 Polar Record 54 (275): 108–118 (2018). *© Cambridge University Press 2018.* *doi:10.1017/S0032247418000268*

Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North

Mirva Salminen
The Northern Institute for Environmental and Minority Law at the Arctic Centre, University of Lapland, Rovaniemi, Finland (mirva.salminen@ulapland.fi)

Kamrul Hossain
The Northern Institute for Environmental and Minority Law at the Arctic Centre, and Faculty of Law, University of Lapland, Rovaniemi, Finland

Received October 2017; revised version received April 2018; accepted April 2018; first published online 25 June 2018

ABSTRACT. Overarching digitalisation is producing significant socio-cultural, economic and policy changes in the European High North. These changes create new opportunities, but also challenges and concerns for people and communities living in the region. Digital development is guided by supranational, national and regional digital policies and is secured through national cybersecurity agendas. These frameworks concentrate on advancing overall economic growth and safeguarding critical information infrastructure and information security, but pay inadequate attention to the interests, needs and fears of people and communities experiencing digitalisation in everyday life. In order to generate a more comprehensive cybersecurity agenda, which focuses on human security and empowering people to influence the digital development, a research framework highlighting the actual ways people use, wish to use, or are unable to use information and communication technologies is needed. The focus of this article is therefore on regionally contextualised digital opportunities and threats as they may be experienced by local people and communities. It utilises insights of securitisation theory to grant people a say in the direction of digital development in their region. The aim is to introduce issues of human security to cybersecurity agendas, for a more comprehensive understanding of the societal changes that digitalisation generates.

Introduction

Digitalisation is changing societies rapidly and is therefore attracting increased regulatory attention. Numerous studies and policy papers describe the ongoing development, and explicate policies to facilitate digitalisation but also to mitigate its (potentially) harmful effects. These policies, developed in national capitals, aim at sustaining overall economic growth, advancing the information society, ensuring national security, and enhancing service provisioning. By contrast, they pay little attention to the interests and needs of people and communities living in so-called developing regions within a country. Most commonly, these people and communities are treated merely as objects of development, whose lives digitalisation is expected to improve.

This article presents a novel framework for analysis, bringing together human security and securitisation approaches, national digitalisation and cybersecurity policies, as well as regional perspectives to encompass an understanding of the effects of digitalisation on everyday life in the European High North (EHN). It focuses on digital development in the northernmost parts of Finland (Lapland), Sweden (Norrbotten) and Norway (Finnmark, Troms and Nordland). It serves as an introduction to the research project "Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy)", which critically interrogates the presumptions on which digital development is based and the trajectories it is expected to take. The article raises important concerns over ownership and stakeholdership in the evolution of human well-being in the rapidly digitalising region. It utilises policy papers and reports extensively, as there is little research literature available on the topic.

The article scrutinises the EHN as an entity with particular characteristics and connections across national borders. Digitalisation takes place under three national regulations – those of Finland, Sweden and Norway – and is secured within three national cybersecurity frameworks supported by Nordic, European and global cooperation. The aim of these frameworks is to safeguard the functioning of society through improving critical infrastructure protection and information security. Existing regulation and the security measures it enables focus primarily on ensuring digital development (positive security) and mitigating its harmful effects (negative security) within each society. Regional development, again, is on the agendas of the associations of local and regional authorities, regional or county councils, municipalities, and ad hoc cooperative bodies. Structural cross-border digital development in the EHN is scarce, if not completely absent. More importantly, there is a lack of visibility of local conditions articulated in national policies as, for example, cybersecurity strategies are chiefly concerned with ministerial level decision making.

Within the rearticulated research framework, cybersecurity may be redefined to integrate human security dimensions, and digitalisation refocused to support development defined by the people and communities themselves. Thus it becomes possible to examine the connections and potential problems between digitalisation, economic development, environmental threats, societal concerns, and

cybersecurity. This article identifies important questions for future study, as cybersecurity has been little examined within the human security framework. Similarly, questions of human security have rarely been addressed on cybersecurity agendas (Dunn Cavelty, 2013). We suggest that refocused and redefined cybersecurity can better support inclusive digitalisation in the European High North.

The article consists of four parts. First, it contextualises digital development taking place in the EHN with regard to national and regional societal steering of digitalisation. It argues that rethinking digitalisation and cybersecurity policies from a regional, instead of national, policy can improve the integration of people's and communities' interests, needs and fears into decision making. Second, the article describes the theoretical framework that can be utilised as a basis for this kind of rethinking. In so doing, it brings together theories on digitalisation, cybersecurity, human security, human rights and securitisation. Third, it considers topical questions and concerns regarding digitalisation and cybersecurity in the EHN. The fourth part summarises the article.

Emphasising regional focus over national policies in the digitalisation of the European High North

Digitalisation of the European High North is taking place within the global networks of internet governance, industrial standardisation, and intergovernmental organisations, such as the International Telecommunication Union (ITU). By the time of writing, the main Arctic governance organisations, such as the Arctic Council or the Barents Euro-Arctic Council, had indicated only modest interest in digitalisation and cybersecurity. However, the newly established Arctic Economic Council (AEC) has shown initiative and run a special working group on telecommunications. The working group published its "Arctic Broadband" report in January 2017 (AEC, 2017). The AEC has also organised an annual Top of the World Arctic Broadband Summit since 2016, which aims to bring together "business executives, policy decision makers, representatives of academia and tech industry experts to discuss the opportunities and challenges of connectivity in the Arctic" (AEC, 2018). Connectivity is one of the four priorities of the Finnish chairmanship of the Arctic Council for the term 2017–2019 (the other priorities being environmental protection, meteorological cooperation, and education) (Ministry for Foreign Affairs, 2016). Similarly, digitalisation is one of the main themes of the Swedish presidency of the Nordic Council of Ministers for 2018 (Nordic Council of Ministers, 2017). In addition, the North Atlantic Treaty Organization is highly active in cybersecurity and recognises the increasing strategic importance of the Arctic region. It is not irrelevant in which context and by whom the topic is discussed, as the framing directs ways of defining the problem and of developing solutions to it (Finnemore & Hollis, 2016). If digitalisation in the EHN is presented merely from a technical, economic or strategic point of view, the interests, needs and fears of people and communities remain unheard and therefore unaddressed. This neglect causes uncertainty, anxiety, frustration or even anger, when people feel that they have little chance of influencing the direction of digital development that affects their everyday life.

