

- II. Salminen, Mirva (2019) Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North. *The Yearbook of Polar Law* X, 321–356. https://doi.org/10.1163/22116427_010010015.

Reproduced as a part of a doctoral dissertation with the kind permission of the copyright holder.

The Yearbook of Polar Law

Volume 10, 2018

Edited by

Gudmundur Alfredsson
Timo Koivurova

Special Editors for Volume 10

Dorothee Cambou
Joëlle Klein



BRILL
NIJHOFF

LEIDEN | BOSTON

For use by the Author only | © 2019 Koninklijke Brill NV

Contents

Preface IX

The Need to Safeguard an Official Language by Law: The Case of Greenland 1

Hon. Vivian Motzfeldt

Two Key Developments in Polar Law and Diplomacy: A New Arctic Science Agreement and Establishment of the World's Largest Marine Protected Area in Antarctica's Ross Sea 11

Evan T. Bloom

Indigenous Peoples' Rights

Sámi's Reindeer Husbandry and EU Legislation (beyond Finland and Sweden's Accession Treaty) 23

Enrico Albanesi

Indigenous Persons with Disabilities: The Quest for Legal Recognition of Intersectionality and the Prohibition of Multiple Discrimination using the Example of the Sámi People in Finland 41

Leena Heinämäki

The Place of Indigenous Languages in the Russian System of School Education: A Legal Analysis 75

Ekaterina Andreyevna Zmyvalova

Environment and Cooperation in the Arctic

Nordic Cooperation at a Crossroads 105

Matti Niemivuo and Lotta Viikari

Region Building and Regional Cooperation in Response to Environmental Challenges: A Case Study from the Barents Region 132

Sarah E. Mackie

For use by the Author only | © 2019 Koninklijke Brill NV

Comparison of the Nordic Chairmanship Programmes and the Outputs of the Arctic Council in 2000–2013 158

Paula Kovari

Transboundary Environmental Harm in the Arctic – In Search of Accountability for an Oil Spill 187

Outi Penttilä

Environmental Governance of the Arctic: Next Steps – Diverse, Compatible, Needed 215

Joseph F.C. DiMento, Christine Schrottenbaum and Elizabeth Taylor

Digital and Cyber Security

Digital Language Divide in the European High North: The Level of Online Presence of Minority Languages from Northern Finland, Norway and Sweden 247

Marcin Dymet

The Evolving Information-Based Society and Its Influence on Traditional Culture: Framing Community Culture and Human Security of the Sámi in the European High North 275

Kamrul Hossain

The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens 297

Gerald Zojer

Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North 321

Mirva Salminen

China and the Arctic

Arctic Governance and China's First Arctic Policy: An UNCLOS Perspective 359

Xueping Li

For use by the Author only | © 2019 Koninklijke Brill NV

The South China Sea Award: Prompting a Revived Interest in the Validity of Canada's Historic Internal Waters Claim? 386

Krittika Singh and Timo Koivurova

Non-Peer Reviewed Articles

The 'Greenland Factor' in China's Expanding Arctic Diplomacy 415

Marc Lanteigne

China & the Arctic: Why the Focus on International Law Matters 427

Timo Koivurova

China's Arctic Policy and Belt and Road Initiative: Synergy or Conflict? 431

Nengye Liu

Developing an Iranian Antarctic Science Roadmap: A Legal and Policy Outlook 435

Zia E. Madani and Julia Jabour

Book Reviews

Alexandra Xanthaki, Sanna Valkonen, Leena Heinämäki and Piia Nuorgam (eds), *Indigenous Peoples' Cultural Heritage: Rights, Debates, Challenges* 455

Laura Olsén

Timo Koivurova, Pamela Lesser et al. (eds), *Environmental Impact Assessment in the Arctic: A Guide to Best Practice* 459

Uzuazo Etemire

Elena Conde and Sara Iglesias Sánchez (eds), *Global Challenges in the Arctic Region: Sovereignty, Environment and Geopolitical Balance* 463

Alexander Proelss

Niels Vestergaard, Brooks A. Kaiser, Linda Fernandez and Joan Nymand Larsen (eds), *Arctic Marine Resource Governance and Development* 466

Joseph F. C. DiMento

For use by the Author only | © 2019 Koninklijke Brill NV

Timo Koivurova, Qin Tianbao, Sébastien Duyck and Tapio Nykänen (eds),
Arctic Law and Governance – The Role of China and Finland 470
Stefan Kirchner

Project Announcements

Executive Summary of the HuSArctic Conference Outcomes 477
Ed. Joëlle Klein

Research Plan Åland 481
Göran Lindholm

Refocusing and Redefining Cybersecurity: Individual Security in the Digitalising European High North

*Mirva Salminen**

Abstract

This article introduces cybersecurity in the discussion on security in the European High North in a redefined and refocused form. Instead of scrutinising the technical measures taken to protect the confidentiality, integrity and availability of information in systems and networks (information security) or the criticality of a number of digitally operated infrastructures to the functioning of society (national cybersecurity), it concentrates on the human being. It examines cybersecurity from an individual's perspective by asking what kind of personal security concerns people may have with regard to digitalisation and how those are or are not present in the discussion on health and social security re-organisation in the Finnish Lapland.

The theoretical foundation of this article rests within the human security framework. Individuals living their everyday lives in particular cyber-physical environments are taken as the referent object of security. In the digitalising European High North, multiple aspects of everyday security depend upon cybersecurity, including economic, environmental, and food securities. This article concentrates on health and social security. It examines linkages between the re-organisation of health and social security in Finland and personal security concerns with a particular focus on the case of Länsi-Pohja area in south-western Lapland. The overall aim is to create room for bottom-up influence on the primarily top-down processes of security production in the cyber-physical environment.

Keywords

digitalisation – cybersecurity – human security – administrative restructuring

* Researcher, PhD Candidate, Arctic Centre, University of Lapland.

1 Introduction

Digitisation¹ and digitalisation² emerged as state policies in the mid 1990's in Finland. In the new millennium, these policies became geographically extensive and have been intensively driven by the governments. In 2008, for example, the Finnish government declared internet access as a fundamental right, which precipitated country-wide, state-supported broadband construction programmes with regional implementation. Similarly, national information security strategies were established in the early 2000's. Cybersecurity as a national policy emerged in the early 2010's. Development in Sweden and Norway has proceeded along similar lines. For example, all of the states have published national information society, digitalisation, information security and cybersecurity strategies from the 1990's onwards. Information and communication technologies (ICTs) have penetrated the Nordic societies to such an extent that the nominator "cyber-physical" is used in the article to describe the everyday environment in which people live. A given starting point is that actions in the digital sphere affect the physical environment – and vice versa.

In the European High North, that is, in the northernmost parts of Finland, Sweden and Norway,³ digital development has followed the national timetables. Alongside climate change, digitalisation is the main contemporary driver of change in the region, even if infrastructural challenges exist. For instance, the region has been, and remains, the main beneficiary of country-wide network development programmes. Yet, it simultaneously serves as a test-bed for digital innovations and structural societal conversion. For example, Lapland has been a forerunner in digital education due to its sparse population, vast distances and general cost-efficiency pressures. Similarly, it has intensively developed digital health and social security services. The stated aim of the development has been to continue service provisioning close to people regardless of the continuous restructuring of national, regional and local administrations, which has centralised services to population centres. Prime concerns and opposition presented have related to increasing uncertainty and fears

1 S Brennen and D Kreiss, 'Digitization and Digitalization' (Culture Digitally, 2014) <<http://culturedigitally.org/2014/09/digitalization-and-digitization/>> accessed 6 January 2018. Conversion of analogical information into digital, binary format.

2 Ibid. Increasing use and dissemination of information and communication technologies in virtually all aspects of human life so that they begin to influence, shape and structure the environment.

3 Finland: Lapland; Sweden: Norrbotten; Norway: Troms, Finnmark and Nordland.

for reduced everyday security when service provisioning withers away from rural areas.⁴

Individual security questions are at the heart of the on-going re-organisation of health and social security in Finland. In this article, these concerns are presented through a case study in Lapland. The focus is on the political fight over future service provisioning in Länsi-Pohja, which is an area consisting of two towns and four municipalities in south-western Lapland. In governmental plans, this area would lose some of its services for the aim is to reduce regional duplication. Service provisioning would continue in Rovaniemi, the regional capital of Lapland, which is located around 100 kilometres away. Enhanced digitisation has been one of the envisioned substitutive policies to ensure that people will still have an easy service access. However, residents, town and municipality leaders, as well as health and social security professionals working in the area, resist the relocation plans. This confrontation has led to a political dispute within Länsi-Pohja, within Lapland, within political parties, as well as between local and national administrations. The case study has been chosen for it brings forth tensions embedded in the on-going restructuring of health and social security in Finland. It also well depicts the related security concerns that incentivise people to act upon the matter.

Cybersecurity has rarely been addressed in the framework of human security.⁵ However, aspects related to human vulnerability in the turmoil of digitalisation have been discussed in science, technology and society literature⁶ and theorising on digital divides.⁷ Cybersecurity literature, on the other hand, does not interrogate human security but, at its best, highlights the

4 For further information see M Salminen and K Hossain, 'Digitalization and Human Security Dimensions in Cybersecurity: Appraisal for the European High North' (2018) 54 *Polar Record*.

5 For example, the overview of human security theorising given by D Gasper and O A Gomez, 'Evolution of Thinking and Research on Human and Personal Security 1994–2013' (UNDP Human Development Report Office 2014) Occasional paper. <http://hdr.undp.org/sites/default/files/gomez_hdr14.pdf> accessed 3 November 2017.

6 For example, G Yansen and M Zukerfeld, 'Why Don't Women Program? Exploring Links between Gender, Technology and Software' (2014) 19(3) *Science, Technology & Society* 305; P Cockshott and K Renaud, 'Humans, robots and values' (2016) 45 *Technology in Society*, 19; H Kukka and others, 'From cyberpunk to calm urban computing: Exploring the role of technology in the future cityscape' (2013) 84 *Technological Forecasting & Social Change* 29.

7 For example, S Taipale, 'The use of e-government services and the Internet: The role of socio-demographic, economic and geographical predictors' (2012) 37(4–5) *Telecommunications Policy* 413; P Räsänen, 'The Persistence of Information Structures in Nordic Countries' (2008) 24(4) *The Information Society* 219; D P Subramony, 'Understanding the Complex Dimensions of the Digital Divide: Lessons Learned in the Alaskan Arctic' (2007) 76(1) *The Journal of Negro Education* 57; B Warf, 'Contours, contrasts, and contradictions of the Arctic internet' (2011) 34(3) *Polar Geography* 193.

importance of teaching and training people to use ICTs in a smart manner. The object to be secured is “digital opportunities”, but the mainstream literature discusses merely the opportunities for states, businesses and/or other organisations while often bypassing people. In contradiction, information society and digitalisation literatures address the opportunities for people as well, but remain fairly silent about security. Therefore, there is a demand for bringing digitalisation and cybersecurity agendas together – not only for more holistic and extensive knowledge production, but also for improved policies that take human security questions related to digitalisation seriously.

