European Journal of Human Security

UDK 3.351.78:004.738.5]:551.583 (4-17)
https://doi.org/10.18485/fb_ejhs.2018.2.3

Human Security in Cyberspace and Climate Change: A Reflection from the European High North

Kamrul Hossain[1]

Introduction

This article reconceptualises human security by linking it to components of the framework of cyber security. The concept of human security recognises both the enablement of and threats to human wellbeing. Cyber security, until recently, has been mainly explored from a national, rather than a human, security perspective. The connection to security in cyberspace, on a more general level, has been mainly addressed through traditional security perspectives. That is, states themselves are primarily the referent objects of cyber security, given that most threats are targeted at critical infrastructures where national authorities are the intended victims either directly or indirectly. Therefore, cyberspace is argued to be a primary operational environment for national security, which is hence to be protected with both defensive and offensive military means (Lehto, Huhtinen & Jantunen, 2011). Threats to cyber security, however, also reflect the security needs of people within states which have so far been ignored (Liaropoulos, 2015. p. 189). People's security needs are shaped, among others, by various compo-

1 Research Professor and the Director of the Northern Institute for Environmental and Minority Law (NIEM) at the Arctic Centre of the University of Lapland. This article is produced as part of the research project entitled Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy) funded by NordForsk and the ESRC (UK), and hosted by NIEM. khossain@ulapland.fi

nents of human security concerns, such as basic needs in terms of ensuring services related to, for example, health care, education, supply of water and energy, etc. An uninterrupted functioning of critical infrastructures, which are run through digital or cyber technology, for example, ensures the fulfilment of these security needs. As a result, the aspects of cyber security having both positive and negative implications for human wellbeing go hand in hand with what the concept of human security stands for. The following article discusses aspects of cyber security that have an impact on the lives of individuals and communities at the sub-state level, as well as across states at the regional level. This article focuses on the European High North (EHN) – a trans-national region composed of the northern parts of Finland, Norway and Sweden, as well as the north-western part of Russia. Given that the region and its population, including a number of indigenous communities, faces severe challenges due to the impacts of climate change, this article examines how interlinked implications of climate change and cyber security impact human security, particularly in the EHN region.

Human Security Reconceptualised

The traditional understanding of security was reconceptualised at the end of the Cold War. In the early 1990s, state-centric military understandings of security – referred to as traditional security – was supplemented by a rather broadened and deepened understanding of security. The notion of security was reformed around multiple referent objects – with states not being the only referent object – and at multiple levels, both within, and beyond, the state. In other words, the concept of security refers not only to threats to states' survival, but rather calls for a comprehensive approach to addressing threats and risks at various levels by engaging multiple actors, including individuals and communities, as referent objects. This new approach therefore develops a deeper dimension to

addressing security with greater focus on human beings at its core (Jano, 2009, p. 74).

Traditional state-centric security is largely complemented by this comprehensive approach (Ruiz De Garibay, 2007; Cilliers, 2004, p. 10). The more a state is internally secure within itself, the more its political integrity is secure. Today, security does not hold a fixed meaning (Hossain et al., 2018). It relates to a context-specific understanding, framing the concept both as contested and with many different meanings. Security nowadays does not only refer to threats to states' existence; rather, it is more focused on the survival of humans and the promotion of their wellbeing. Reducing vulnerabilities and thereby promoting the wellbeing of individuals and communities at all levels of governance is the central purpose of security. Hence, threats impacting the lives of humans and communities, including on the sub-national, trans-national and supra-national levels, are fundamentally security concerns. The common articulation of these threats is built around the concept of human security. The United Nations (UN) Human Development Report (HDR) endorsed by the United Nations Development Programme (UNDP) in 1994 played a crucial role in promoting and popularizing the concept. The HDR analysed human security through seven specific indicators, such as health, food, community, personal, environmental, economic and political. These seven components are interconnected – they are at times contradictory, hence one undermines the other, and at other times complementary, when one influences the other to further accelerate existing threats. For example, the promotion of environmental security contradicts the promotion of economic security, considering that the more environmentally secure a community is, the less economically secure it is (Hossain, 2017, p. 11). Similarly, environmental security is interconnected with many other components of human security, and thereby threats to environmental security may accelerate threats in other sectors too, such as in food, health, community security, etc.