Principal actors contributing to digitalisation and cybersecurity in the EHN are the European Union (EU) and the Nordic countries. In practice, regional administrations such as the Regional Council of Lapland, the County Council of Norrbotten and the counties of Nordland, Finnmark and Troms play a significant role in developing information infrastructure and digital services, channelling state or EU funding to projects, as well as coordinating cybersecurity arrangements by applying national strategies locally. This article examines only the national and regional digitalisation and cybersecurity frameworks. The following strategies have been included in the study:

Norway: Digital Agenda for Norge 2015–2016. IKT for en enklere hverdag og økt produktivitet [Digital Agenda for Norway 2015–2016. ICT for a simpler everyday life and increased productivity] (2016); Nasjonal strategi for informasjonssikkerhet (CSSN) [Cyber Security Strategy for Norway] (2012); Digitaliseringsstrategi 2013–2016 for kommuner og fylkeskommuner [Digitalisation strategy 2013–2016 for municipalities and counties] (2013); and Digitaliseringsstrategi. Finnmark fylkeskommune 2015–2018 [Digitalisation strategy of Finnmark county] (2015). Troms and Nordland do not have a digitalisation strategy online.

Sweden: It i människans tjänst – en digital agenda för Sverige [ICT for Everyone – A Digital Agenda for Sweden] (2011); Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten [Cybersecurity in Sweden. Strategy and measures for secure information in central government] (2015); Nationell strategi för samhällets informations och cybersäkerhet (NCSS) [A National Cyber Security Strategy] (2016); and Digital Agenda. Norrbotten (2013).

Finland: Tuottava ja uudistuva Suomi – Digitaalinen agenda vuosille 2011–2020 [Productive and inventive Finland. Digital Agenda for 2011–2020] (2011); Suomen kyberturvallisuusstrategia (FCSS) [Finland's Cyber Security Strategy] (2013); Maailman luotetuinta digitaalista liiketoimintaa – Suomen tietoturvallisuusstrategia [Information Security Strategy for Finland. The World's Most Trusted Digital Business Environment] (2016); and Lapin digiohjelma 2020 [Digitalisation programme for Lapland 2020] (2013).

According to national strategies, everyone has a role to play in the processes of digitalisation and in its safeguarding. Information and communication technologies (ICTs) are perceived as a general-purpose technology, whose benefits are network benefits and hence cannot be produced by other means (Ministry of Local Government and Modernisation, 2016). Therefore, cooperation and coordination within and between government branches,

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

between all stakeholders in society, as well as internationally, need to be improved. Everyone's actions affect (in)security and (un)trustworthiness of the globally interlinked digital environment and everyone is affected by the activities of others. The state plays a central coordinating role, as its main task is to provide good conditions for the utilisation of digital opportunities. It carries out this role by reforming regulations, formulating clear policy goals, removing obstacles to positive development, funding research, promoting networks and connections, and protecting society from grave cybersecurity threats that may endanger the functioning of society and the economy. (See the Nordic strategies.)

Unlike in the development of national strategies, people and organisations based in the EHN have reportedly had a chance to participate in the framing of regional digitalisation policies (Lapin liitto, 2013; Norrbotten, 2013). The regional agendas have eight characteristics in common. First, they repeatedly emphasise the urgency of improving information infrastructure and connections in the EHN for the benefit of local people, communities, businesses and administration. Second, they emphasise the role of ICTs in the overall societal and economic development. Third, they highlight the need to fit digital services to user needs and the demand for new, flexible services that are easy and secure to use. Fourth, digitalisation ought to ease everyday life in the region. Fifth, decision making around digitalisation should facilitate the development of local businesses into skilled utilisers of digital opportunities. Sixth, educational institutes in the region should be allocated the resources necessary for self-development towards digital forerunners. Seventh, digitising the administration requires reformed thought and operating models. Finally, solutions based on open data and open source code are to be favoured and supported. (See regional strategies.)

As the challenges faced and the solutions developed for overcoming them are similar throughout the EHN – in both national and regional policies – the primacy of national over regional development can be questioned. Firstly, a national focus on data production, analysis, decision making and the following policies – in both public and commercial sectors – masks regional digital divides, threats and fears, and their consequences in people's everyday life. Regional voices raise concern over lacking mobile telephony, or restricted access to the digital environment, and even though programmes to develop information infrastructure have been running since the 1990s, problems exist in areas that are perceived as being most difficult or least profitable to connect (personal communication with representatives of the Regional Council of Lapland, Lapland Hospital District, and the Centre of Excellence on Social Welfare in Northern Finland at the Arctic Centre, University of Lapland, 15 August 2016). In addition, available services do not necessarily meet the needs of people and communities living in developing regions of the Nordic countries, as they have not been developed with their needs in mind. Moreover, they may not meet the specific needs of any customer, as the basis for their development and adoption lies most commonly in administrative processes (Lapin liitto, 2013).

Secondly, regional political, socio-cultural or economic tensions do not easily transmit to nationally focused decision making, as they are perceived to be marginal, concerning only a small number of people or a fragment of the market or economy. They may be experienced as far-away problems, and less important than potentially highly damaging problems that concern the majority of the population or a significant share of the national economy. Yet regional challenges posit people and communities to either beneficial or detrimental positions in information society, with access and ability to act safely in the digital environment becoming a divider between insiders and outsiders. Problems that may seem marginal from the hub's perspective stand in the way of regional development and the utilisation of opportunities provided by digitalisation.

It should be possible therefore to consider the northernmost regions of the Nordic countries as an entity in which digitalisation is supported and secured through a shared regional framework rather than three national ones. Infrastructural development, product and service provision, as well as education and training could be organised on a regional basis so that they truly respond to the interests, needs and fears of people and communities, while taking economic, socio-cultural and environmental characteristics into consideration. Examination of these opportunities usually hits the wall of nationally focused structures, processes and practices, which do not (yet) adapt to the cross-border alternatives facilitated by digitalisation (personal communication with representatives of the Regional Council of Lapland, Lapland Hospital District, and the Centre of Excellence on Social Welfare in Northern Finland at the Arctic Centre, University of Lapland, 15 August 2016). Further, open-minded study of the topic is necessary, and ought to include analysis of existing (potential for) cooperative structures, processes and practices across borders, as well as envision further options based on local perspectives.