In this article, I will first briefly address the prevailing understanding of cybersecurity as both a technical and a national security question. In the second section, I will scrutinise how refocusing cybersecurity around the human being changes the prevailing understanding and calls for redefined cybersecurity. The third, and the main, section of the article discusses individuals’ security concerns related to the restructuring of health and social security in Lapland. As a conclusion, a more inclusive digital framework for the European High North is needed in order to address the existing security concerns.

2 Prevailing Understanding of Cybersecurity

The mainstream understanding of cybersecurity has developed together with information and communication technologies (ICTs) becoming ever more important for running and steering society and economy.⁸ It brings together responses to the vulnerability of ICTs and national security concerns. Technology-focused information security⁹ approach highlights the protection of information in systems and networks through technical, organisational and educational measures. It aims at safeguarding the confidentiality, integrity and

⁸ For example, M Mueller, *Will the Internet Fragment?* (Polity Press 2017) 12.

⁹ In this article, information security is used as an umbrella term encompassing also computer security/hygiene and network security. The non-ICT-related aspects of information security, like professional confidentiality and storing of sensitive documents in strongboxes, are not considered.

availability of information in all situations.¹⁰ It also lays on the background of cybersecurity approach.¹¹

Cybersecurity lifts information security to another level by concentrating on the protection of infrastructures that enable the functioning of society. Technical vulnerabilities are inherent in these infrastructures hence opening a door for disruptions in their operations. The causes of disruptions may be accidental (for technical or environmental reasons) or intended (as malefactors seek to abuse the vulnerabilities). Moreover, the human being – who is still using ICTs or in charge of overseeing the (semi-)automated ICT operations – has been recognised as a major vulnerability, mainly due to his or her gullibility or vengefulness.¹² Regardless of the cause of disruption, the main aim in cybersecurity is to ensure the functioning of infrastructures deemed critical for the functioning of society and economy in all situations. As majority of these infrastructures run on or are steered through ICTs, cybersecurity is a society-wide concern. Therefore, comprehensive national and supranational cybersecurity strategies have been developed to ensure societal (and organisational) resilience against cybersecurity incidents.¹³

It is argued here that in all its comprehensiveness, the prevailing, systemic understanding of cybersecurity allocates inadequate attention to the human being.¹⁴ When concentrating on the protection of information and

-
- 10 For example, N Gcaza and others, 'A general morphological analysis: delineating a cyber-security culture' (2017) 25(3) *Information & Computer Security* 259; S DeKay and K Belva, 'Privacy Roles and Responsibilities' in C W Axelrod, J L Bayuk and D Schutzer (eds) *Enterprise Information Security and Privacy* (Artech House, 2009) 8–9; J R Vacca, 'Introduction' in J R Vacca (ed) *Managing Information Security* (2nd edn, Elsevier, 2014) xix–xx.
- 11 R D Alexander and S Panguluri, 'Cybersecurity Terminology and Frameworks' in R M Clark and S Hakim (eds) *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level* (Springer 2017) 22–24; N Ben-Asher and C Gonzalez, 'Effects of cyber security knowledge on attack detection' (2015) 48 *Computers in Human Behavior* 51; Gcaza and others (n 10).
- 12 For example, A F Ginter, 'Cyber Perimeters for Critical Infrastructures' in R M Clark and S Hakim (eds) *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level* (Springer 2017) 72; S J White, 'Assessing Cyber Threats and Solutions for Municipalities' in R M Clark and S Hakim (eds) *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level* (Springer 2017) 54–55; M Hall, 'Why people are key to cyber-security' (2016) (6) *Network Security* 9.
- 13 Also, for example, E Matani, L Yoffe and M Mashkautsan, 'A Three-Layer Framework for a Comprehensive National Cybersecurity Strategy' (2016) 17(3) *Georgetown Journal of International Affairs*, 77.
- 14 Similar claims have been made, for example, by M Dunn Cavelty, 'Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities' (2014) 20(3) *Science and Engineering Ethics* 701; Gcaza and others (n 10).

infrastructures, it bypasses the interests, needs and fears of people experiencing the consequences of omnipresent digitalisation. Trustworthiness and concealability of information, as well as the functioning or non-functioning of infrastructures, become meaningful only when people start experiencing the consequences of successful and/or failed protection in their everyday life. Inspired by the human security line of argumentation, this article brings the individual to the heart of cybersecurity and scrutinises the implications this move has, firstly, for the prevailing cybersecurity understanding and, secondly, for everyday life in the European High North.

3 Cybersecurity from an Individual Security Point of View

Human security strives both to examine the factors that cause insecurity to individuals and communities and to improve the situation. It is a critical, situational approach shedding light on the consequences of top-down decision-making in the experienced circumstances and enabling bottom-up influence in the decisions.¹⁵ In the European High North, this means scrutinising the implications – both positive and negative – that politically, economically and technologically driven digitalisation has in people's everyday life and empowering individuals to influence the future trajectories of their cyber-physical environment. For society-wide digitalisation and cybersecurity strategies and programmes are decided upon in state capitals, they fail to accommodate the particularities of digital development in the regions. The cyber-physical environment becomes easily understood as a unified entity even if, for instance, geographical and infrastructural settings can vary greatly within a country. In addition, internet (over which a great deal of communication is carried out) is by definition a network of networks which vary, for instance, in terms of their robustness, security and resilience.¹⁶ These variations impact, for example, how good internet and/or cellular connections are, who is covering the costs of digital development and what kind of products

15 M Glasius and M Kaldor, 'A human security vision for Europe and beyond' in M Glasius and M Kaldor (eds) *A Human Security Doctrine for Europe: Project, Principles, Practicalities* (Routledge 2005) 3–19; United Nations Human Security Unit, 'Human Security in Theory and Practice. An Overview of the Human Security Concept and the United Nations Trust Fund for Human Security' <www.un.org/humansecurity/sites/www.un.org.humansecurity/files/human_security_in_theory_and_practice_english.pdf> accessed 20 January 2018.

16 Mueller (n 8) 15–17.

and/or services are required. Besides material factors, people's skills, awareness and confidence to act in the cyber-physical environment vary.

Currently, an acknowledged gap in cybersecurity awareness and ICT-skills exists around the world.¹⁷ In this regard, the European High North is not an exception. Projects run throughout the region have strived to familiarise people with existing digital opportunities and/or risks and to improve their skills.¹⁸ Similarly, state and/or EU-supported projects attempt to bring fast and reliable digital networks within everyone's reach¹⁹ and to dismantle obstacles to digital access, for instance, for individuals of old age and/or with disabilities.²⁰ These projects, however, come with goals stated by the funder or initiator without much local influence on the agenda.²¹ Contrarily, the efforts of regional councils (funneling state, EU or other funders' resources) and local municipalities at least state that local people, communities, businesses and administration have been consulted in the processes of digitalisation programme formulation.²²

17 For example, Special Eurobarometer 464a 'Europeans' attitudes towards cyber security' <<http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2171>> accessed 1 December 2017; Special Eurobarometer 460 'Attitudes towards the impact of digitization and automation on daily life' <<http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2160>> accessed 1 December 2017.

18 For example, the DigimpiLappi project <www.digimpilappi.com/> which targeted people over 55 years of age, for instance, through peer support (Digi Emissaries, who voluntarily help people to use digital services) and guidance (both online and face-to-face).

19 For example, the Fast Broadband project in Finland <www.viestintavirasto.fi/ohjausjavalvonta/nopealaajakaista.html> which has been running under different names since 2008. Areas where the construction of high-speed broadband network is not beneficial under market terms can apply for state support under certain conditions.

20 For example, the accessibility programmes run by the Finnish Ministry of Transport and Communications since the early 2000's. The first implementation programme was published in 2005. <www.lvm.fi/documents/20181/817515/Kohti+esteetonta+viestintaa.+Toimenpideohjelman/88703178-f7af-4fbb-9d40fc96d7fe80d6?version=1.0> accessed 18 July 2016. These programmes are still running and regularly updated.

21 For example, the Regional Council of Lapland has given such criticism. Lapin liitto, 'Lapin Digiohjelman 2020' (2013) 36 <www.lappi.fi/lapinliitto/c/document_library/get_file?folderId=1457612&name=DLFE-21300.pdf> accessed 28 July 2016; J. Tiihonen, 'Lapin liitto: Vastuukuntamalli ei toimi Lapissa' *YLE* (17 March 2014) <<https://yle.fi/uutiset/3-7140029>> accessed 19 December 2017.

22 Lapin liitto (n 21); IT-Norrbottn, 'Digital Agenda Norrbotten' (2014) <www.itnorrbottn.se/wp-content/uploads/2016/11/digital_agenda_norrbottn.pdf> accessed 23 November 2016.

The state of information infrastructure in the European High North varies greatly,²³ but in general connectivity is fairly good. Where there is no fixed broadband, mobile networks enable both calling and data transfer. Connections are best in towns and along the main roads, whereas no reception may be available in the wilderness. Most of the region falls somewhere in between these two extremes. Zero reception is a concern, for example, for search and rescue – especially, when the number of tourists visiting the region keeps rising. In addition, some of the villages are dependent on only one fibre-optic cable. Ever increasing digitalisation, improving ICTs, and further digitisation of services set constant pressure for bandwidth availability and demand for infrastructure updates. In some areas, overlaps in frequencies forestall updates,²⁴ but in general the cycle of renewals is the same throughout the Nordic countries. Harsh climate and vast distances set additional requirements for both technologies and companies maintaining them in the region.²⁵

This article leans on the aspects of human security defined in the 1994 United Nations Development Programme (UNDP) report on human development. These aspects entail personal, community, environmental, health, food, economic, and political security. The article focuses on the impacts of digitisation, and the related insecurities, on healthcare in the European High North. Social security issues have been integrated in health security, because health and social security policies are bound together in the region. In the UNDP report, social security was to an extent included in economic security.²⁶ The impacts of digitisation are examined from an individual's perspective leaving community aspects aside.²⁷ By anchoring the examination to the individual, the aim is to concretise the human security framework in the chosen situational setting. Thus, in its part, it strives to address the main criticism towards the framework as being too comprehensive to eventually say anything

23 See the coverage maps available on the Fast Broadband-project's website <www.viestintavirasto.fi/ohjausjavalvonta/nopealaajakaista/hankkeeneteneminen.html> accessed 9 October 2017.

24 For example, close to the Russian border 4G technology cannot be utilised but 3G is operational. YLE, 'Venäjän vaatimukset hidastavat rajaseudun 4G-verkkoa' (22 November 2011) <<https://yle.fi/uutiset/3-5457094>> accessed 9 January 2018.

25 For additional information see, for example, M Salminen, 'Digital Security as an Aspect of Human Security in the Barents Region' in Kamrul Hossain, Dorothée Cambou (eds) *Society, Environment and Human Security in the Arctic Barents Region* (Routledge, Oxon 2018).

26 UNDP, 'Human Development Report 1994' 25–26 <http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf> accessed 8 November 2016.

27 Community aspects are addressed, for instance, in Kamrul Hossain's article in this volume.

What is secured?

COMMON CYBERSECURITY PERSPECTIVE <> INDIVIDUAL SECURITY

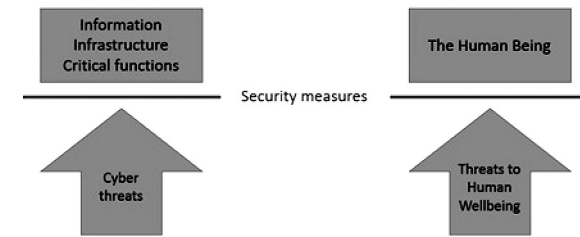


FIGURE 1 From securing information and/or infrastructure to securing the human being

meaningful about security.²⁸ Similarly, the concept has been criticised for arbitrarily separating and highlighting the seven aspects,²⁹ but the discussion falls outside the scope of this article.