The importance of human security lies in the fact that, unlike traditional security threats, human security threats arising out of, for example, threats to the environment, health and food, etc. "kill far more people" than war, genocide and terrorism combined (Human Security Report, 2005). Threats to human security create the root causes of all insecurities (UNGA, 2005). They affect the vital core of all human lives (Commission on Human Security, 2003). Therefore, fulfilling basic human needs for survival is at the heart of the concept (UNDP, 1994). As a policy tool, human security offers an "emancipatory and empowering framework" to address urgent issues in specific situations (McCormack, 2008). It has both preventive and pro-active dimensions; in other words, it embraces both top-down and bottom-up approaches. It represents both negative security – "security from" (threats) and positive security – "security to" (enablement) (Hoogensen Gjørv, 2012). The referent objects of security – individuals or communities – are not only subject to protection from threats; they also exercise agency in building the capacity to avoid risks and in improving the system of protection (Commission on Human Security, 2003).

Human security is therefore more about protecting and promoting a society in which people live with a set of freedoms – from "fear", "want" and "indignity". These terms, however, are elusive and render the human security concept to incoherent and abstract representations (Paris, 2001, p. 90), for there are no established indicators to determine the level of threat at which point a response or prevention mechanism should be invoked. Yet these non-traditional sources of security threats do have utility in identifying specific threats that impact humans and communities (Owen, 2004, p. 382). Addressing human security threats in a policy framework provides added-value, and promotes agendas on behalf of individuals or communities who are the objects of threats. Including individuals and communities within the policy framework to define the security threats affecting them promotes capacity building for those who might other-

wise be marginalized (Hoogensen and Vigeland Rottem, p. 2004). Identifying and addressing these sources of insecurity, and promoting response mechanisms to mitigate them, requires an innovative approach (Jano, 2009, p. 75). The human security framework certainly provides such an approach – an analytical tool – offering insightful understanding of multi-dimensional aspects resulting in security threats (Booth, 2005; Sheehan, 2005). The framework asks security for whom, security for which values, how much security, and security from what threats, by what means, at what cost, and in what time period (Baldwin, 1997, pp. 12–18).

The reconceptualised model of human security, because of its broadened character, embraces yet other kinds of threats or risks linked to human safety that may result from, for example, civil safety, which includes emergency response and preparedness in case of potential natural or man-made disasters, making human security and human safety intertwined. The sources of un-interrupted functioning of the conditions, such as critical infrastructures, on which the physical existence of an individual and community is dependent can well be interpreted as part of human security. In most recent literature, human security is also addressed from the viewpoint of the present "yet invisible" reality – the so-called post-human security (Burgess, 2017, pp. 63–73), where human functions are increasingly being replaced by technological innovation. While humans still outperform machines in many functions, such as specialist thinking or complex communication (Holopainen & Jokikaarre), technological innovation is expected to increasingly take over many critical functions, which will eventually create a machine-dependent society, capable of causing other kinds of threats to human security. Any disruption to or technological failure by machines in their everyday functioning will therefore have serious consequence for humans. It is in this context that cyber security integrates the concept of human security since

it involves the protection of individuals and communities in their everyday life.

At the same time cyber security also embraces the threat and enablement approach of human security in that it seeks to safeguard cyberspace for individuals and communities, yet also promote the development of infrastructure and protection measures to secure individual and community interactions with cyber technology. Apparently, cyberspace is gradually becoming primarily a "digital civil society", in which cyberspace is seen as a place where both material and non-material products and services are offered (Lehto, Huhtinen & Jantunen, 2011). Consequently, a broad definition of cyberspace integrating phenomena from technological and social concepts (ibid.) offers new elements in the understanding of human security, which states often "undervalue". However, it is today argued that cyber security is addressed as a facilitating tool for human empowerment, whereby people and communities benefit from interacting with cyberspace (Liaropoulos, 2015, p. 192). A reconceptualised approach of human security thus complements the existing structure by perceiving the adoption of measures for practices and policies linked to increasingly technology-dependent humans. In this context, the following section analyses the interrelated implications arising out of climate change and cyber security posing threats to human security.