An alternative would be to intensify and modify existing national policies so that regional particularities receive the deserved attention. Instead of approaching regional development merely as obligatory expenditure, it should be framed as a way to support human security defined by people and communities for themselves. It would thus facilitate the realisation of human rights, sustainable regional development, advancement of the underlying societal values and, eventually, national cybersecurity through shared ownership, responsibility and accountability. For these purposes, data and analysis of the actual ways in which people and communities use or do not use, and would or would not like to use ICTs for what purposes is necessary (Figuères & Eugelink, 2014). The study ought to include critical examination of the reasons for, justifications of, and expected or unexpected consequences of existing policies and decisions made or not made. It should map existing infrastructures, products

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

and services, and list their lacks and gaps. In addition, it needs to create room for people and communities to envision solutions to regional challenges, as well as to facilitate their realisation.

Digitalisation and cybersecurity: integrating human security dimensions

Problematising the prevailing frameworks of digitalisation and cybersecurity

Digitalisation refers to the ongoing development in which ICTs are increasingly used in virtually all aspects of human life. Their use is gradually turning processes, practices and structures into information-based ones (Brennen & Kreiss, 2014; Kluver, 2000). This development is commonly perceived as a neutral process treating equally everyone who adapts to its conditions. Adaptation requires access and basic skills to use ICTs. Yet digitalisation is neither neutral nor determined by technology, but its appearance and outlook result from human decision making (Crosby, 2016; Mordini, 2014; Webster, 2014).

In policy papers, digitalisation is approached somewhat deterministically (regarding the human ways of relating to technology, see Carr, 2012). ICTs are treated as a force of nature that turns things around for both good and bad. In the development, the old providers of safety and minimum requisites for human life, whose operation was based on physical presence and bureaucratic treatment, are turning into digital facilitators of individual choice operating under strict cost-efficiency pressures (see the Nordic strategies). Economic and political decision making is centralised to globally connected hubs that are able to tap into the flows of information, materials, finance and skilled people (Aaltola, Käpylä, & Vuorisalo, 2014; Castells, 2009, 2010). National information society programmes and digital agendas facilitate transformation, which ought to increase the chances for global connectedness. Opting out is not an option (Kilpeläinen, 2016; Statens Offentliga Utredningar, 2015, p. 23). The prevailing understanding of digitalisation thus leaves in isolation areas without the required information infrastructure and/or resources, as well as people without the necessary skills to benefit from the development (Kilpeläinen, 2016).

When economies and societies become information-based, they are increasingly dependent on functioning critical information infrastructure. This labelling well describes the contemporary role of ICTs: they constitute a structure underlying society and the economy, keeping them running. However, technology is inherently vulnerable (Axelrod, 2004). ICTs are prone to systemic malfunctions, mistakes or neglect in their use, intentional and unintentional abuses, and outside intrusions. Therefore, in order to keep the flows running along favourable routes, critical information infrastructure needs to be safeguarded (Giacomello, 2014; Mayer-Schönberger & Hurley, 2000; Norden, 2013). The recognised criticality of information infrastructure has led to the adoption of the cybersecurity concept. As there is no unanimous definition for the term, national approaches effectual in the EHN are utilised in this article. In principle, cybersecurity refers to the security of the digital environment, which constantly interacts with operations in the physical environment (Limnéll, Majewski, & Salminen, 2015).

In the Nordic context, cybersecurity has been understood as "the desired end state in which the cyber domain is reliable and in which its functioning is ensured", as in Finland (FCSS, 2013, p. 1), or as the "[p]rotection of data and systems connected to the Internet", as in Norway (CSSN, 2012, p. 28). The Swedish information and cybersecurity strategy highlights information, systems used to store and handle information, vital functions to society, and critical infrastructures, as well as the profound values held by the society, as objects to be secured (NCSS, 2016, p. 6). The Nordic countries have two tracks for managing the opportunities and challenges related to digitalisation. On the one hand, digital opportunities and the addressing of digital divides and privacy concerns are situated within the digitalisation framework. On the other hand, the cybersecurity framework concentrates on protecting information and its exchange, critical information infrastructure and national security against cyber threats. One of the goals in redefining cybersecurity is to bring the two tracks together so that (1) the narrow, national security-focused conceptualisation of cybersecurity is broadened to truly address human security dimensions, and (2) the dependence of successful digitalisation on effective, redefined cybersecurity is fully acknowledged.

Human security: placing threats arising from the use of ICTs

The concept of human security has reshaped security discourse significantly since its occurrence in the 1994 United Nations Development Programme's Human Development Report (UNDP, 1994). As a result, the state-centric and sovereignty-oriented approach is no longer the sole viable international security framework. Human security professes security as having both preventive and pro-active tools and introduces a multilevel security structure, which incorporates actors inside and outside the state. This broadened and deepened conceptualisation presents a reformed agenda, which includes various other-than-military forms of instability resulting from, for example, environmental degradation or societal volatility (Davi, 2009). It offers an insightful understanding of what constitutes a threat to whom, even beyond the interstate level (Booth, 2005; Sheehan, 2005).

Human security aims at ensuring freedom from fear and from want, with a view to assuring freedom from indignity for individuals and communities. Fulfilling the basic human needs for survival stands at its heart (UNDP, 1994). This prerequisite goes hand in hand with the established normativity of human rights framework: the fulfilment of basic human needs is guaranteed by the means of enjoyment of universal human rights (Kaldor, Martin, & Selchow, 2007). As a policy tool, human security, while reflecting human rights norms, offers an

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

emancipatory and empowering framework to address urgent issues in specific situations (McCormack, 2008). It is a paradigm that centres on the human being and recognises that threats may arise from a number of sources (Buzan & Hansen, 2009; Davi, 2009.) Its underlying point suggests that protected people can exercise choice and, once empowered, they are capable of both avoiding risks and improving the system of protection (Commission on Human Security, 2003). In addition, it acknowledges that certain threats affect people and communities regardless of whether debates over them can be labelled as existential.