When the human being is shifted to the focus and made the referent object of cybersecurity, not only the perceived threats (from cyber threats to threats to human wellbeing) but also the implemented security measures transform. A comparison of the understandings is depicted in figure 1 above.

In the prevailing understanding of cybersecurity, threats to information, infrastructure and/or critical societal functions are presented either as taxonomies of technical threats or as strategic threat tables. The former list items such as malware, web based attacks, web application attacks, denial of service, botnets, phishing, spam, exploit kits, data breaches, and identity thefts.³⁰ The latter usually include the categories of cyber activism (or hacktivism), cybercrime, politically and/or economically motivated espionage, cyber terrorism and cyber operations (or warfare) (increasing in estimated severity to

28 For example, R E Howard-Hassman, 'Human Security: Undermining Human Rights?' (2012) 34(1) *Human Rights Quarterly* 88; M Martin, 'A Road Still to Be Travelled: Human Security and a Continuing Search for Meaning' in S Takahashi (ed) *Human Rights, Human Security, and State Security: The Intersection*, vol. 2 (Praeger 2014).

29 Gasper and Gomez (n 5) 14–19.

30 ENISA, 'Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends' (2017) <www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016> accessed 27 September 2017.

the functioning of society).³¹ Security measures then taken include technical, organisational and educational fixes to the perceived problems.³²

It has been argued that existing cybersecurity approaches focus more “on saving money or developing elegant technical solutions than on working and protecting lives and property”.³³ This misfocus can be addressed through an individual security approach. Moreover, both technical and strategic threat depictions remain fairly abstract and distant to people’s everyday experience. They make little sense to those not used to the professional discourse, transform quickly without becoming more coherent and, thus, sustain the knowledge-related power positions and divisions in, between, and across societies. While doing so, they marginalise the majority of population from political, economic and technical decision-making processes in which the future of cyber-physical environment is decided.³⁴ In order to open the discussion on digitalisation and cybersecurity to a wider public, the prevailing discourses are in need of refocusing and redefining. They need to be concretised and brought closer to people’s everyday experience.

Discourses understandable in layman’s terms, as well as more inclusive strategies and programmes, enable individuals to strive for freedom from fear, want and indignity also in the digital environment. People’s fears are usually related to the unfamiliarity of ICTs, inexperience in their use, doubt in one’s own skills, and concerns of being excluded due to lacking knowledge and skills. Freedom from want entails that people do not fall victim to cybercrime, for instance, scams and cons; and that they are able to provide themselves, for example, by applying for jobs online, using the equipment and software at work, and/or claiming social security online. People ought to utilise ICTs fearlessly and with confidence. Freedom from indignity adds to the latter point by indicating that people should not become named and shamed online without evidence, treated as inferiors due to their treats, and all have access to the same services. In addition, they should not become victims of harassment, snooping and/

31 For example, Finland’s Cyber Security Strategy. Government Resolution 24 January 2013 <<https://turvallisuuskomitea.fi/index.php/en/component/k2/38-cyber-security-strategy>> accessed 27 September 2017; see E Tikki, ‘Ten Rules for Cyber Security’ (2011) 53(3) *Survival* 119.

32 For example, Alexander & Panguluri (n 11); Ginter (n 12); White (n 12).

33 R R Schell, ‘Privacy and Security. Cyber Defense Triad for Where Security Matters’ (2016) 59(11) *Communications of the ACM* 20.

34 For example, M G F P D Garcia, ‘Knowledge and New Technologies: From Ethics to Politics and Law’ in M V de Azevedo Cunha and others (eds) *New Technologies and Human Rights: Challenges to Regulation* (Routledge 2016).

or hate speech.³⁵ In contradiction, ICTs ought to empower people to improve their everyday security and wellbeing in the cyber-physical environment.³⁶ In the prevailing cybersecurity discourse, the positive, empowering side of security is easily neglected or becomes addressed in inadequate terms. Utilisation of human security framework can change this state of affairs.

In an individual security approach to cybersecurity, the human being in his or her cyber-physical environment becomes the object to be secured. Similarly, he or she becomes an active producer of security and gains a say in decision-making concerning digitalisation and cybersecurity. He or she is perceived as one of the stakeholders to attend the definition processes of digital development and cybersecurity. Threats to human wellbeing can be analysed, for example, in the context of the aforementioned seven aspects of human security. Security measures, again, become understood in a more comprehensive manner, including not only specific measures taken to safeguard the functioning of digital infrastructure and the confidentiality, integrity and availability of information, but also issues such as adequate income to acquire the necessary equipment and digital literacy to use the increasingly digitised services provided in the European High North. In the next section, I will turn to individual security in the cyber-physical environment in more detail.

4 Individual Security in the Digitalising European High North

In national cybersecurity strategies, as well as in many corporate policies, the individual is given a number of security-related roles. Firstly, he or she is recognised as a potential malevolent: a cybercriminal, a cyberterrorist, a cyber-mercenary, a digital spy, a grunted insider, or a hacktivist, who tries to raise attention towards a specific issue. Secondly, he or she may be a non-tech-savvy employee who endangers the organisation by behaving in an unwise manner in the digital environment. Thirdly, he or she is expected to do his or her part in the production of comprehensive cybersecurity, for instance, by acquiring necessary security software; learning how to secure one's own devices, networks and communication; improving his or her ICT-skills so that mistakes do not happen; as well as reading small prints in user agreements and

35 For the frequency and consequences of such demoting acts see, for example, D K Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 35–55.

36 See also E Mordini, 'Considering the Human Implications of New and Emerging Technologies in the Area of Human Security' (2014) 20(3) *Science and Engineering Ethics* 617.

acknowledging where liability lies in each case. The problem is that whereas the first group (usually) knows the cyber-physical environment rather well, the latter two either do not know it or may not wish to familiarise themselves with it.³⁷

While the existing societal (security) organisations are busy with finding solutions to the protection of meta- and meso-levels of cybersecurity (global, societal and organisational levels), the individual is often left alone to find ways to carry out his or her responsibility to secure him- or herself.³⁸ The state of affairs is problematic, because for individuals who are not familiar with the principles of information security and/or cybersecurity, the demand for self-protection appears absurd. In addition, interest in the topic may be lacking. If one does not recognise risks inherent in the digitisation of his or her living environment or does not feel the need to worry about such things, one can hardly plan and execute security measures that may help mitigating risks and securing opportunities. In the opposing end of the continuum, intense cyber threat and risk discussion may prevent people from utilising ICTs or “seizing digital opportunities”.

For analytical purposes, individual security in the cyber-physical environment is in this article divided into following categories: (1) physical security (often claimed to be improved through technical solutions promising less human error); (2) ICT-skills and confidence to act in the digital environment; (3) awareness of digital opportunities, but also of related vulnerabilities, risks and threats; (4) privacy issues; (5) a say in technology development; (6) felt (emotional) security; and (7) human rights questions in the cyber-physical environment. In practical terms, these aspects often overlap and become intertwined in everyday life. In this article, the focus is on the re-organisation of health and social security in the Finnish Lapland. As from an individual's perspective the safety of digitising health and social security services is also a question of personal security, the latter receives a fair amount of attention. I will begin with personal security concerns as they lay on the background when people evaluate the positive and negative impacts of digitalisation.

37 See B von Solms and J van Niekerk, 'From Information Security to Cyber Security' (2013) 38 *Computers and Security* 97; Gcaza and others (n 10).

38 About individual decision-making in cybersecurity situations see, for example, H Rosoff, J Cui and R S John, 'Heuristics and biases in cyber security dilemmas' (2013) 33(4) *Environment Systems and Decisions* 517; N Ben-Asher and C Gonzalez, 'Effects of cyber security knowledge on attack detection' (2015) 48 *Computers in Human Behavior* 51.

4.1 *Personal Security in the Cyber-Physical Environment*

In the UNDP report on human development, personal security is tied to physical security.³⁹ The report does not recognise the need to protect individuals in the digital environment, which can be explained by the lesser role that ICTs played in everyday life in the early 1990's (for example, email and internet browsers were only a few years old; commercial internet and the social media sites we know today did not exist⁴⁰), as well as the then paucity of people's experience with them. On the contrary, nowadays personal security ought to recognise the entanglement of physical and digital security – protection from harm caused by the state, other states, other groups of people, individuals and gangs, as well as cover threats at women, children and to self⁴¹ in any environment – and cover a wider range of issues emerging in the cyber-physical environment. Many of these issues relate to individuals' everyday life as (1) customers of health and social security services, (2) objects of examination carried out by health and social security professionals and with digital clinical histories, (3) users of ICTs and digital health and social security services, (4) cost units evaluated by administrative decision makers as parts of wider data sets, (5) citizens with the related rights and obligations, and (6) psycho-physical entities bearing particular rights as human beings.

In the context of cybersecurity, individuals' personal security becomes easily reduced to technical questions of privacy – the protection, concealment and deletion of personal details; privacy of communication and of one's premises; and/or the ability to select which information about one's life becomes publicly available.⁴² Moreover, quite often the “cybersecurity dilemma” is presented as a continuous balancing act between security and privacy, which positions two integral dimensions of personal security as somehow oppositional.⁴³ In the extreme, people may be expected to live a fully transparent life

39 UNDP (n 26) 30–31.

40 S Greenstein, *How the Internet Became Commercial: Innovation, Privatization, and the Birth of a New Network* (Princeton University Press 2015).

41 UNDP (n 26) 30.

42 For example, A Bergström, 'Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses' (2015) 53 *Computers in Human Behavior* 419; D Le Métayer, (2016) 'Whom to Trust? Using Technology to Enforce Privacy' in D Wright & P De Hert (eds) *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (Springer, 2016); M-O Baumann & W J Schünemann, 'Introduction: Privacy, Data Protection and Cybersecurity in Europe. The Conceptual and Factual Field' in W J Schünemann & M-O Baumann (eds) *Privacy, Data Protection and Cybersecurity in Europe* (Springer, 2017) 6.

