber-Security Dilemma," 701–715.
32. ENISA, *ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends* (January 28, 2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport.
33. Ibid.
34. Diebert, "Human-Centric Approach," 411–418.
35. D Joyce, "Internet Freedom and Human Rights," *The European Journal of International Law* 26, no. 2 (2015), 493–514.; N Cardozo et al., "Promoting Security Researchers' Rights in the Americas" (2018), https://eff.org/coders-rights-americas.
36. ENISA, *Analysis of the European R&D Priorities in Cybersecurity: Strategic Priorities in Cybersecurity for a Safer Europe* (December 19, 2018), https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity/at_download/fullReport.
37. Hossain, "Human Security," 55–74.
38. D P Subramony, "Understanding the Complex Dimensions of the Digital Divide: Lessons Learned in the Alaskan Arctic," *The Journal of Negro Education* 76, no. 1 (2007), 57–67.
39. Arctic Council, *Telecommunications Infrastructure*.
40. Ibid.
41. Zojer and Hossain, "Re-thinking Multifaceted Human Security," 42.
42. G Zojer, "The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised Through the Human Security Lens," in *Yearbook of Polar Law: Volume 10*, eds. T Koivurova, G Alfredsson, D Cambou, and J Klein (Leiden: Brill, 2019), 297–320; G Zojer, "Free and Open Source Software as a Contribution to Digital Security in the Arctic," *The Arctic Yearbook* (2019), 1–16.
43. M Salminen, "Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North," in *Yearbook of Polar Law: Volume 10*, eds. T Koivurova, G Alfredsson, D Cambou, and J Klein (Leiden: Brill, 2019), 321–357.
44. M Dymet, "Digital Language Divide in the European High North: The Level of Online Presence of Minority Languages from Northern Finland, Norway and Sweden," in *Yearbook of Polar Law: Volume 10*, eds. T Koivurova, G Alfredsson, D Cambou, and J Klein (Leiden: Brill, 2019), 247–274.
45. S Cassotta and R Sidortsov, "Sustainable Cybersecurity? Rethinking Approaches to Protecting Energy Infrastructure in the European High North," *Energy Research & Social Science* 51 (2019), 129–133.
46. Myriam Dunn Cavelty, "Cybersecurity Research Meets Science and Technology Studies," *Politics and Governance* 6, no. 2 (2018), 22–30; W E Bijker, "Why and How Technology Matters," In *The Oxford Handbook of Contextual Political Analysis*, eds. R E Goodin and C Tilly (Oxford: Oxford University Press, 2006), 681–706.
47. Zojer, "The Interconnectedness of Digitalisation," 309.
48. K Booth, *Critical Security Studies and World Politics* (Boulder: Lynne Rienner Publishers, 2005).
49. Hoogensen, "Security by Any Other Name," 853–859.
50. M Salminen, "Refocusing and Redefining Cybersecurity," 321–357.
51. Cassotta and Sidortsov, "Sustainable Cybersecurity?" 132.

52. Hossain, "Human Security," 55–74.
53. Ibid.; N2 Consultants, *The Link: CyberSpace and The Climate: Our False Sense of Security Climate Change and Cyberthreats* (N2 Consultants, 2015).
54. D Allen, *Climate Change and Cyber Threats: Acknowledging the Links* (The Center for Climate and Security, 2014), https://climateandsecurity.org/2014/09/08/climate-change-and-cyber-threats-acknowledging-the-links.
55. G S Eskeland and L S Flottorp, "Climate Change in the Arctic: A Discussion of the Impact on Economic Activity," in *Statistics Norway: The Economy of the North* (2006), 85, https://www.ssb.no/a/english/publikasjoner/pdf/sa84_en/kap6.pdf.
56. Hossain, "Human Security," 55–74.
57. Salminen, "Digital Security," 187–204; M Salminen, "Refocusing and Redefining Cybersecurity," 321–357.
58. Ibid.
59. Ibid., 350–351.
60. Ibid., 349.
61. Ibid.
62. A S Skjervedal, *Current Practices of Public Participation with Focus on Youth Engagement in Greenland* (October 17, 2017), Lecture, https://www.youtube.com/watch?v=LQx4gv9h2QI&t=918s&fbclid=IwAR0mMuhuzdfcRAjEO3Fbw1a87mfrteYjUcHfygg2fDtDvLRNOl_2f0RIJns.
63. M Rosing, *Potential for Geologic Resources in Greenland: Strategic Assessment of Development of the Arctic* (December 3, 2013), https://www.arcticinfo.eu/en/features/88-potential-for-geologic-resources-in-greenland.
64. Ibid.
65. Ibid.
66. G Amatulli and J Klein, "Indigenous Community Security in the Barents Region," in *Society, Environment and Human Security in the Arctic Barents Region*, eds. D Cambou and K Hossain (Abingdon, Oxon: Routledge, 2018).
67. For example, see the online Facebook language group for Inupiaq language learners: https://www.facebook.com/groups/153697614729578/?hc_ref=ARRpqqNRW1HFmjMjpk1y-IHAb-SJF5ejtjtXjit2Wp1A9cqJy_dbewthYL0tkfAEA_9U&__tn__=CH-R.
68. For example, see the Memrise course for beginners Inupiaq: https://www.memrise.com/course/314973/beginner-inupiaq/ (accessed April 15, 2019).