Climate Change and Cyber Security

The impacts of climate change are diverse and transboundary. Climate change impacts the entire ecological system, and is eventually capable of contributing to impacts on the environment, economy, infrastructure, society, politics and demography. Such impacts cause significant challenges across regions and can lead to global instability. The most common challenges climate change presents are: changes in ecosystem services on which the

life support system is dependent; an increase in natural disasters; resource scarcity; changing land use practices that result in an unequal distribution of natural resources; the large-scale displacement of populations that ultimately changes the demographic balance affecting community structure. Human suffering increases as a result of, for example, a loss of local environment contributing to poverty, poor quality of life, unequal resource distribution, lack of access to clean water, detrimental impacts on infrastructures that support critical services to humans and communities, etc. The eventual consequences of climate change can give rise to changes in the socio-political system and lead to various forms of local and regional conflict. In addition, climate change hinders the ability to produce or reproduce most basic utilities such as food, water and energy infrastructures, potentially undermining, for example, global food markets and economic growth (Allen, 2014). It is in this latter context, as discussed later in this section, that the effect of climate change relates to cyber security infrastructure.

Cyber security is generally referred to as threats arising out of cyber warfare, cyber-attacks, cybercrime, etc. From a security perspective, cyberspace is considered the next platform of modern warfare (Bruijn & Janssen, 2017). Cyber threats refer to attacks intended to damage, or obtain unauthorized access to, internet or computer network systems. These attempts include, for example, hacking into financial accounts or institutional operation systems either to obtain financial information or to make unauthorized gains. The promotion of cyber security is about undertaking measures to counteract cyber threats, such as running current antivirus programs and verifying that one's computer system is fully secure (N2 Consultants, 2015). As previously discussed, cyber threats are generally addressed from national security perspectives. However, today the most basic resources, such as water and energy infrastructures – the so-called critical infrastructures – are increasingly integrated through cyber interconnectedness. Critical in-

frastructure refers to a set of physical installations or cyber systems and resources that are so essential to an organization or nation that their failure or damage would be extremely detrimental to the populations they serve (N2 Consultants, 2015). Energy, transport, the financial network system, computer-based health care and online commercial infrastructures are some of the examples. Computer-based technologies, with cyberspace and the internet being a primary conduit (Allen, 2014), are indispensable in maintaining the function of critical infrastructures. Moreover, today social and economic development in all sectors are integrally dependent on infrastructures supported by cyber technologies.

Establishing links between climate change and cyber security is complex. Climate change is linked to the impact of human behaviour affecting the earth's atmosphere and natural environment, whereas cyberspace lies within the inner world (N2 Consultants, 2015), affecting the human-built environment. Billions of actors have an impact on the global climate, and in the same way they have an impact on functions in cyberspace (N2 Consultants, 2015). The earth's atmosphere and cyberspace are two distinct extraterritorial arenas (Shackelford, 2016, p. 656). These two regimes are apparently unrelated. There are differences, for example in terms of the variables affecting climate and cyberspace. However, the risks associated with them both are anthropogenic (Allen, 2014). Cyberspace and the climate regime are linked by their status as originating from man-made threats (N2 Consultants, 2015). They both threaten homogenous elements, such as critical equities including food, water, energy, and infrastructures (Allen, 2014). Both the implications of climate change and cyber security threats often have an impact on the same critical infrastructures, such as the electric grid, the water supply system, etc. Impacts of climate change, such as floods or other natural disasters, increase the risk of damage to physical infrastructures, such as electricity or energy supply chains. The consequence of climate change has of-

ten been little considered during the construction of such infrastructures. This is because they were largely built at a time when threats from climate change and cyber development were either not evident, poorly-understood, or simply ignored (N2 Consultants, 2015). Furthermore, the rapid pace of the development and introduction of new technologies meant that their implementation in critical infrastructures was unprecedentedly fast and therefore vulnerable. For example, some of the important critical infrastructures in Alaska are found degraded or threatened due to the melting of permafrost because of the consequences of climate change (Allen, 2014). It is also important to look into specific regional characteristics while framing strategies for building new physical infrastructures supported by cyber technology because they might well be vulnerable unless threats to cyber security are addressed. Moreover, climate change also causes a domino effect as a disruption to any one infrastructure can cause disruptions to others due to their extensive interdependencies (Allen, 2014).