43 A F Brantly, 'The Cyber Losers' (2014) 10(2) *Democracy and Security* 132; M Hildebrandt, 'Balance or Trade-Off? Online Security Technologies and Fundamental Rights' (2013)

in order to assist security experts and authorities in the provision of (national and/or societal) security. “I have nothing to hide” thinking and the revenue model embedded in free information sharing on social media sites that requires corporations developing and maintaining these sites to push the users towards ever more sharing add to this transparency requirement.⁴⁴ Regardless of the headlines raised by the concealed information collection practices of some states and corporations, people continue hand out information about their everyday life, including their health and social standing, hence contributing to the “loss of privacy”.⁴⁵

Nonetheless, an alternative approach exists recognising the mutually constitutive relationship between security and privacy. For the individual, privacy is an aspect of personal integrity. Personal security is hence not only about the protection, tampering or loss of data sets, but about one’s self-image and the ability to control to an extent his or her social appearance. Misplaced or disclosed personal details, as well as incorrect, profane information may lead to violations of one’s physical security, emotional wellbeing, or security of one’s possessions, as well as to a loss of reputation and/or income. Misused and/or abused personal details facilitate identity thefts that can be followed, for instance, by criminal charges. They may also cause any imaginable restriction to one’s individual freedom due to financial, legal or social obligations taken under one’s identity without the acknowledgement of the true owner of that identity. Fortunately, all national cybersecurity strategies effective in the European High North recognise the importance of privacy and the protection of human rights in the digital environment.⁴⁶ Yet, the daily news about, for

26(4) *Philosophy and Technology* 357; M Taddeo, ‘Cyber Security and Individual Rights, Striking the Right Balance’ (2013) 26(4) *Philosophy and Technology* 353; A Biletzki, ‘Online Security: What’s in a Name?’ (2013) 26(4) *Philosophy and Technology* 397; S Stalla-Bourdillon, ‘Privacy Versus Security ... Are We Done Yet?’ in S Stalla-Bourdillon, J Phillips & M D Ryan (eds) *Privacy vs. Security* (Springer, 2014).

44 J P Albrecht, ‘Regaining Control and Sovereignty in the Digital Age’ in D Wright and P De Hert (eds) *Enforcing Privacy. Regulatory, Legal and Technological Approaches* (Springer 2016) 473–475; Stalla-Bourdillon (n 43); J Marichal, *Facebook Democracy. The Architecture of Disclosure and the Threat to Public Life* (Ashgate, 2012).

45 R Moll, S Pieschl and R Bromme, ‘Whoever will read it – The overload heuristic in collective privacy expectations’ (2017) 75 *Computers in Human Behavior* 484; Albrecht (n 44) 473–474; Bergström (n 42).

46 Cyber Security Strategy for Norway (2012) <www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf> accessed 28 September 2017; Finland’s Cyber Security Strategy (n 31); Nationell strategi för samhällets informations- och cybersäkerhet (2017) Skr. 2016/17:213 <www.regeringen.se/49f22c/contentassets/3f89e3c77ad74163909c092b1beae15e/nationell-strategi-for-samhallet>

example, data breaches, accidental data disclosures, online scams and frauds, successful phishing operations, or purposeful data exposures and smearing testify that people and organisations are only partially able to protect digitised information.

Privacy is not the only concern of personal security in the European High North. A considerable amount of public and private services are either primarily or only provided in the digital format in the region. Development in the provisioning of health and social security is heavily geared towards this direction. Reasoning on the background can be found, for instance, in opportunities provided by developing ICTs and automation, cost-efficiency, fragmentation of daily routines and hence the need to make services available all-day round, reduced need to travel long distances, and the globalisation of service markets. For example, in Finland the development of digital public services began in the 1990's when, according to government strategies, they were developed to support physical service provisioning. Over the years, digital services became first equivalent to physical services and, finally, the primary form of service provisioning.⁴⁷ Similar development has taken place in Norway.⁴⁸

However, the digital skills and awareness of individuals have not followed the same development curve. When being asked, people express concern over their own and others' ability, know-how and comprehension to use digital services, as well as their preference to talk to a person face-to-face.⁴⁹ For example, according to an EU-wide Eurobarometer survey, 67 per cent of Europeans thought digitalisation has had a positive impact on their quality of life. Similarly, 71 per cent found themselves having the sufficient skills to use ICTs in everyday life, whereas 65 per cent considered themselves skilled enough to use digitised public services.⁵⁰ In other words, around 30 per cent of people do not think they are skilled enough to operate in the digital environment or that digitalisation has improved their wellbeing. Furthermore, large differences exists "in perceptions related to digital skills across Europe, depending on the

s-informations–och-cybersakerhet-skr.-201617213> accessed 28 September 2017. The Swedish strategy in particular points out the mutual constitutiveness of security and privacy.

47 See information society and digitalisation strategies from 1995 onwards.

48 Cyber Security Strategy for Norway (n 46).

49 Arctic Café 4 April 2017: Digitalisaatio – Lappilaisten mahdollisuus vai uhka? Arctic Centre, University of Lapland. Panel discussion <www.youtube.com/watch?v=yBpvOSA-ZOO4> accessed 22 November 2017.

50 Special Eurobarometer 460 (n 17) 3.

country, age or educational background”.⁵¹ Especially for an unaccustomed internet-user, the services likely appear complicated, confusing, difficult to use and unreliable.

Without a full confidence to use digital services, people easily become afraid of utilising them.⁵² Advice and support to the users has been arranged, for instance, by municipalities, non-government organisations, volunteers, service providers and state authorities in their still remaining physical service points,⁵³ but people utilise or do not utilise the provided support for a number of reasons. They may feel ashamed of their lacking skills and understanding, protest against digitalisation, get frustrated with the seemingly non-functioning services, or find it difficult to learn new ways of operating. In sparsely populated areas where everyone knows one another people also express unwillingness to bring their interests, needs and fears to the knowledge of fellow villagers. In addition, people with disabilities report on difficulties in using digital services tailored for the imaginary average user.⁵⁴

Individuals’ personal security in the cyber-physical environment hence depends on whether one trusts the environment and has the confidence, skills and ability to harness the known digital opportunities to his or her benefit. Without the aforementioned capabilities one may become excluded from service provisioning to his or her detriment, which feeds into both felt and objectively measurable personal insecurity. Insecurity is generated and sustained by one’s negative experiences, fears and concerns, experiences of other people (either directly or indirectly consulted), news and social media stories, as well as one’s assessment of whether wrongdoings become remedied. In the development of trust in the cyber-physical environment an important role is played by the product and service providers, as well as by the administrative systems organised to both facilitate and control the development. Whether the providers are developing secure products and services, and whether people adopt them and learn to use them in a safe manner, is a condition of prime importance. In addition, the regulatory framework – industries’ self-regulation, national and international regulation, as well as regulation carried out through transnational voluntary organisations working on technology governance – frames each digital encounter. People’s experiences may be conveyed to product, service and regulatory development through, for instance, market surveys, collected test-user experiences, polls and studies. However, in

⁵¹ Ibid.

⁵² For instance, Bergström (n 42).

⁵³ Arctic Café (n 49).

⁵⁴ See, for example, reports of the accessibility programmes as in n 20.

these forms of experience collection the questions are decided upon by the commissioners of the research while people have a little free say.

Yet it ought to be highlighted that digitalisation empowers people to improve their personal security. Firstly, it generally amends people's access to information that can be used to enhance their well-being. A limitless number of information sources exist online – the difficulty lies in recognising the most trustful ones. Moreover, (public) service providers are increasingly opening their registers so that individuals can check, correct and, to an extent, control and benefit from their personal data.⁵⁵ Furthermore, by googling one's own name, one can check what has been published about him or her online. If the need arises, he or she can request service providers to take down, for example, factually wrong and/or dishonouring claims.⁵⁶ Secondly, enhanced connectivity enables, *inter alia*, social interaction and running errands across time and distances. Thus, increased flexibility and subsequently lessened need to travel, for instance, decreases the chances of traffic accidents and reduces environmental footprint. Easier exchange of news between family members, friends, colleagues, peers and other significant others improves emotional well-being and the feeling of being secure.⁵⁷ Thirdly, the ability to publish and actively disseminate information about wrongdoings, for example, human rights violations can result in sufficient regional, national or transnational pressure to interfere in or change the situation (can also lead to the worsening of the situation). For instance, through online information dissemination the general awareness of the situation of the Sámi has risen.

From an individual's perspective, the aforementioned opportunities for eased everyday life are the main benefits of the digitisation of health and social security services. Cost-efficiency in service production is a secondary concern – unlike in political and/or administrative decision-making. Similarly, the aforementioned personal security concerns trouble people in service digitisation as they ponder upon the trustworthiness, reliability, and usability of digital services. In the next section, the discussion is concretised further through a case study of the dispute present in the on-going restructuring of healthcare and social security in the Finnish Lapland.

55 That is MyData initiatives such as A Poikola, K Kuikkaniemi & O Kuittinen, 'My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen' (Open Knowledge Finland and Ministry of Transport and Communication 2014) <http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/77875/My_data_-_johdatus_ihmiskeskeiseen_henkilotiedon_hyodyntamiseen.pdf?sequence=1> accessed 28 October 2017.

56 The right to be forgotten; reaffirmed by, for example, the EU's General Data Protection Regulation (GDPR).

57 Lapin liitto (n 21); IT-Norrbottn (n 22).

4.2 *Health and Social Security in Länsi-Pohja*

The change caused by digitalisation in people's everyday life has been tangible in the provisioning of health and social security services. Over the past twenty years, these services have been privatised and digitised to a great extent in the European High North.⁵⁸ In terms of human security, health security is depicted in the UNDP report on human development as protection from diseases, malnutrition, unhealthy lifestyles and harmful environmental impacts. It also entails access to healthcare. Threats to health security are noted to be greatest for the poorest, people living in rural areas, racial minorities, and children.⁵⁹ Social security, again, is in the report attached to one's ability to provide him- or herself and the family. It is defined as "compensation for loss of income for the sick and temporarily disabled; payments to the elderly, the permanently disabled and the unemployed; family, maternity and child allowances and the cost of welfare services".⁶⁰ The report remarks that such social safety net exists in the minority of the world's countries and is everywhere under curtailment.⁶¹ All Nordic states belong to this group of countries.

In this article, only the main features of regional digitalisation are touched upon for the issue-area is wide and develops quickly. They are discussed in the context of health and social security re-organisation in Länsi-Pohja. Under scrutiny is a dispute between the Finnish government, two existing healthcare districts in Lapland (Länsi-Pohja and Lappi), a private multinational healthcare corporation (Mehiläinen) and its competitors (Pihlajalinna, Attendo and Terveystalo), as well as the two towns (Kemi and Tornio) and four municipalities (Keminmaa, Simo, Tervola and Ylitornio) comprising Länsi-Pohja. The area lies in south-western Lapland bordering Sweden and, in fact, Tornio and Haparanda in Sweden constitute a twin city across the border. Healthcare and social security services in Länsi-Pohja may be provided in both Finnish and

58 The implications of this structural change have gradually become an object of study. For example, A Kilpeläinen, *Teknologiavälitteisyys kylälaisten arjessa. Tutkimus ikäntyvien sivukyläien teknologia-välitteisyydestä ja sen rajapinnoista maaseutuosiaalityöhön*. (Doctoral dissertation. Acta Universitatis Lapponiensis 316. University of Lapland 2016); L Viinamäki and others, '... ajasta ja paikasta riippumatta ... Digikansalaisuus ja palveluiden saavutettavuus maaseudulla-hankkeen loppuraportti'. (Series A. Referee-studies 1/2017. Lapland University of Applied Sciences 2017) <www.theseus.fi/bitstream/handle/10024/137218/A%201%202017%20Viinamaki%20Kivivirta%20Selkala%20Voutilainen%20Syvajarvi%20Suikkanen.pdf?sequence=1&isAllowed=y> accessed 9 January 2018.