While the broad conceptualisation of human security makes the identification of elements falling within and remaining outside of its scope problematic (Paris, 2001, p. 90), the actual goals of the concept are clearly recognised: addressing human vulnerability following from the events that take place around us and developing appropriate response mechanisms based on urgency. Applying human security to digitalisation in the EHN requires a further discussion integrating human rights and securitisation.

Cybersecurity is a means to protect human rights offline. In the information society, the realisation of human rights depends on functioning critical infrastructures controlled through and/or running on information infrastructure (e.g. Figuères & Eugelink, 2014). Mis- or dysfunctioning infrastructures constitute a threat primarily because of the second- or third-order consequences felt by individuals and communities in everyday life, which are caused by disruption or halting of functions such as electric supply, money transfer or logistics (e.g. Finnemore & Hollis, 2016). Lacking cybersecurity, and similarly lacking access to the digital environment, can be perceived as a threat to the realisation of human rights (Skepys, 2012).

However, cybersecurity understood merely as the protection of information and infrastructure risks neglecting the protection of human rights online; especially when preparations for an emergency are carried out or when such a situation (actual or imagined) arises. The Nordic cybersecurity strategies acknowledge and commit to the protection of digital rights such as freedom of opinion, expression and assembly, and the right to privacy, while also emphasising the overarching values of democracy, good governance and equality. Yet the intensifying pressure for improving intelligence collection and analysis in the face of increasingly complex security threats cannot be ignored. In addition, commercial information collection, for example, about people's interests, browsing habits, and social media behaviour is global. This information is not only valuable to website administrators and digital service providers but can also be sold, for example, to marketing companies or to anyone willing to pay for it (e.g. Marichal, 2012.) The related digital rights concern is that people are not always aware of and/or cannot control what information is collected and to whom it is distributed.

The relationship between human rights and digitalisation is not straightforward. On the one hand, human rights can be used as a political, legal and rhetorical tool against actors who advocate censorship or blocking of online content, criminalise legitimate content, use cyber-attacks on political opponents or economic rivalries, or neglect the protection of privacy and data in general (e.g. UNHRC, 2011). On the other hand, the United Nations (2011) and some countries, including Finland (2008), have declared free (from technical, political, linguistic or economic constraints, and surveillance) internet access to be a human right.

Unlike the human security framework, which does not explain how an issue becomes a security concern, securitisation theory suggests a process-oriented approach to understanding security. Security is claimed as a social construct by virtue of a speech act. In the process, an issue that gains enough attention from its audience becomes a security threat going beyond the normal political process. Thus, the potential use of extraordinary measures becomes reality. Consequently, emergency measures are taken to return the issue to the political process so that the threat is stabilised (Buzan, Wæver, & de Wilde, 1998; Buzan & Waever, 2003). The prevailing cybersecurity framework, on the one hand, establishes actors from individuals, corporations and other organisations to states and multinational groupings as security threats (e.g. Limnéll et al., 2015; Singer & Friedman, 2014). On the other hand, technical operations such as malware, phishing, ransomware, cracking or code injection can be defined as threats (e.g. ENISA Threat landscape reports). The choice of discourse utilised depends on the audience.

Threats identified within the human security framework do not follow the afore-described securitisation logic. The point at which a threat matures is unknown and undefined, resulting in confusion and perplexities in the relationship between human security and human rights (Davi, 2009). While such confusion may undermine human rights norms because of the employment of the under-conceptualised notion of human security framework (Davi, 2009), we consider that the analytical approach of human security is significant in identifying the particularities embodied in the normative structure of human rights framework. Hence, the human security concept plays an important role in analysing patterns of political violence, major human rights violations, and the structural sources of insecurity and vulnerability. While the human security approach is argued to be relatively less persuasive than securitisation theory, which comprehends a "whole spectrum of security relations across the interplay of actors, sectors and levels" (Davi, 2009), we are convinced that threats also arise from everyday situations and nebulous sources (Burgess & Sissel, 2008). Therefore, by combining these approaches in the examination of digitalisation in the EHN, it is possible to strive towards a redefinition of cybersecurity that takes regional particularities into consideration, and takes the aim of empowering people and communities seriously.

When the existing digitalisation and cybersecurity frameworks concentrate on economic opportunities and

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

efficiencies, as well as threats to national security, they miss the by-product processes of digitalisation, which generate fear and concerns amongst people and communities in the EHN. For instance, digitalisation is promised to guarantee the realisation of everyone's right to equal access to public services but it cannot reach that goal as long as there are gaps in information infrastructure and people's digital know-how. Without the realisation of everyone's right to a set standard of living, employment or social security, participation in the information society becomes difficult. An ability to pay for the required equipment and digital connection or an ability to travel to places where public internet access is provided is currently a condition of digital participation. Moreover, digitalisation does not treat all cultural groups similarly, for which reason its impacts on inclusion and exclusion should be examined. In the EHN, this concern relates most visibly to the different Sámi groups and linguistic minorities living throughout the region.

A widened and deepened cybersecurity framework focusing on the human being can better address the underlying challenges faced by digitalising societies. Instead of only pointing out the human being as the weakest link of cybersecurity, it concentrates on facilitating human development, advancing the interests and mitigating the fears that people encounter in everyday life. It treats individuals and communities as active security producers instead of perceiving them merely as passive receivers of security. It also highlights the importance of providing ways for people to have a say in digitalisation and protect themselves in the digital environment. Eventually, the development will feed into the state-centric and sovereignty-oriented security approach in the form of improved national and economic cybersecurity.

Characteristics of digitalisation and cybersecurity in the European High North

The EHN has a complex system of socio-cultural, political, economic and environmental dynamics linking actors from inside and outside the region, with both local and global implications. For instance, as a sparsely populated region with pristine environmental characteristics, which is simultaneously rich in natural resources, it attracts human activities such as oil and gas development in marine areas or inland mining and mineral activities. These activities are detrimental to the environment and also invite negative digital attention in the form of attempted network and system intrusions or information thefts and possibly subsequent blackmailing for both economic and ideological reasons. Digital solutions may serve as a partial solution to environmental problems, but they may also feed into such problems, for example, due to the production processes of ICTs, increased local energy consumption or pollution caused by misfunctioning of automated industrial processes. A sustainable solution achieving a proper balance between detrimental human activities and digital potentials can mitigate problems related to climate change and other environmental threats.