A cyber security threat – a cyber-attack for example – to computers and industrial equipment responsible for the smooth operation of these critical infrastructures, such as electric and nuclear power plants, may have serious negative impacts, not only on physical infrastructures, but also eventually on human lives and on their basic needs. When cyber-attacks on critical infrastructures coincide with vulnerabilities from climate-induced changes impacting the same infrastructures, the implications for human security are grave. The potential devastating impact on infrastructures or establishments would contribute to increased human suffering. Given the similar nature of threats originating from both cyberspace and climate regimes, cyber security is argued to reinforce human security where the effect of climate change, physical structures, and the continued functioning of critical infrastructures are interdependent. Developing strategies to mitigate these interrelated challenges thus

contributes to promoting human security as well as a climate- and cyber-secure future (Allen, 2014).

Human Security as It Applies to Cyber Security Infrastructure

A human security approach to cyber security is a comprehensive, complementary approach which acknowledges multiple sources of vulnerability to individuals, and includes strategies to address them. However, as referred to earlier, discussions on cyber security often fail to utilize human security as an analytical tool. Rather, states' national security is often linked to cyber security. While it is true that a safe, secure and open cyberspace is not possible without the involvement of states, they are themselves at times violators of the security of their own subjects. In particular, in those states where an effective and functioning democracy is rather weak, intelligence agencies exploit and manipulate personal data, making cyberspace at times more insecure for citizens. Such practices also hinder the removal of known insecurities (Kerr, 2016), such as those connected to threats to personal and political security. Cyber security embraces elements that place consequences on individuals when information infrastructure is breached or its protection is not ensured. Personal data protection and privacy, the human right to private life, and protection from cyber-attacks are central to contemporary human needs and presented in cyber security literature in connection to human security (Salminen, Hossain, 2018). Threats within a cyber security framework can, if realized, restrict a number of individual and community freedoms that enable personal security. However, the promotion of human security in cyberspace does provide opportunities for empowerment, and for communities and individuals to flourish in contemporary life. Often resilience is the key term used for the promotion of such empowerment, which in other words means enhancing one's skills in the use of computer networks and information technology and promoting

know-how on information sharing while being aware of the associated risks.

Given that this particular article examines human security as it applies to cyber security in connection to the implications of climate change, and in the context of the EHN, the particular threats referred to herein are the ones emerging from a disruption or dysfunction in the system or the failure of technology-driven digital infrastructures, which have consequences on basic human needs. Therefore, these threats are referred to as second- or third-order consequences felt by individuals and communities in their everyday life (Salminen, Hossain, 2018) given that any interruption in the functioning of such infrastructure affects crucial supplies and services, such as energy, water, health and other services, etc. These critical functions are at risk from threats that exist in cyberspace. However, the human dimensions of such threats are much less commonly associated with the human security framework despite the fact that the disruption of these utilities puts at risk individuals and communities in their everyday life – they are not necessarily purely existential threats though (Burgess, Sissel, 2008). Therefore, instead of pinpointing humans as the weakest link to cyber security (Salminen, Hossain, 2018), it is focusing on the risks inflicted upon individuals and communities as a consequence of climate change implications to critical infrastructures and to everyday services, and thereafter addressing them adequately, that would be a constitutive application of underlying human security principles.

Human security is jeopardized when a disruption increases vulnerabilities to accessing basic resources supported by digitally controlled critical infrastructures (such as energy or water supplies), services such as health and education, as well as the functioning of livelihood activities. The impacts of such disruptions go beyond physical damage to installations and infrastructure. They also involve costs associated with the repair or replacement of affected infrastructures, as well as

the subsequent economic, social and environmental impacts. If supply chains are disrupted, economic activities might be suspended, and consequently social wellbeing might be subject to threats. For example, public health and safety issues are increasingly supported by critical infrastructures whose operation is linked to the cyber security framework. Risks arising out of the impacts of climate change on these infrastructures would not only cause damage to physical infrastructures offering critical functioning, but would also potentially result in economic losses, such as the cost to rebuild assets, the cost to respond to and recover from attack as well as costs resulting from the disruption of products or services (N2 Consultants, 2015). Moreover, losses also arise in the long-term costs of environmental damage. These losses impact economic and political institutions and the ability of the government or industry to maintain order in ensuring the delivery of minimum essential public services, public health and safety (N2 Consultants, 2015). These issues contribute to significant human suffering and can be translated into a number of human security threats, such as threats to health, food, environment, economy, community, etc.