59 UNDP (n 26) 27–28.

60 Ibid 222.

61 Ibid 25–26.

Swedish languages,⁶² whereas in northern Lapland service provisioning in both Finnish and the Sámi languages is a bigger concern.⁶³ At the moment of writing, both Lappish healthcare districts have a central hospital (Länsi-Pohja has one in Kemi and Lappi has one in Rovaniemi) with emergency duties. The dispute centres on the threat of eliminating some of the hospital functions in Kemi so that those would only be carried out in Rovaniemi about 100 km away. The structural change affects over 60 000 people living in the area. The overall population of Lapland is slightly over 180 000 people and its geographical size is about one-third of the overall area of Finland.

The dispute embeds in two Finnish government projects: one of digitising a bigger share of public services and another of restructuring health and social security service provisioning in the country. The programme facilitating the running of errands digitally and e-democracy (SADE-programme) was established in 2009 with the aim of producing good quality and interoperable digital services in the public sector. Digitisation was to generate cost efficiency and savings, as well as benefits for citizens, corporations, communities, municipalities and state officials. Principles that guided the programme, which ended in 2015, included co-development with service users, adequate information security, utilisation of market solutions and innovations from the private sector, advancement of open data and the use of open source code in public administration, and bilingual service provisioning.⁶⁴

In Lapland, the digitisation of health and social security services, including the development of the *virtu.fi* service portal, was funded through the SADE-programme. In the *virtu.fi*-portal, the residents of Lappish towns and municipalities⁶⁵ can, for instance, use a number of metrics and calculators for self-evaluation, book an appointment with a healthcare or a social security professional, contact professionals via videophone, use a documentation camera for preliminary diagnostics, fill in pre-registration forms, and utilise general advice provided. In addition, they can check their digital medical histories in

62 A Heikinmatti, 'Ruotsalaisten rahat kelpaisivat Länsikälle myös sote-aikana' YLE (29 September 2014) <<https://yle.fi/uutiset/3-7492038>> accessed 19 December 2017; YLE 16 June 2016. Finland is a bilingual country.

63 A Lakkala and E Niskanen, 'Huovinen: Saamelaisten tulee saada palveluita omalla äidinkielellään' YLE (12 September 2014) <https://yle.fi/uutiset/osasto/sapmi/huovinen_saamelaisten_tulee_saada_palveluita_omalla_aidinkielellaan/7468063> accessed 19 December 2017; YLE 17 May 2016; YLE 4 July 2016. Three Sámi languages are spoken in Finland and they all have an official minority language status.

64 For further information, see the programme website <<http://vm.fi/sade>> accessed 21 December 2017.

65 Digital services provided depend on the town and/or municipality. On the landing site, one first chooses which town's and/or municipality's services he or she wishes to use.

the national omakanta.fi service portal,⁶⁶ add and/or correct the information, as well as utilise a number of other digital services provided by public, private or third sector service providers.⁶⁷ Digitisation of services has, for instance, speeded up diagnostics in rural areas, enabled people to renew their prescriptions without meeting a doctor face-to-face, and smoothened the transfer of information to and amongst service providers. The virtu.fi-portal also provides support services to healthcare and social security professionals, such as online consultation platforms, consultation opportunities via videophone, general advice, secure information transfer channels, and online reporting platforms.⁶⁸ Digitalisation is one of the focus areas of the current government and digitisation of public services is one of its flagship projects.⁶⁹

The restructuring of healthcare and social security is a recurrent issue in Finnish politics. The on-going re-organisation is one of the reforms put forward in the government programme. The plan is to move the responsibility for the provisioning of healthcare and social security from municipalities to 18 counties to be established by 2020. The goal is that everyone has an equal access to these services and that freedom of choice can be executed in a broad manner. Digitalisation is one of the ways to strive towards this goal. Service queues ought to shorten, people to have an appointment quicker, data to travel smoothly between service providers, and people still to be able to use services close to their place of residence and/or where they prefer. Service providers

66 See the service portal <www.kanta.fi/omakanta> accessed 11 January 2018. In early 2018, information security problems concerning the service portal were reported, for example, a wide abuse of the portal by healthcare professionals and an inability of the individual to check who has viewed his or her details. See A-M Huhtanen, 'Kanta-palvelussa on tapahtunut rikoskäsitteilyynkin johtanutta urkintaa, kun esimerkiksi naapurin terveystietoja on katsottu luvatta – "Tuomioitakin on tullut"' *Helsingin Sanomat* (7 January 2018) <www.hs.fi/kotimaa/art-2000005516158.html> accessed 7 January 2018; M Valtavaara, 'Potilastietoja urkitaan joka päivä ja selitykset ovat kirjavia, sanoo tietosuojavaltuutettu – "Organisaation johto on usein heikoin lenkki"' *Helsingin Sanomat* (9 January 2018) <www.hs.fi/kotimaa/art-2000005518627.html?ref=rss> accessed 9 January 2018.

67 See the service portal <www.sosiaalikallega.fi/virtu.fi/> accessed 3 December 2017. The portal has links to the digital services of, for example, Kela (an independent national social security institution) and A-Clinic Foundation (a non-governmental organisation providing services in treatment and rehabilitation, substance abuse prevention, and substance abuse and psychosocial problems).

68 See the service portal <www.sosiaalikallega.fi/virtu.fi/ammattilaiset> accessed 14 January 2018.

69 See the government programme <<http://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio>> accessed 21 December 2017.

can come from public, private, as well as voluntary sectors.⁷⁰ Implementation of the re-organisation programme has proven to be difficult, because it generates schism and disputes within and between the different levels of state administration, amongst service providers, amongst decision makers and people using the services, as well as between population centres and rural areas. Currently, different areas in the country are moving forward at different paces and with varying plans as the overarching legislative basis is uncertain and the government has had to change its implementation plans for several times. In Lapland, the re-organisation of service structure was prepared in Lapin Sote-Savotta-project which ran between 2014 and 2017. The aim was to create a tailored, innovative service network that could safeguard service provisioning to all residents of the region. It achieved positive results, but also contributed to the dispute under scrutiny in this article.⁷¹

The case study of Länsi-Pohja is carried out by presenting a short historical narrative and the main security concerns in the dispute as they can be read from the regional news website of the national broadcasting company, YLE Lappi.⁷² The pieces of news were collected by searching with different combinations of keywords “sote”, “Länsi-Pohja”, “Kemi” and “sote uudistus” in December 2017. When a piece of news recommended further readings, the additional readings were included in the data. Only news published while the current government has been in power were included.⁷³ Thus, a sample of 79 news articles published between 16th of June 2015 and 22nd of December 2017 was collected.⁷⁴ The data source was selected for its national coverage, that is, its readership does not restrict to, for instance, people subscribing to local newspapers or receiving free newsletters in the region.

The recurrent themes around which the dispute revolves are related to people's fear for disappearing or deteriorating physical healthcare and social security services; increasing travel times and distances; degenerating economic situation within the area and its lessening attractiveness amongst students, working people, and health and social security professionals; as well as the loss of areal self-determination. Within the regional administration, the contradicting fears are for the loss of regional income and self-determination

70 For further information, see the reform website <<http://alueuudistus.fi/palvelut-ja-valinnanvapaus>> accessed 21 December 2017.

71 See the project website <<http://lapinsotesavotta.fi/>> accessed 11 January 2018.

72 YLE Lappi has newsrooms in both Kemi and Rovaniemi. Other data sources were also examined, like the online archive of the regional newspaper Lapin Kansa, but the flood of data eventually forced to concentrate on one data source.

73 The current government was appointed by the President of Finland on May 29th, 2015.

74 The pieces of news are listed in Appendix 1.

if people from Länsi-Pohja begin to run their errands in Oulu,⁷⁵ instead of Rovaniemi, thus generating an outflow of capital to Northern Ostrobothnia.⁷⁶ Additionally, the fear is for an inability to provide health and social security services equally in the entire Lapland. For the government, the main concern is that the Länsi-Pohja case generates a model for other areas to follow hence endangering the already agreed national re-organisation programme. I will next examine these themes further.

National re-organisation of healthcare and social security services was on the agendas of previous governments, but it became re-planned when the current government began its work. Negotiations for the re-organisation in Lapland were carried out between the representatives of both healthcare districts, as well as those of the towns and municipalities. When the Lapin Sote-Savotta-project was running, it became clear that significant differences existed in the opinions of Länsi-Pohja healthcare district and those of Lappi healthcare district concerning future service provisioning. Media reports about these differences of opinion pointed out that the representatives of Länsi-Pohja felt that their concerns were not addressed or even heard in the negotiations, but the representatives of Lappi were pushing for service centralisation to Rovaniemi. Lappi responded by pointing towards requirements set by legislation and practical necessities in cases where legislation per se did not require centralisation. On the background was mistrust felt towards the negotiating partner due to past experiences, for instance, from an earlier re-organisation process of highest occupational education. Länsi-Pohja felt that it had lost the university of applied sciences to Rovaniemi as a result of unfair negotiations. Fears for similar development and unhappiness with the negotiating process were expressed. The discontinuation of basic healthcare provisioning close to the customers, as well as the removal of delivery ward and extensive emergency duties away from Länsi-Pohja central hospital, were the main concerns.⁷⁷ Consequently, while the negotiations were on-going, the

75 Oulu is the biggest population and economic centre in northern Finland, but it belongs to the Ostrobothnia region and, thus, will not be part of the future county of Lapland.

76 See (n 74) YLE 14 November 2017b; YLE 17 November 2017b.

77 See (n 74) YLE 12 November 2015; YLE 26 January 2016; YLE 22 March 2017; YLE 23 March 2017; YLE 27 March 2017; YLE 25 April 2017; YLE 5 July 2017a; YLE 20 November 2017; YLE 19 May 2016a; YLE 19 May 2016b In the government plan, it was aligned that extensive emergency duty would in the future exist in Rovaniemi and Oulu, while in Kemi the duty would be restricted to basic healthcare combined with some special healthcare functions. Also YLE 28 August 2016; YLE 27 October 2016; YLE 9 November 2016.

towns and municipalities of Länsi-Pohja reactivated the examination of alternatives for health and social security provisioning.⁷⁸

One of the options investigated was an extensive outsourcing of healthcare services to a private corporation. Which services would be outsourced, and to what extent, was to be decided by each town and municipality. The suggested outsourcing format was the establishment of a co-owned company of which the private corporation would have the biggest share, while the towns and municipalities would become minority partners.⁷⁹ The primary goal was to ensure that physical service provisioning in Länsi-Pohja would remain at the existing level also in the future. People would have both basic and special healthcare services provided close to their place of residence. Psychiatric and rehabilitation services, surgical operations, as well as the delivery ward would continue in the area. Education and occupational training of healthcare professionals would continue hence providing the necessary workforce. The industries located in the area could rely on the emergency response capability of the healthcare sector also in the future.⁸⁰ When the negotiations between Länsi-Pohja and Lappi were on-going, the examination of other alternatives was presented merely as an option. However, it was also interpreted as a means of pressuring the negotiating partner and the government – both of which were in the media presented as unwilling to listen to the local concerns and, thus, taken by surprise by the decisions finally made in town and municipality councils.⁸¹

In the spring 2017, the negotiations about the division of work between Länsi-Pohja and Lappi in the future county of Lapland ended without a

78 See (n 74) YLE 12 April 2016. The examination of Länsi-Pohja specific health and social security solution had already begun when the previous government was in power. T Rantamartti, 'Paikallinen sote-työ jatkuu Länsi-Pohjassa' YLE (19 February 2015) <<https://yle.fi/uutiset/3-7817084>> accessed 19 December 2017. Also YLE 16 June 2015; YLE 17 November 2017b.