In addition, the EHN inhibits unique groups, such as the Sámi indigenous communities, with particular needs for sustaining a distinct identity. It is important to examine how digitalisation adapts or does not adapt to the prevailing conditions in these communities. Subsequently, it is necessary to search for the means to address local fears, needs and interests in the most suitable and considerate way: how can digital development improve human security when adapted to local conditions? Globalisation and the emergence of new economic opportunities have resulted in significant potentials for the region. These potentials will be addressed in more detail in the following paragraphs. Yet the EHN has a limited and fragmented information infrastructure, and people's skills and confidence to act in the digital environment vary, which makes economic development challenging and always costly (Norrbotten, 2013); personal communication with representatives of the Regional Council of Lapland, Lapland Hospital District, and the Centre of Excellence on Social Welfare in Northern Finland at the Arctic Centre, University of Lapland, 15 August 2016). Digitalisation thus affects human interests, needs and fears from a number of perspectives, making human security an applicable analytical tool to explore the digital development.

Commonly acknowledged opportunities and challenges residing in digitalisation become intensified in the EHN due to the region's characteristics. Positive digital development comes in the form of, for instance, increased efficiencies in production, administration and service provision; novel and transformed operating models, livelihoods, and potentials for lessening human error; platforms for self-expression and cultural identity formation; increased transparency, as well as information collection, storage and exchange; and improved access to knowledge (see the Nordic strategies; also Sartor, 2013). A cold, yet warming, climate; vast distances; a sparse population, which is gradually concentrating in urban centres; a diminishing and ageing population; an economy divided between traditional livelihoods, small-scale production, the tourism and experience industry, resource extraction, high- and cold-tech industries, as well as a relatively large public sector; and the coexistence of different cultural identities generate twists and context-bound particularities in the presumably neutral processes of digitalisation (Larsen & Fondahl, 2014). Therefore, the region often serves as a test bed for innovations and solutions that are later adopted in wider use (Lapin liitto, 2013; Norrbotten, 2013). An example of such testing activity is the AURORA project in the Kolari-Muonio area of Finland. The aim of the smart road experiment is to increase traffic safety in the difficult conditions of the Arctic winter through increased utilisation of sensors, automation and information sharing (Finnish Transport Agency, 2016).

Threats to critical infrastructures and functions vital to society, which are well covered in national strategies (cyber activism, espionage, terrorism, crime and warfare),

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

endanger human security in the information society. Yet they are not the only threats.

> The term digital divide refers to the gap between people with effective access to digital and information technologies (…) and those with very limited or no access at all. (…) Digital divides also exist along wealth, gender, geographical and social lines within States. (…) [P]eople in rural areas are often confronted with obstacles to Internet access, such as lack of technological availability, slower Internet connection, and/or higher costs. Furthermore, even where Internet connection is available, disadvantaged minorities, such as for example disabled people, often face barriers to accessing the Internet in a way that is meaningful, relevant and useful to them in their daily lives (UNHRC, 2011, p. 17; also Cruz-Jesus, Oliveira, & Bacao, 2012.)

These reservations apply to the digitalising of the European High North as well.

Ubiquitous digitalisation has the potential to address existing human inequalities. For example, in the EHN education and training can be provided digitally to a greater number of pupils and students regardless of their physical location. Digital public services remove the restriction of having to visit an authority within office hours. Dealings with health professionals, social services or tax authorities, for example, can be carried out online. This reduces the need to travel and, thus, the environmental burden and travel costs. The option of distance work amidst natural beauty is expected to lure more people into the region (see regional strategies). However, the mere existence of interconnected networks and online services does not automatically diminish inequalities (Figuères & Eugelink, 2014). On the contrary, it can also enhance them. Decision making supporting positive development and active policies to bridge digital divides are thus required. Those best able to describe the divides, and how to address them, are the ones experiencing them. Well-meaning attempts may turn into a waste of time and money if people do not feel comfortable with the options provided (Kilpeläinen, 2016). In order to improve the existing situation, a widened digital ownership is required.

Little systematic research on digital divides between or within the Nordic countries is available (for existing research see Kilpeläinen, 2016; Räsänen, 2008; Taipale, 2012). In general, they are considered to be highly developed information societies. For example, on the European Union Digital Scoreboard their standings are above the EU average. Fixed broadband connection is available to almost everyone (99% of homes in Sweden, 97% in Finland and 95% in Norway) and 4G access is making its way through (available to 76% of homes in Sweden, 75% in Finland and 80% in Norway). In Sweden, 89% of the population uses the internet frequently and 72% has basic digital skills. In Finland the figures are 91% and 75%, respectively, and in Norway 96% and 80%. E-government services are utilised by 49% of the population in Sweden, by 63% in Finland and by 59% in Norway. Whereas the connection price in Finland is the second lowest in the entire EU, the connection price in Norway is above the EU average (EU Digital Scoreboard, Progress by Country reports as in 2016).

However, aggregated figures tell little about the regional, socio-cultural, economic or other digital divides within these countries. The existence of digital divides is acknowledged in the Nordic countries. Usually, they become addressed through special policies and by setting legal obligations, for example, to service providers (see, for example, the national and regional broadband programmes in the Nordic countries and the accessibility programme and reports of the Finnish Ministry of Transport and Communications 2005–2015). Providing connections to and reaching disconnected people has proven financially and attitudinally difficult (Norrbotten, 2013). This constitutes a considerable threat to human security in information societies where digital services are the main form of communication between public authorities, businesses and organisations, and the residents (Kommunenes Sentralforbund, 2013; Ministry of Transport and Communication, 2011).

The aforementioned issues have not usually been addressed in the language of security but of development, equality, quality of life, and self-cultivation/expression. They have been perceived as being less urgent than digital espionage, potentialities of cyberwar or cyber terrorism. However, they pose threats to human security, as people may be afraid of engaging in the digital environment because of a lack of skills, may not have access to it, or may not have the know-how to critically evaluate available information and are thus vulnerable to being misled. As being able and feeling confident to act in the digital environment is an everyday security consideration in the information society, these issues should be located on the agenda to which they belong.

