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.