79 See (n 74) YLE 24 March 2017; YLE 24 April 2017; YLE 5 July 2017b; YLE 15 November 2017a; YLE 16 November 2017b.

80 For example, in YLE 19 October 2017 it was speculated that delays due to increasing distances to special healthcare would lead to additional paralyses and heart damages, as well as an increased risk of death. The logistic capacity would meet its limits rather quickly, for instance, in case of a major industrial accident. Additionally, the education and training of healthcare professionals in the area would likely end. In YLE 22 March 2017 it was hypothesised which of the functions of the Kemi central hospital would be moved to Rovaniemi. In YLE 3 November 2017b the economic implications recurring from the selection of either the county of Lapland model or the co-owned company model were depicted. The county model was expected to lead to economic deprivation, while the co-owned company model would generate savings and increased tax revenue.

81 See (n 74) YLE 17 November 2017b.

result.⁸² Towns and municipalities in Länsi-Pohja intensified the examination of the outsourcing option⁸³ and, eventually, put out a tender. Three offers were accepted for further negotiations – one from Mehiläinen, one from Pihlajalinn and one combined from the offers of Attendo and Terveystalo.⁸⁴ When the examination of outsourcing was on its way, the representatives of Lappi healthcare district, the management of the future county of Lapland, as well as the government reacted to the development. Appeals for returning to the negotiating table with Lappi healthcare district were presented and disinterest of the representatives of Länsi-Pohja to participate in the common planning was wondered.⁸⁵ Some local and national politicians, the Union of Health and Social Care Professionals, some healthcare professionals, as well as local people pointed out that outsourcing would not safeguard services and jobs in the area. Furthermore, as the prime operating principle of a private corporation is to generate profit to its owners, this was presumed to rule over the local needs.⁸⁶ Others, including doctors working in the Kemi central hospital, saw outsourcing as the only option for otherwise decision-making power would shift to Rovaniemi and service provisioning in the area reduce.⁸⁷ In many town and municipality councils, the decision was to be made between the evils of outsourcing and the fears of losing jobs and services. The outsourcing plan would move forward only, if every town and municipality agreed to the plan.⁸⁸ Negotiation failure with regard to the division of work in the future county of Lapland quickly politicised the dispute – which, to an extent, was also advocated for the wide ranging decision-making needs exceeded the mandate of healthcare districts.⁸⁹

When it began to look more likely that the towns and municipalities of Länsi-Pohja would opt for outsourcing, the government decided to establish a team of two investigators, both former ministers living in Lapland, tasked to provide a compromise solution to the dispute.⁹⁰ The move had already been suggested by the head of Lappi healthcare district.⁹¹ The government also

82 See (n 74) YLE 22 March 2017.

83 See (n 74) YLE 25 April 2017.

84 See (n 74) YLE 30 May 2017; YLE 14 June 2017; YLE 5 July 2017b.

85 See (n 74) YLE 27 October 2017; YLE 3 November 2017a.

86 See (n 74) YLE 12 April 2017; YLE 14 June 2017; YLE 9 November 2017a.

87 See (n 74) About the discussion in town and municipality councils, see YLE 25 April 2017. In YLE 19 October 2017, doctors working in the Kemi central hospital expressed their concern over service disappearance from Länsi-Pohja.

88 See (n 74) YLE 12 April 2017b; YLE 24 April 2017; YLE 25 April 2017.

89 See (n 74) YLE 23 March 2017; YLE 24 April 2017.

90 See (n 74) YLE 9 November 2017a; YLE 14 November 2017a.

91 See (n 74) YLE 3 November 2017c.

quickly put forward a bill to tighten the conditions under which towns and municipalities could do such outsourcing decisions. As the bill would become enforceable earliest in the beginning of 2018, the towns and municipalities in Länsi-Pohja also speeded up their processes. The outsourcing agreement with the selected private provider would have to be signed before the end of 2017 to be probated.⁹² In the media, the Minister of Family Affairs and Social Services, as well as the Prime Minister, gave statements in which they found the on-going development highly detrimental and dangerous for the nation-wide re-organisation project.⁹³ The Ministry of Social Affairs and Health published calculations according to which the ligature of one-third of the budget of the future county of Lapland to the provision of health and social security in Länsi-Pohja would endanger the independency of the county. As it seemed unlikely that the county would be able to arrange all of its obligatory tasks with the resources allocated to it, the possibility of combining it with the county of Northern Ostrobothnia entered the media discussion.⁹⁴

The dispute culminated in autumn 2017. The personnel of the Kemi central hospital, for instance, organised a demonstration regarding the future of the hospital. Statements both for and against the co-owned company were presented. A separate demonstration opposing outsourcing was organised a few days later.⁹⁵ Nevertheless, town and municipality councils in Länsi-Pohja decided to proceed with the co-owned company plan. This company would take care of the services that were nationally allocated to the basket of services which provider customers could freely choose, such as the maintenance of healthcare centres and, in this case, of an entire central hospital. The length of the agreement would be 15 years and the termination of the contract would cost the towns and municipalities – and hence also the future county of Lapland – about 100 million euros. Additionally, services provided to families and elderly people, as well as the public authority functions, would be moved to the extended healthcare district until taken over by the future county of

92 See (n 74) YLE 5 July 2017a; YLE 9 November 2017a; YLE 15 November 2017c; YLE 16 November 2017a; YLE 30 November 2017d. According to the bill, towns and municipalities could no longer carry out major outsourcing decisions that would affect 30 per cent or over of the public services and/or do contracts that would last for longer than five years. Also YLE 14 December 2017a; YLE 22 December 2017a; YLE 22 December 2017b.

93 See (n 74) YLE 3 November 2017a; YLE 15 November 2017a; YLE 15 November 2017b; YLE 16 November 2017a.

94 See (n 74) YLE 10 November 2017; YLE 14 November 2017c; YLE 15 November 2017b; YLE 21 November 2017a; YLE 21 November 2017b; YLE 23 November 2017.

95 See (n 74) YLE 9 November 2017a; YLE 9 November 2017b.

Lapland.⁹⁶ Each town and municipality would participate in the restructuring of healthcare in ways that best served its interests.⁹⁷

In the media, the government was accused of pressuring and fear mongering after an initially deferred reaction to the security concerns expressed by the people of Länsi-Pohja.⁹⁸ Lappi healthcare district and the management of the future county of Lapland were accused of having by-passed the interests, needs and fears of people living and industries operating in Länsi-Pohja, while preferring the centralisation of services and valuing money over human beings.⁹⁹ Representatives of Länsi-Pohja were accused of taking the overall re-organisation of healthcare and social security as a hostage for selfish reasons and without considering what would be best for entire Lapland. This selfishness was said to endanger, amongst others, health and social security provisioning in other areas of Lapland.¹⁰⁰ The Union of Health and Social Care Professionals felt that they had not had a say.¹⁰¹ Finally, the broadcasting company YLE was accused of propagating for the outsourcing option.¹⁰² People living in Länsi-Pohja, as well as in other areas of Lapland, had differing opinions about the topic. In the media, they expressed fears for uncertainty regarding, for instance, the pricing and availability of services in the future, whether familiar personnel would be present in healthcare stations, how people without the abilities to make decisions about their own care would be taken into consideration, and what would happen to child health services or healthcare in schools.¹⁰³

After the outsourcing decision was made in Länsi-Pohja, pressure towards Rovaniemi for coming further to the half-way intensified in the media. Such advice was given, for example, by the members of parliament representing

96 See (n 74) YLE 30 November 2017d; YLE 24 April 2017; YLE 23 October 2017; YLE 14 November 2017a; YLE 15 November 2017b. According to the Finnish law, public authority functions, such as custody decisions or involuntary commitment, cannot be outsourced. Also YLE 16 June 2016; YLE 5 July 2017b.

97 See (n 74) Kemi, Tornio, Simo and Keminmaa decided to fully participate in the co-owned company, whereas Ylitornio and Tervola would only contribute in terms of special healthcare. YLE 14 June 2016; YLE 9 November 2017b; YLE 14 November 2017a; YLE 14 November 2017b. Keminmaa and Tervola also examined the option of a separate outsourcing of the majority of healthcare services. YLE 29 March 2017b; YLE 21 September 2017; YLE 16 November 2017c.

98 See (n 74) YLE 17 November 2017b.

99 See (n 74) YLE 17 November 2017b.

100 See (n 74) YLE 3 November 2017c; YLE 23 November 2017.

101 See (n 74) YLE 16 November 2017d.

102 K Kärki, 'Yhteisyritys vaarantaa koko Lapin maakunnan' *Lapin Kansa* (Rovaniemi 15 November 2017) A4.

103 See (n 74) YLE 30 November 2017c; YLE 14 December 2017a.

the region. Willingness to continue negotiations was also expressed by the representatives of Rovaniemi.¹⁰⁴ Simultaneously, negotiations between the chosen private corporation, Mehiläinen, and the towns and municipalities of Länsi-Pohja continued on the details, such as which healthcare services would be provided where and how.¹⁰⁵ The area also continued investing in equipment and facilities.¹⁰⁶ One of the other bidders, Pihlajalinna, complained to the Market Court about the outsourcing process.¹⁰⁷ The Ministry of Social Affairs and Health tasked the Regional State Administrative Agency of Lapland to investigate the legality of the outsourcing decision.¹⁰⁸ According to the Agency, giving a final statement was impossible before the signing of the contract, but in principle the decision was legal.¹⁰⁹ A sequel was played in Kemi. After having suspended the processing of the outsourcing decision and hence attempting to prevent the mayor from signing the contract, the town's executive committee faced a vote of no confidence.¹¹⁰ The committee eventually granted the mayor to sign,¹¹¹ which happened before Christmas (Kemi, Tornio, Simo, Keminmaa, Länsi-Pohja healthcare district and Mehiläinen as signatories). The contract came to force in the beginning of 2018.¹¹²

Neither social services nor digitalisation ever became a major item in the discussion. Instead, the dispute centred on the location of physical healthcare service points. While digitisation changes both the reach and availability of health and social security services, it was only mentioned, for instance, when the future provisioning of healthcare was envisioned. Special healthcare was expected to become increasingly mobile and utilise novel digital services to a great extent.¹¹³ Basic healthcare would also be arranged so that a nurse accompanied with a computer would visit the customer in his or her home, instead of the customer coming to see the nurse in a healthcare centre.¹¹⁴ A representative of Lappi healthcare district regretted that the representatives of Länsi-Pohja had been unwilling to consider the advantages digitalisation

104 See (n 74) YLE 29 November 2017a; YLE 30 November 2017b.

105 See (n 74) YLE 29 November 2017b; YLE 5 December 2017.

106 See (n 74) YLE 30 November 2017a; YLE 31 November 2017d; YLE 15 August 2017.

107 See (n 74) YLE 4 December 2017.

108 See (n 74) YLE 14 November 2017b; YLE 16 November 2017a; YLE 21 November 2017a.

109 See (n 74) YLE 1 December 2017.

110 See (n 74) YLE 5 December 2017; YLE 11 December 2017a; YLE 11 December 2017b; YLE 14 December 2017a; YLE 14 December 2017b.