Of the threats recognised in the cybersecurity framework, cybercrime – and digital abuse, which often borders cybercrime depending on national legislation – is what individuals are most commonly aware of. The term refers to illegal activities that are either dependent on or enabled by the use of ICTs. The former include technical operations, such as malware for financial gain and theft of personal or organisational information, which would not be possible without computers and networks. The latter comprises activities that can be carried out both online and offline, but the scale or nature of which has changed due to the use of ICTs, for instance, fraud and illegal drug trade (Limnéll et al., 2015; National Crime Agency, 2016).

The effects of cybercrime can be felt directly in everyday life and can restrict people's willingness to act online. Over the years, cybercrime has become more common, sophisticated, professional and organised. Nonetheless, people still fall victim to simple online scams or hand over their personal details surprisingly easily. Those lacking awareness are particularly easy targets, whose deception does not require advanced technical skills. For example,

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

only 35% of consumers in the Nordic countries believe that they have a full awareness and understanding of the consequences of data breaches; 52% believe they have a partial understanding and 12% declare they have little or no understanding (FireEye, 2016).

In principle, what constitutes a crime in the offline environment is also a crime in the online environment. Thus, novel legislation has been developed only for borderline cases, and existing legislation and law enforcement have been applied as a rule. However, cybercrime retains its attractiveness because of the perceived low risks of detection and prosecution (Clough, 2010). There are no studies focusing on cybercrime in the EHN, but some reports on the Nordic countries exist. According to FireEye (2015), regional traits such as natural resources, innovations in healthcare and renewable energy, a high level of connectedness and high-tech industry, a strong shipping industry, as well as transparent governance make them targets of hostile cyber activities. Similarly to national strategies and policies, these reports address threats merely at the national and organisational levels, ignoring fears experienced by people and communities. Less attention is given to digital piracy, fraud, scams, illegal, harmful and offensive online content, and, in general, the victimisation of individuals and ethnic or cultural groups (cf. Yar, 2006). Yet these phenomena are important for inclusive digital development.

Digital abuse involves the use of ICTs to bully, intimidate, harass or stalk another person. It often takes the form of verbal abuse, social manipulation or disclosing of sensitive content publicly online. People engaging in digital abuse do not generally acknowledge breaking any laws or moral codes but utilise the means they are familiar with, such as social media and instant messaging. Yet it should be recognised that, for example, hate speech or stalking are always criminal offences (Clough, 2010; Yar, 2006). In the EHN, hate speech (delivering a message of racial inferiority, directed against a historically oppressed group and of hateful or degrading nature (Yar, 2006)) against an ethnic and/or cultural group may be considered to be a high-likelihood phenomenon, even if systematic studies have not yet been carried out.

Refocusing cybersecurity and bringing people and communities to the forefront so that cyber threats to critical information infrastructure and cybercrime are realigned with the questions of digital divides and digital abuse facilitates the establishment of a truly comprehensive cybersecurity agenda. On such an agenda, for instance, security and privacy no longer need to be perceived as opposing one another such that a balancing act is required (cf. Taddeo, 2013; Yar, 2006), but as mutually reinforcing and complementary aspects of cybersecurity (e.g. NCSS, 2016). This shift enables and enhances the attainment of human security and the protection of human rights in digitalising societies. How to define cybersecurity; what to include in the cybersecurity agenda; as well as what kind of processes, practices and structures to build for security production are human decisions taken today. However, they also define the outlook of digitalised EHN for a long period of time.

Conclusion

Digitalisation of the European High North takes place within supranational, national and regional frameworks. It is supported and secured through programmes that serve aggregated national and supranational interests in the name of the functioning of society and economic growth. Whether these policies help realise the opportunities and/or mitigate the threats residing in regional digital development has thus far been given inadequate attention. Deterministic expectations and assumptions about the neutrality and transformative power of technology overrule examination.

In order to address the existing gaps in knowledge and thus improve the targeting, inclusivity and effectiveness of both public and commercial policies in the developing regions of the Nordic information societies, a comprehensive study of digitalisation and cybersecurity from the human security perspective is crucial. The identification of opportunities and threats, as well as the ways to support positive developments while mitigating negative ones, ought to be carried out in cooperation with people and communities living in the EHN. The aims should include identifying processes through which digital threats rise onto the cybersecurity agenda, finding ways to incorporate threats to human security in the agenda, and focusing on the advancement of human development and the empowerment of people to direct digitalisation so that it serves their interests and needs. More inclusive digitalisation and improved cybersecurity will strengthen human security in the EHN.

There is a clear need to understand human responsibility in developing digitalisation and cybersecurity so that they do not only serve national security interests and economic growth. The Nordic strategies contain inconsistencies in what is said and what is done, which is evident in the contradictions existing in national and regional framings. For instance, the national strategies acknowledge the need to reformulate digital service provision on the basis of people's needs and so that using services is safe and simple, regardless of an individual's condition. Services should be provided in multiple languages "to the extent deemed necessary" (Ministry of Transport and Communications, 2011). In addition, they should be designed collectively so that different segments in society are able to participate in the early stages of the process. However, regional voices raise concern regarding imperfect consultation in the design of national services and networks. They bring forth challenges in service provision in regionally spoken languages and to people and businesses in areas with restricted connectivity. Moreover, the existing regional silence around cybersecurity – there are no regional cybersecurity strategies, as the organisation and coordination of cybersecurity has been centralised to the state, even if the responsibility for

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

cybersecurity rests on the shoulders of all actors in the society – can be interpreted as a mark of confusion over who should be doing what, and what cybersecurity entails at the regional level.

In order to improve cybersecurity in the EHN, increased regional data production, as well as the explication of processes that enable refocusing and redefining cybersecurity in terms of human security, need to be carried out. ICTs, digitalisation and cybersecurity are not forces of nature but human constructs whose appearance and outlook follow from contextualised human decision making.

References

Aaltola, M., Käpylä, J., & Vuorisalo, V. (2014). *The challenge of global commons and flows for US power. The perils of missing the human domain*. Farnham: Ashgate.