The European High North Context

The EHN can be identified as an ideal region to demonstrate how interconnected human security threats arise out of the implications of climate change and the existing cyber security framework. There is no clear definition for the EHN region. This article refers to the northern parts of Finland, Norway, Sweden, and the north-western part of Russia as the EHN. It is a part of the broader Arctic region and therefore shares some common Arctic features, such as remoteness, sparse populations, sporadic and vast distances between settlements, and the presence of local and indigenous communities participating in subsistence livelihoods. However, compared to other parts of the Arctic, the EHN, with the exception of the

north-western part of Russia, is relatively well-advanced and well-developed in terms of infrastructure and connectedness. The region and its population benefit from the use of readily available modern technology. A number of major urban centres are located in the region, including: Oulu and Rovaniemi in Finland; Tromso, Alta, and Kirkenes in Norway; Murmansk, Apatity, and Kirovsk in Russia; and Luleå and Kiruna in Sweden. These urban centres are capable of extending at least some basic support services to rural communities, given that most of the EHN is accessible through a well-connected road network. However, the most remote areas in the vicinity still face critical challenges arising from a lack of adequate infrastructure and support services.

Climate change has implications for both negative and positive consequences in the EHN, as in other parts of the Arctic. Changes in the natural environment have become evident due to warming temperatures, which are two to three times greater in the Arctic region than the global average (IPCC, 2018, p. 6) and contribute to the melting of permafrost and changes in precipitation (Eskeland, Flottorp, 2006, p. 81). Such changes contribute to extreme weather patterns – an increase in temperatures can change the direction of wind and water currents, rendering some parts of the region warmer and others colder (Eskeland, Flottorp, 2006, p. 81). In other words, the region experiences more uncertainty as the implications of climate change intensify, which accelerates with the unpredictability of the region's climatic conditions. Moreover, a long winter season, darkness, and a harsh environment, when combined with such unpredictable conditions, can result in major challenges to the region's infrastructures and economy, and its population. Climate change, particularly in the Arctic context, is often referred to as a threat multiplier (Werrell, Femia, 2015), which exacerbates other threats to security and results in diverse challenges for humans and communities. For example, concerning livelihood practices in the EHN region, traditional and nature-based activities are either

replaced by new economic activities, such as the exploration and extractions of minerals and petroleum, tourism, transportation, the construction of infrastructure, etc. (Eskeland, Flottorp, 2006, p. 89) or adapted to take advantage of contemporary technologies. For example, GPS and satellite information systems are being adapted for use in traditional livelihoods, such as reindeer herding practices. The use of GPS collars to track reindeer provides data with exact coordinates that are useful for locating the herd (Reindeer Herders' Association, 2015, p. 6), but the data is also useful for herders to use in mapping pasture circulation (Pöyry, 2015).

Increasingly, information technology is used as a supporting tool to promote numerous services by replacing physical public service infrastructures. In the EHN, the promotion of such services is evidently being increased as the region faces de-population as a result of the continued out-migration of the younger population, and thereby requires better and efficient support services. As a result, a digital public service support system, in particular for a growing older population, is becoming an obvious necessity. It is also partly caused by the push to adopt digital mechanisms in order to both promote effective services and reduce public expenditure on those services. Health care, education and financial sectors in the EHN are increasingly taking place online and people's everyday needs are shaped around this. In the region, digitalization is taking over the services needed for humans' and communities' continued existence and prosperity. An increasingly technology-dependent, but less environmentally resilient, EHN community is becoming a regional reality. The fulfilment of the region's needs is integrally connected to digital infrastructure; the uninterrupted functioning of such an infrastructure is hence a precondition for communities to function.

Finnish Lapland has set specific goals through a project called "Digital Lapland is Reality – the Lapps are digi skilled and the world is in anyone's reach" aiming at de-

veloping location-independent work, services and education by 2040 (Holopainen, Jokikaarre). Recently, construction work in Lapland to establish 4G connections for the promotion of better information networks was completed. However, because new base stations have not been constructed, shadow areas exist in mobile connections in different parts of Lapland (Holopainen, Jokikaarre). The construction of base stations or other modern physical support infrastructures is generally carried out during summer months only. This is due to the climatic peculiarity of the EHN and therefore the timeframe for such infrastructure development is often too short. The climate is a hindrance to implementing physical infrastructures. On the one hand, the unpredictable and extreme climatic conditions prevailing in the region threaten the stability of its physical critical infrastructures and their uninterrupted functioning, and on the other hand any disruption or malfunction of such infrastructures e.g. because of a cyber-attack, will cause devastating effects on humans and communities. For example, climate change in the region impacts hydropower production as changes in precipitation influence inflow, storage and production. Distribution networks may be affected because of poor infrastructural conditions (Eskeland, Flottorp, 2006, p. 85). Thawing permafrost may also have potential impacts on the physical structures that digitally support the functioning of infrastructures in favour of human needs. As a result, extreme climatic conditions prevailing in the EHN would require more stable and climate-resilient digital structures and infrastructures capable of sustaining climate change-induced threats. Moreover, malfunctioning physical information installations or critical infrastructures, either due to a climatic catastrophe or cyber-attack, would require replacement or repair, which in the fragile EHN climatic context is extremely critical and complex, as well as expensive and time-consuming. Therefore, in addition to climate-resilient infrastructures, strengthening security measures to counter any cyber-attacks on critical infrastructures should be a strategic priority in