111 See (n 74) YLE 19 December 2017.

112 See (n 74) YLE 22 December 2017a; YLE 22 December 2017b.

113 See (n 74) YLE 12 April 2016.

114 See (n 74) YLE 16 June 2016.

in service provisioning.¹¹⁵ Additionally, private healthcare corporations had already pointed out that they would also examine opportunities for service digitisation.¹¹⁶ The personal security concerns related to digitalisation that were outlined in the previous section of this article never entered the media discussion on future healthcare and social security provisioning in Länsi-Pohja.

It seems that the nation-wide re-organisation of health and social security services, including the digitisation of these services, moves ahead without much dialogue with people's everyday experience. The re-organisation is pushed forward for economic and administrative reasons while justifying it in terms of improved service provisioning, increased freedom of choice, and more customer say. Centralisation and digitalisation are the guiding stars for the future. On the contrary, and leaving the regional power struggles aside, people are primarily concerned about the reduction of everyday security due to the disappearance of physical healthcare service points from their area of residence – not asking for more digitalisation, access to these services from their homes, and/or the ability to freely choose their service providers. As the current development is proceeding to the opposing direction, it creates and sustains individual security concerns in the Finnish Lapland.¹¹⁷ Digitalisation is not a trend that can be overturned, but it should be integrated in policy discussions across issue-areas so that its consequences; alternative policy choices; the associated opportunities, but also threats and risks; as well as people's expectations and experiences would become part of the decision-making concerning the future development of the cyber-physical European High North.

5 A More Inclusive Digital Framework for the European High North is Required

In people's perceptions, their everyday security does not revolve around digitalisation. As the case of Länsi-Pohja presents, cybersecurity questions related to individual security are not discussed even when the re-organisation of health and social security in the Finnish Lapland generates major disputes within the region and between regional and national policy processes. The conversion of digital and physical, and the related penetration of ICTs to virtually all aspects

115 E Melamies, 'Meri-Lapin sote-ratkaisu huolestuttaa muuta Lappia' *Lapin Kansa* (Rovaniemi 16 November 2017) A6.

116 V Vaarama, 'Tienestii siintää myös pohjoisen SOTE – alueella' *YLE* (1 October 2014) <<https://yle.fi/uutiset/3-7503544>> accessed 19 December 2017.

117 See (n 74) About the decreasing influence of rural areas in decision-making see, for example, *YLE* 20 November 2017.

of human life, lay on the background of this societal restructuring. However, the expressed security concerns relate to physical service provisioning, even if the opportunities generated by digitalisation drive the ongoing societal transformation. It is a failure of politicians and administrative policy makers, if they cannot reason, explain and justify the chosen policy options and address the security concerns hence generated and/or intensified. Instead of threat politics, a constructive dialogue remarking people's interests, needs and fears ought to be utilised. Digitalisation should thus not be discussed as a separate issue-area, for example, from health and social security. Furthermore, cybersecurity should not be isolated into another issue-area where technology and/or national security professionals discuss in highly abstract terms about the functionality of society in all security situations, but to be brought into everyday security discussions. Opportunities generated by digitalisation are the reason for its political and administrative advancement, but these neither coincide with people's desires nor become well conveyed in the discussion.

Usually, when digitalisation and cybersecurity are discussed in the context of healthcare, the discourse does not revolve around user interfaces or people's experiences with or fears for service digitisation. Instead, it concentrates on, for example, increasingly precise care, robot-assisted or fully automated operations, and optimisation of churn times. In social security, the discourse focuses on internet-based self-service and reporting portals, safe money transfers, and professional-customer communication via digital means. The envisioned outlook of both health and social security depend on functioning ICTs and their safe use. In particular, in the sparsely populated regions, where the physical service network is already thin. By engaging the local people as customers of health and social security services, objects of professional examination who have digital clinical histories, users of ICTs and digital services, cost units in service provisioning, citizens, as well as human beings who bear particular rights, in the decision-making concerning the cyber-physical future of the European High North both the awareness of and felt satisfaction with the re-organisation of health and social security can be increased. People will thus gain a say in the development of their living environment.

People need to be aware of digital services and have the skills to use them. Regardless of the campaigns run and support provided, many are still not familiar with the services. In addition, people need the confidence and mental strength to use the services, which may be an obstacle, for instance, for individuals with mental health issues. Next to that, they need internet banking credentials or digital ID-cards to use the services, which cannot be taken for granted. The confidentiality, integrity and availability of digital health and social security services ought to be guaranteed in all situations, which has

turned out to be a challenge. If a digital service is not available, malfunctions or does not provide adequate guidance, the legal protection of the service users should not become endangered.¹¹⁸ In sum, there is a number of issues that require settling so that people know what digital services exist, know how to use them, receive the support they need in utilising them, will not be marginalised because of digitisation, and will be treated equally in service provisioning.

Moreover, health and social security provisioning depends, for instance, on functioning power and water infrastructures which are either run or directed through ICTs. It also embeds in the national, supranational and international networks of, for instance, logistics or medicine and appliances manufacturing which also depend on functioning digital infrastructure. Problems in any of the networks and/or infrastructures has significant consequences in people's everyday life.¹¹⁹ Therefore, they should also be openly discussed. The aim should be not to increase fears and/or concerns, but to enhance individual security and wellbeing by sharing information, addressing existing concerns, and taking desires into consideration.

Digitalisation creates a shift in responsibility from the public (or less frequently private) administration to the individual. As there are more online forms to fill in and more service platforms to use, the individual becomes the one required to master all of these forms and platforms. He or she is expected to know what information to provide on which platform, where to find the platforms and how to use them, manage a range of security credentials, remember when to update the details or check the test results. Of course, if he or she is tech-savvy, many of the services can be synched and/or reminders sent to

¹¹⁸ For example, several people in Finland were taken by surprise and lost their unemployment benefit in the autumn 2017 for the public employment services did not advice job seekers well enough in the use of online services. J Auramies, 'Usean työttömän tuki on katkennut sähköisen lomakkeen teknisen puutteen takia – Mikko kertoo, ettei ole saanut 2 kuukauteen "pennin jeniä"' MTV3 (27 November 2017) <www.mtv.fi/uutiset/kotimaa/artikkeli/usean-tyottoman-tuki-on-katkennut-sahkoisen-lomakkeen-teknisen-puutteen-takia-mikko-kertoo-ettei-ole-saanut-2-kuukauteen-penninjenia/6670894?_ga=2.118585353.1213175442.1512318451181452300.1510420205#gs.HjldZPE> accessed 3 December 2017.

¹¹⁹ For example, when WannaCry ransomware infected ICTs of the National Health Service in the UK, people were left without or with only reduced care for several days. Operations had to be cancelled or people sent abroad. L Hay Newman, 'The Ransomware Meltdown Experts Warned About Is Here' Wired (15 December 2017) <www.wired.com/2017/05/ransomware-meltdown-experts-warned/> accessed 19 January 2018. Similarly, problems in the supply logistics caused several weeks delays in Oriola's medicine supply in Finland. A-K Urpelainen, 'Oriola pahoissa ongelmissa – tilausten käsittelyjen vaikeudet jatkuvat, mutta valo tunnelin päässä näkyy jo' TiVi (8 September 2017) <www.tivi.fi/Kaikki_uutiset/oriola-pahoissa-ongelmissa-tilausten-kasittelyjen-vaikeudet-jatkuvat-mutta-valo-tunnelin-paassa-nakyy-jo-6675040> accessed 19 January 2018.

one's smartphone or email about scheduled meetings. Yet, every additional link increases the complexity and vulnerability of the entirety hence also increasing security challenges. Moreover, these links are becoming increasingly automatised, which means that more information is collected directly from, for example, heart rate monitors and blood pressure meters without human interference.

This article does not wish to challenge or deny digital opportunities, but aims at broadening and deepening the discourse. From an individual's perspective, health and social security does not only involve as quick and precise care as possible, but also one's ability to follow his or her own care, acquire information, make informed decisions, and have a say in the means through which his or her health and social situation is supported. In principle, the on-going developments to compile data to single service portals and to grant people the right to check and correct their personal information are taking the development to a good direction. Nonetheless, they also face the challenge of people not being aware and having troubles in using the platforms, as well as information and cybersecurity challenges recognised by the mainstream cybersecurity discourse. When people's personal details are collected to single databases, security concerns and potentials for abuse ought to be carefully addressed.¹²⁰ Individuals' personal security concerns should prevail, instead of administrative cost-efficiency pressures.

Defining of a cybersecurity culture specific to the European High North, and thus recognising its regional characteristics, could be a partial answer the challenges depicted throughout this article.¹²¹ It is likely that cybersecurity concerns related to personal security become more actual for individuals, when they become accustomed to digitised service provisioning with both its pros and cons. When they do, an open and engaging dialogue should be part of the cybersecurity culture. Alongside the embedded threats and risks, it should highlight the positive, enabling sides of digitalisation and cybersecurity that empower people to improve their wellbeing. Centring on individuals' physical and emotional security, ICT-skills and confidence to act in the digital environment, digital awareness, privacy issues, and human rights questions in the cyber-physical environment, the culture could better reason the importance of security measures taken at all levels of society. Instead of abstracts concerns, it ought to concentrate on practical security questions that people encounter in their everyday life in the cyber-physical European High North.

¹²⁰ See (n 66).

¹²¹ See, for example, Gcaza and others (n 10).

Appendix 1: Research Data

News articles collected from YLE web portal <www.yle.fi>

16.6.2015	Tornion uusi kaupunginjohtaja: Kuntien tehtävät on mietittävä uusiksi / J Tiihonen
9.11.2015	“Kaikkea päivystystä ei voi keskittää 12 paikkaan” / R Rautiainen
12.11.2015	Kansalaisaloite kaatui – Länsi-Pohjassa uskotaan silti omaan synnytyssosastoon / H Hannukainen
26.1.2016	Lapissa valmistaudutaan maakuntahallintoon luottamustapaamisilla / A Passoja
6.4.2016	“Mahdollisuudet hyvään mutta myös riskejä” – miten Lapin käy sote-uudistuksessa? / A Leppävuori
12.4.2016	Länsi-Pohja valmistelee omaa sotea – hallituksen linjaus on luettu tarkkaan / K Marttala
2.5.2016	Kaatuuko Meri-Lapin kuntien sote-yhtiö uuteen lakiin? / J Tiihonen
17.5.2016	Sipilän ja Saamelaiskäräjien tapaamisen keskiössä pohjoismainen saamelaissojimus ja sote-uudistus / M Alajärvi
19.5.2016a	Länsi-Pohjassa odotetaan ympärivuokautisen päivystykseen säilyvän alueella / K Marttala
19.5.2016b	Tässä ovat sote-uudistuksen laajan päivystyksen sairaalat / T de Fresnes
16.6.2016	Sote-muutosjohtaja: Virtuaalinen sairaanhoito syrjäseutujen pelastus / A Passoja
20.6.2016	Hanna Mäntylä: Valinnanvapaus ei saa johtaa monopoliasemaan / J Tiihonen
4.7.2016	600 sivua sotea, saamelaisista muutama maininta / P Näkkäläjärvi & G Satokangas
28.8.2016	Viisi tarinaa sote-myrskyn silmästä – uudistus kätilön mielessä päivittäin: “Mitä tämä diipadaapa-puhe tarkoittaa?” / E Kuivas
27.10.2016	Länsi-Pohjan synnytykset jatkuvat ainakin kaksi vuotta / A Heikinmatti
9.11.2016	Länsi-Pohjan sote-valmistelu käynnistyi / K Vaara
18.11.2016	Nopea netti mahdollistaa etätyön syrjäkylälläkin – saavatko kunnat nyt uusia asukkaita? / K Vaara
22.3.2017	Erikoissairaanhoitoa viedään Kemistä Rovaniemelle – sairaanhoitopiirien neuvottelut katkesivat erimielisyyksiin / A Heikinmatti