Arctic Economic Council (AEC). (2017). Arctic Broadband. Recommendations for an interconnected Arctic. Retrieved 3 October 2017 from https://arcticeconomiccouncil.com/wp-content/uploads/2017/02/

AEC (Arctic Economic Council). (2018). Save the date: 3rd Top of the world Arctic broadband summit 2018, Sapporo, Japan. Retrieved 8 March 2018 from https://arcticeconomiccouncil.com/save-date-3rd-top-world-arctic-broadband-summit-2018-sapporo-japan/

Axelrod, W. (2004). *Outsourcing information security*. Norwood, MA: Artech House Books.

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

Brennen, S., & Kreiss, D. (2014). Digitalization and digitization. Culture Digitally [group blog]. Retrieved 16 August 2016 from http://culturedigitally.org/2014/09/digitalization-and-digitization/

Burgess, J.P., & Sissel, H.J. (2008). *The influence of globalization on societal security: the international setting*. PRIO Policy Brief 3. Retrieved 14 March 2018 from https://www.prio.org/utility/ DownloadFile.ashx?id=176&type=publicationfile

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge: Cambridge University Press.

Buzan, B., & Wæver, O. (2003). *Regions and powers: The structure of international security*. Cambridge: Cambridge University Press.

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

Carr, M. (2012). The political history of the Internet: A theoretical approach to the implications for U.S. power. In S. S. Costigan & J. Perry (Eds.), *Cyberspace and global affairs* (pp. 173–187). Farnham: Ashgate.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press.

Castells, M. (2010). *The rise of the network society* (2nd ed.). Malden, MA: Wiley-Blackwell.

Clough, J. (2010). *Principles of cybercrime*. Cambridge: Cambridge University Press.

Commission on Human Security. (2003). *Human security now*. Retrieved 4 January 2017 from http://www.un.org/humansecurity/sites/www.un.org.humansecurity/files/chs_final_report_-_english.pdf

Crosby, E. (2016). Information technology's cultural setting: Some considerations. In L. J. Janczewski & W. Caelli (Eds.), *Cyber conflicts and small states* (pp. 8–17). Abingdon: Ashgate.

Cruz-Jesus, F., Oliveira, T., & Bacao, F. (2012). Digital divide across the European Union. *Information and Management*, *49*(6), 278–291. http://doi.org/10.1016/j.im.2012.09.003

CSSN (Cyber Security Strategy for Norway) 17.12.2012. Ministry of Government Administration, Reform and Church Affairs. Retrieved 11 August 2016 from https://www.regjeringen.no/globalassets/upload/fad/vedlegg/iktpolitikk/cyber_security_strategy_norway.pdf

Davi, M. (2009). Human security as the one size fits all policy approach? The European Security and Defence Forum WS2, Chatham House. Retrieved 4 October 2016 from https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/1109esdf_davi.pdf

Dunn Cavelty, M. (2013). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

European Commission. (2016). Digital Single Market, Digital Scoreboard, Progress by Country -reports for Finland, Sweden and Norway. Retrieved 26 August 2016 from https://ec.europa.eu/digital-single-market/en/progress-country

European Union Agency for Network and Information Security (ENISA). Threat Landscape-reports for 2012, 2013, 2014 and 2015. Retrieved 14 December 2016 from https://www.enisa.europa.eu/publications#c5=2006&c5=2016&c5=false&c2=publicationDate&reversed=on&b_start=0

Figuères, C. M., & Eugelink, H. (2014). The role of ICTs in poverty eradication: More than 15 years' experience from the field. In H. Kaur & X. Tao (Eds.), *ICTs and the millennium development goals. A United Nations perspective* (pp. 199–222). New York, NY: Springer.

FCSS (Finland's Cyber Security Strategy). Government Resolution 24.1.2013. Secretariat of the Security Committee. Retrieved 26 August 2016 from http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, *110*(3), 425–479. Retrieved 5 April 2018 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2843913

Finnish Transport Agency / Centre for Economic Development, Transport and the Environment. (2016). AURORA, valtatie 21/E8 Kolari-Muonio-Kilpisjärvi.2/2016. Retrieved 3 October 2017 from https://devtest.liikennevirasto.fi/webgis-aineistot/Tie_Aurora_Vt21_E8.pdf

Finnmark Fylkeskommune [Finnmark County]. (2015). Digitaliseringsstrategi Finnmark fylkeskommune 2015–2018. [Digitalisation strategy of Finnmark county 2015-2018] Retrieved 5 September 2016 from http://www.ffk.no/Handlers/fh.ashx?MId1=11523&FilId=25682

FireEye. (2015). Cyber threats to the Nordic region. Threat intelligence report. Retrieved July 11, 2016 from https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-nordic-threat-landscape.pdf

FireEye. (2016). Beyond the bottom line: The real costs of data breaches. Retrieved 11 July 2016 from https://www2.fireeye.com/WEB-Real-Cost-of-Data-Breaches.html

Giacomello, G. (2014). Introduction: Security in cyberspace. In G. Giacomello (Ed.), *Security in cyberspace. Targeting nations, infrastructures, individuals* (pp. 1–19). New York, NY: Bloomsbury.

Greenstein, S. (2015). *How the Internet became commercial: Innovation, privatization, and the birth of the network*. Princeton, NJ: Princeton University Press.

Informations och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. [Cybersecurity in Sweden. Strategy and measures for secure information in central government] Statens Offentliga Utredningar (SOU) 2015: 23. Retrieved 19 October 2016 from http://www.sou.gov.se/wp-content/uploads/2015/03/SOU-2015_23_webb.pdf

Kaldor, M. H., Martin, M. E., & Selchow, S. (2007). Human security: A new strategic narrative for Europe. *International Affairs*, *83*(2), 273–288. https://doi.org/10.1111/j.1468-2346.2007.00618.x

Kilpeläinen, A. (2016). *Teknologiavälitteisyys kyläläisten arjessa. Tutkimus ikääntyvien sivukylien teknologiavälitteisyydestä ja sen rajapinnoista maaseutusosiaalityöhön.* [Technology mediatedness in the everyday life of people living in rural villages. A study of technology mediatedness in ageing villages and interfaces with social work in the countryside] (Doctoral dissertation). University of Lapland. Rovaniemi: Acta Universitatis Lapponiensis 316.