order to eliminate potential human security threats arising out of digital disruptions or malfunctions.

Conclusion

The implications of climate change threaten the stability of critical infrastructures. Critical infrastructures are dependent on technology to function. These infrastructures are operated through digital means and supported by required physical structures. The most crucial for these structures to function is to have infrastructures capable of being sustained in response to environmental change as well as threats arising out of cyber security threats. The most basic human needs, such as water and energy supply, as well as service sectors such as health, economy and education, are increasingly becoming digitalized and technology-dependent. Consequently, an emerging technology-dependent human community faces challenges that can be translated into human security threats once there is a failure or disruption in the continued functioning of critical infrastructures. This article examined the context of human security from the perspective of the interlinked implications of climate change and cyber security regimes and from the viewpoint of the EHN region. The findings herein suggest that, due to the climatic peculiarity of the region, the placement of climate-resilient, secure and sustainable critical infrastructures is necessary for a sustainable EHN community to prosper. The continued functioning of these infrastructures will not only meet critical human needs in prevailing regional conditions, but will also provide an opportunity for innovation and prosperity. It is within this context that the climate change regime, cyber security and human security frameworks are inter-connected in the EHN context.

REFERENCES

Allen, D. (2014) *Climate Change and Cyber Threats: Acknowledging the Links*. The Center for Climate and Security. Available at https://climateandsecurity.org/2014/09/08/climate-change-and-cyber-threats-acknowledging-the-links/, accessed November 23, 2018.

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5–26. https://doi.org/10.1017/S0260210597000053

Booth, K. (2005). "Introduction to Part One", in: Booth, K. (Ed.). *Critical security studies and world politics*. Boulder, Colo: Lynne Rienner Publishers.

Burgess, J. P., and Sissel, H. J. (2008). *The influence of globalization on societal security: the international setting*. PRIO Policy Brief 3. Available at https://www.prio.org/utility/DownloadFile.ashx?id=176&type=publicationfile, accessed November 23, 2018.

Burgess, J. P. (2017). "Posthuman Security" *European Journal of Human Security, 1*, 63-73.

Cilliers, J., & African Human Security Initiative. (2004). *Human security in Africa: a conceptual framework for review*. Pretoria: African Human Security Initiative. Available at https://www.africaportal.org/publications/human-security-in-africa-a-conceptual-framework-for-review/, accessed November 23, 2018.

Commission on Human Security (Ed.). (2003). *Human security now: protecting and empowering people*. New York. Available at https://reliefweb.int/sites/reliefweb.int/files/resources/91BAEEDBA50C6907C1256D19006A9353-chs-security-may03.pdf, accessed November 23, 2018.

Eskeland, Gunnar S. and Flottorp, Line Sunniva. (2006). "Climate change in the Arctic: A discussion of the impact on economic activity," Statistics Norway:

The Economy of the North. https://www.ssb.no/a/english/publikasjoner/pdf/sa84_en/kap6.pdf

Holopainen, Päivi and Jokikaarre, Pirita. The Effects of Digitalisation on Different Industries and on the Region – Case Lapland. http://luotsi.lappi.fi/c/document_library/get_file?folderId=683161&name=DLFE-30483.pdf

Hoogensen, G. (2012). Security by any other name: negative security, positive security, and a multi-actor security approach. *Review of International Studies*, *38*(04), 835–859. https://doi.org/10.1017/S0260210511000751

Hoogensen, G., & Rottem, S. V. (2004). Gender Identity and the Subject of Security. *Security Dialogue*, *35*(2), 155–171. https://doi.org/10.1177/0967010604044974

Hossain, K., Roncero Martin, J. M., & Petrétei, A. (Eds.). (2018). *Human and societal security in the circumpolar Arctic: local and indigenous communities*. Leiden ; Boston: Brill Nijhoff.