For use by the Author only | © 2019 Koninklijke Brill NV

- 23.3.2017 Merilappilaiset voivat äänestää soteasiassa jaloillaan – “Se on maakunnalle iso suonenisku” / A Heikinmatti
- 24.3.2017a “Ei ole mitään järkeä pistää sadan miljoonan investoinnit Rovaniemelle ja jättää kunnossaoleva infra käyttämättä” / A Heikinmatti
- 24.3.2017b Keminmaa alkaa selvittää sosiaali- ja terveystalouden yksityistämistä / J Mehtonen
- 27.3.2017 Kansanedustaja Kulmuni: Synnytykset jatkuvat Kemissä ja Lappiin jää kaksi keskussairaalaa / J Tiihonen
- 12.4.2017a Vasemmistopuolueet vastustavat soten yksityistämistä Meri-Lapissa / A Heikinmatti
- 12.4.2017b Länsi-Pohjan sote voi ratketa Kemin demareiden kantaan / J Tiihonen
- 13.4.2017 Kemin demarit linjasivat: Ei Meri-Lapin sote-ratkaisulle / M Aula
- 24.4.2017 Kemi sanoi kyllä Meri-Lapin sote-ratkaisun edistämiseksi – Ylitornio tyrmäsi / J Mehtonen
- 25.4.2017 Meri-Lapin sote-ratkaisu aiheutti Kemin valtuustossa kiivasta keskustelua – näin valtuutetut äänestivät / J Mehtonen
- 28.4.2017 Konsulttiyhtiö tekee selvityksen Lapin sairaalatyönjaosta / J Mehtonen
- 30.5.2017 Länsi-Pohja sai yksityisiltä kolme tarjousta sote-palveluiden järjestämisestä / T Rantamartti
- 14.6.2017 Meri-Lapin sote pysähtyy kesän ajaksi – yksityisen palveluntuottajan valinta lykkääntyy / M Aula
- 5.7.2017a Vuoden aikalisä sotessa kelpaa Lapille kunhan valtio korvaa kulut / T Räihä
- 5.7.2017b Ritva Sonntag: Meri-Lapin sote-yhteisyrityksestä päättämistä pitäisi siirtää / A Heikinmatti
- 15.8.2017 Länsi-Pohjan keskussairaalaan uutta laitteistoa syöpä- ja sepelvaltimotautteja varten / R Rautiainen
- 21.9.2017 Tervola päättää uudesta sote-ulkoistuksen selvityksestä – kesällä ulkoistus kaatui Pihlajalinnan vetäytymiseen / J Tiihonen
- 26.9.2017 Henriksson: Uusi laki estäisi leikkaukset myös yksityissairaaloissa – lakialoite aluesairaaloiden tueksi saa kannatusta myös hallituspuolueista / A Vihanta
- 10.10.2017 Kattaako asiakasseteli vain osan kustannuksista? – Länsi-Pohjan sairaanhoitopiirin johtaja kaipaa tietoa soten asiakasmaksuista / J Tiihonen

- 19.10.2017 Lääkärit pelkäävät sairaalan alasajoa: Sairauskohtauksen hoitoviive voisi olla kohtalokas ja teollisuuden suuronnettomuus mahdoton hoitaa / J Mehtonen
- 23.10.2017 Mehiläiselle eniten pisteitä Länsi-Pohjan sote-yhteisyritykseen / J Tiihonen
- 27.10.2017 Meri-Lapista erittäin vähän hakijoita Lapin maakunta- ja sote-uudistuksen valmisteluun / J Tiihonen
- 3.11.2017a Kepuministeriltä tiukkaa sotesanelua Länsi-Pohjaan – “Törkeää poliittista vallankäyttöä” / T Rantamartti
- 3.11.2017b Sairaalan alasajo veisi Meri-Lapista kaikkiaan jopa 1000 työpaikkaa – kaupat, palvelut, koulutus ja asuntomarkkinat kärsisivät / J Mehtonen
- 3.11.2017c Lapin ja Länsi-Pohjan välit tulehtuneet – Lapin sairaanhoitopiirin johtaja ehdottaa avuksi “valtakunnan viisaita” / H Hannukainen
- 9.11.2017a Länsi-Pohjan työntekijöiden huoli mielenilmauksessa – “Ollaanko meidät hylkäämässä” / M Aula
- 9.11.2017b Meri-Lapin sote-tilanteesta kaksi mielenilmausta / M Aula
- 10.11.2017 Ministeriö lähetti Meri-Lapin kuntapäätäjille harhaanjohtavia lukuja tärkeää päätöstä edeltävänä yönä – “Jos ministeriöstä lähetetään jotakin, niin sen luulisi olevan faktaa” / J Mehtonen; K Marttala & M Aula
- 13.11.2017 Kemin kaupunginvaltuusto päätti sote-yhteisyritykseen liittymisestä äänin 22–21 / J Mehtonen
- 14.11.2017a Lapissa tehtiin historiaa: Kokonainen keskussairaala ulkoistetaan / M Aula
- 14.11.2017b Hallitus sai Meri-Lapin sote-pähkinän purtavaksi – valtuutetut päättivät jättiulkoistuksesta / J Mehtonen & M Aula
- 14.11.2017c Rovaniemi pettyi Meri-Lapin sote-ratkaisuun – “Onko Lapilla edellytyksiä jatkaa itsenäisenä” / J Tiihonen
- 15.11.2017a Kemiläispoliitikko sote-palveluiden ulkoistamisesta: “Oli musta aukko ja sitten oli jotain konkreettista” / L Haapanen
- 15.11.2017b Saarikko ärtyi terveysfirmoille – “Miksi suuryritykset samaan aikaan vaativat valinnanvapautta ja betonoivat nykytilaa?” / M Stenroos
- 15.11.2017c Hallitus yrittää estää Meri-Lapin taudin leviämistä – lakia tiukennetaan / M Stenroos
- 16.11.2017a Sipilä huolestui sairaaloiden kohtalosta: “Yksityiset monopolit ottavat asian haltuunsa” / V Sundqvist
- 16.11.2017b Analyysi: Sipilän hallitus koki kolauksen, kun Mehiläinen ja Meri-Lappi saapastelivat yli / K Tolkki

- 16.11.2017c Rajoittamislain tiukennukset vaikuttavat Tervolan sote-ulkoistukseen / J Tiihonen
- 16.11.2017d Tehyn uusi puheenjohtaja: Sotesta tulee vielä viides tuotantokausi / A Blencowe
- 17.11.2017a Meri-Lapin sote-ulkoistus etenee – Länsi-Pohjan sairaanhoitopiirin hallitus teki hankintapäätöksen tiukalla äänestyksellä / J Mehtonen
- 17.11.2017b Pitkään jatkunut väantö Lapin sairaaloiden kesken johti lopulta yksityistämiseen – “Ei tämä minusta ole mikään kapina” / M Aula
- 17.11.2017c Tervola hyväksyi yhteisyrityksen perustamisen – ulkoistuksen takana on nyt jokainen Meri-Lapin kunta / J Tiihonen
- 20.11.2017 “Me emme hyväksy tällaista keskittämispolitiikkaa” – Meri-Lapin keskustapäätäjät ärsyntyivät puolueen painostuksesta / K Vaara; J Mehtonen & M Aula
- 21.11.2017a Länsi-Pohjan sote-ratkaisu aluehallintoviraston syyniin – Lapin kuntien kädet ovat sidotut / P Tuukkanen
- 21.11.2017b Ministeriölähde: Länsi-Pohjan terveydenhoidon kallis ulkoistaminen veisi muun Lapin sote-rahast / M Stenroos
- 23.11.2017 Meri-Lapin sote-ulkoistuksen hinta vain murto-osa Lapin kuluista – “Ei ole tarkoitus mennä kenenkään muun rahoille” / M Aula
- 29.11.2017a Olisiko Lapilla mahdollisuus vielä löytää sote-sopu? Kansanedustaja patistaa kuntia palaamaan neuvottelupöytään / M Aula
- 29.11.2017b Sote-neuvottelut Mehiläisen kanssa alkoivat – Tornion kaupunginjohtaja: Yhteisyritys säilyttää terveyskeskukset / J Tiihonen
- 30.11.2017a Länskan psykiatriatalolle löytyi lopulta yhteinen tahtotila – “Kokouksessa ei tarvinnut edes äänestää” / J Tiihonen
- 30.11.2017b Rovaniemi hakee yhä sotesopua Lappiin – yksi sairaala, kaksi toimipistettä / M Talvitie
- 30.11.2017c Nousevatko asiakasmaksut? Kuinka pääsee hoitoon? – Selvitimme mitä Meri-Lapin sote-yhteisyritys tarkoittaisi potilaalle / J Mehtonen
- 30.11.2017d Ministeriö suitsisi kuntien jättiulkoistuksia ennakoitua tiukemmin – Länsi-Pohja oli viimeinen pisara / H Tikkala
- 1.12.2017 Lapin aluehallintovirasto antoi selvityksensä Meri-Lapin sote-yhteisyrityksestä – “Ei suuria huomioita, jotka olisivat yhteisyrityksestä sopimisen vastaisia” / J Mehtonen
- 4.12.2017 Pihlajalinna on valittanut Meri-Lapin sote-kilpailutuksesta markkinaoikeuteen / J Mehtonen
- 5.12.2017 Kemin vasemmisto äänesti Meri-Lapin sote-yrityksen sopimuskäsittelyn pöydälle – viivytystaistelu kiistetään / J Tiihonen

- 11.12.2017a Uusi käänne Meri-Lapin sotessa: Kemin kaupunginhallitukselle esitetään epäluottamusta – asia sai taakseen kannatusta ja etenee / J Mehtonen
- 11.12.2017b Kemin vasemmisto äänesti Meri-Lapin sote-yrityksen sopimuskäsittelyn pöydälle toistamiseen / J Mehtonen
- 14.12.2017a Meri-Lapin sote-ulkoistus on muuttumassa kilpajuoksuksi – rajoituslaki etenee pikavauhtia / M Aula
- 14.12.2017b Kemin päätös sote-yhteisyrityksestä pysyy – valtuusto ei pidä uutta kokousta maanantaina / J Mehtonen
- 19.12.2017 Kemin kaupunginhallitus myönsi kaupunginjohtajalle luvan allekirjoittaa sote-yhteisyrityksen sopimuspaperit / J Tiihonen & J Mehtonen
- 22.12.2017a Miljardin sote-sopimus allekirjoitettiin Meri-Lapissa – keskussairaala ulkoistetaan 15 vuodeksi / J Mehtonen & M Aula
- 22.12.2017b Hallitukselta tyrmäys Lapin sote-haaveille – ei erillisratkaisua Meri-Lappiin / A Passoja