Kluver, R. (2000). Globalization, informatization and intercultural communication. *American Journal of Communication*, *3*(3). Retrieved 11 November 2015 from unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002006.htm

Kommunenes Sentralforbund [Norwegian Association of Local and Regional Authorities]. (2013). Digitaliseringsstrategi 2013–2016 for kommuner og fylkeskommuner. [Digitalisation strategy 2013–2016 for municipalities and counties]. Retrieved 9 November 2016 from http://www.ks.no/contentassets/e7f699792add4068aaedcb25a97ff56a/ks-digitaliseringsstrategi.pdf?id=8215

Länsstyrelsen Norrbotten [County Council of Norrbotten]. (2013). Digital Agenda. Norrbotten. Retrieved 19 October 2016 from http://www.itnorrbotten.se/files/1394112515_itn_Digital_Agenda_BD_webbversion.pdf

Lapin liitto [Regional Council of Lapland]. (2013). Lapin digiohjelma 2020. [Digitalisation programme for Lapland 2020] Retrieved 28 July 2016 from http://www.lappi.fi/lapinliitto/c/document_library/get_file?folderId=1457612&name=DLFE21300.pdf

Larsen, J. N., & Fondahl, G. (Eds.) (2014). Arctic human development report. Regional processes and global linkages. Nordic Council of Ministers. TemaNord 2014:567. Retrieved 21 November 2016 from http://norden.divaportal.org/smash/get/diva2:788965/FULLTEXT03.pdf

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

Marichal, J. (2012). *Facebook democracy. The architecture of disclosure and the threat to public life*. Farnham: Ashgate.

Mayer-Schönberger, V., & Hurley, D. (2000). Globalization of communication. In J. S. Nye & J. D. Donahue (Eds.), *Governance in a globalizing world* (pp. 135–151). Washington, DC: Brookings Institution.

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

Ministry for Foreign Affairs of Finland. (2016). Finland's Chairmanship Program for the Arctic Council 2017–2019. Exploring common solutions. Retrieved 3 October 2017 from http://arcticjournal.com/sites/default/files/suomen_arktisen_neuvoston_puheenjohtajuusohjelma.pdf

Ministry of Enterprise, Energy and Communications. (2011). ICT for Everyone – A Digital Agenda for Sweden. 2011/342/ITP. Retrieved 26 August 2016 from http://www.government.se/contentassets/8512aaa8012941deaee5cf9594e50ef4/ict-for-everyone—a-digital-agenda-for-sweden

Ministry of Local Government and Modernisation. (2016). Digital agenda for Norway in brief. ICT for a simpler everyday life and increased productivity. Meld. St. 27. Retrieved 25 August 2016 from https://www.regjeringen.no/contentassets/07b212c03fee4d0a94234b101c5b8ef0/engb/pdfs/digital_agenda_for_norway_in_brief.pdf

Ministry of Transport and Communications. (2011). Productive and inventive Finland – Digital agenda for 2011–2020. Retrieved 26 August 2016 from http://oph.fi/download/135323_productive_and_inventive_finland.pdf

Ministry of Transport and Communications. (2016). Information security strategy for Finland. The world's most trusted digital business environment. Publications 9/2016. Retrieved 18 July 2016 from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75353/9-2016_Information_Security_Strategy_for_Finland.pdf?sequence=1

Mordini, E. (2014). Considering the human implications of new and emerging technologies in the area of human security. *Science and Engineering Ethics*, *20*(3), 617–638. https://doi.org/10.1007/s11948-014-9555-7

National Crime Agency, NCA Strategic Cyber Industry Group. (2016). Cyber Crime Assessment 2016 – Need for a stronger law enforcement and business partnership to fight cyber crime. Retrieved 12 December 2016 from http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

NCSS (Nationell strategi för samhällets informations- och cybersäkerhet). [A National Cyber Security Strategy] Skr. 2016/ 17:213. Regeringskansliet [the Government Offices], Justitiedepartementet [Ministry of Justice]. Retrieved 3 October 2017 from http://www.regeringen.se/49f22c/contentassets/3f89e3c77ad74163909c092b1beae15e/nationell-strategi-for-samhallets-informations–och-cybersakerhet-skr.-201617213

Norden – NordForsk. (2013). Societal security in the Nordic countries. Policy paper 1. Retrieved 16 August 2016 from http://norden.diva-portal.org/smash/get/diva2:707865/FULLTEXT01.pdf

Nordic Council of Ministers. (2017). An inclusive, innovative and secure Nordic region. The Swedish Presidency 2018. Retrieved 8 March 2018 from http://norden.diva-portal.org/smash/get/diva2:1151389/FULLTEXT01.pdf

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security*, *26*(2), 87–102. Retrieved 5 April 2018 from http://aix1.uottawa.ca/~rparis/Paris.2001.IS.Human%20Security.pdf

Räsänen, P. (2008). The persistence of information structures in Nordic countries. *The Information Society*, *24*(4), 219–228. https://doi.org/10.1080/01972240802191555

Sartor, G. (2013). Human rights and the information society: Utopias, dystopias and human values. In M. V. de Azevedo Cunha, N. N. G. de Andrade, L. Lixinski, & L. T. Feteira (Eds.), *New technologies and human rights: Challenges to regulation* (pp.11–26). Abingdon: Ashgate.

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

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar. What everyone needs to know*. New York, NY: Oxford University Press.

Skepys, B. (2012). Is there a human right to the Internet? *Journal of Politics and Law*, *5*(4), 15–29. http://dx.doi.org/10.5539/jpl.v5n4p15

Taddeo, M. (2013). Cyber security and individual rights, striking the right balance. *Philosophy and Technology*, *26*(4), 353–357. https://doi.org/10.1007/s13347-013-0140-9

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press

Taipale, S. (2012). The use of e-government services and the Internet: The role of socio-demographic, economic and geographical predictors. *Telecommunications Policy*, *37*(4–5), 413–422. https://doi.org/10.1016/j.telpol.2012.05.005

UNDP (United Nations Development Programme). (1994). Human development report. Retrieved 8 November 2016 from http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

UNHRC (United Nations Human Rights Council). (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HCR/17/27. Retrieved 16 August 2016 from http://www2.ohchr.org/English/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.PDF

Webster, F. (2014). *Theories of the information society* (4th ed.). Abingdon: Routledge.

Yar, M. (2006). *Cybercrime and society*. London: SAGE.

https://doi.org/10.1017/S0032247418000268 Published online by Cambridge University Press