Hossain, K. (2017). "Security – a Shared Concept? Are the Sámi legitimate actors in the securitization move?", pp. 9-18, in: International Conference on Human Security, Stanarević, S., Đorđević, I., Rokvić, V., (Eds.). (2017). *3rd International Conference on Human Security, [Belgrade, May 2017].* Belgrade: *Faculty of Security Studies, Human Research Center*.

IPCC (2018). "Global warming of 1.5°C Summary for Policymakers". Intergovernmental Panel on Climate Change. https://report.ipcc.ch/sr15/pdf/sr15_spm_final.pdf.

Jano, D. (2009). Aspects of Security 'Dilemma': What We Have Learned from the Macedonian Case. *Perceptions: Journal of International Affairs*, *14*, 73–90. http://sam.gov.tr/wp-content/uploads/2012/01/Dorian-Jano.pdf, accessed November 23, 2018.

Kerr, P. (2016). "Human Security", in: Collins, A. (Ed.). (2016). *Contemporary security studies* (Fourth

edition). Oxford, United Kingdom ; New York, NY: Oxford University Press.

Lehto, M., Huhtinen, A. & Jantunen, S. (2011). "The Open Definition of Cyber: Technology or a Social Construction?" International Journal of Cyber Warfare and Terrorism. Vol. 1 (2).

Liaropoulos, Andrew (2015). "Cyber-Security: A Human-Centric Approach", Proceedings of the 14th European Conference on Cyber Warfare & Security, University of Hertfordshire, Hatfield, UK, 2-3 July 2015

McCormack, T. (2008). Power and agency in the human security framework. *Cambridge Review of International Affairs*, *21*(1), 113–128. https://doi.org/10.1080/09557570701828618

N2 Consultans. (2015). *The Link: CyberSpace and The Climate: Our False Sense of Security Climate Change and Cyberthreats.* N2 Consultants.

Owen, T. (2004). Human Security - Conflict, Critique and Consensus: Colloquium Remarks and a Proposal for a Threshold-Based Definition. *Security Dialogue*, *35*(3), 373–387. https://doi.org/10.1177/0967010604047555

Paris, R. (2001). Human Security: Paradigm Shift or Hot Air? *International Security*, *26*(2), 87–102. https://doi.org/10.1162/016228801753191141

Pöyry (2015). "Utilising Reindeers' GPS-collars in Project Planning". http://www.poyry.fi/sites/www.poyry.fi/files/media/related_material/reindeers_gps-collars.pdf

Reindeer Herders' Association (2015). Reindeer herding and large carnivores Socio-economic effects. http://ec.europa.eu/environment/nature/conservation/species/carnivores/pdf/sosioeconomic_aspects_finland.pdf

Ruiz De Garibay, D. (2007). Securing Humans in a Dangerous World. *Human Security Journal*, *3*, 1–23. Available at https://www.academia.edu/7114024/_

La_S%C3%A9curit%C3%A9_humaine_et_l_internationalisation_des_conflits_intra-%C3%A9tatiques_le_cas_du_conflit_au_Sud-Soudan_, accessed November 23, 2018.

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record*, *54*(02), 108–118. https://doi.org/10.1017/S0032247418000268

Shackelford, S. (2015). On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2630333

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

UNDP (Ed.). (1994). *Human development report 1994*. New York: Oxford Univ. Press. Available at http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf, accessed November 23, 2018.

UNGA. (2005). *In larger freedom: towards development, security and human rights for all. Report of the Secretary-General.* United Nations. Available at https://www.globalpolicy.org/images/pdfs/followupreport.pdf, accessed November 23, 2018.

University of British Columbia (Ed.). (2005). *Human Security Report 2005. War and Peace in the 21st Century*. New York: Oxford Univ. Press.

Werrell, Caitlin E. and Femia, Francesco (2015). "Climate Change as Threat Multiplier: Understanding the Broader Nature of the Risk", Briefer, The Centre for Climate and Security. https://climateandsecurity.files.wordpress.com/2012/04/climate-change-as-threat-multiplier_understanding-the-broader-nature-of-the-risk_briefer-252.pdf