”Et nää on näitä meiän kyberhyökkäyksiä nämä”

The government of one and all in everyday digital security in Finnish Lapland

Mirva Salminen

Acta electronica Universitatis Lapponiensis 339

Acta electronica Universitatis Lapponiensis 339

MIRVA SALMINEN

”Et nää on näitä meiän kyberhyökkäyksiä nämä” – The government of one and all in everyday digital security in Finnish Lapland

Academic dissertation to be publicly defended with the permission
of the Faculty of Social Sciences at the University of Lapland
in Esko ja Asko Hall on 20 May 2022 at 12 noon

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Rovaniemi 2022

University of Lapland
Faculty of Social Sciences

Supervised by:

University Lecturer, Docent Tapio Nykänen, University of Lapland

University Lecturer Mika Luoma-aho, University of Lapland

Reviewed by:

Professor Ilpo Helén, University of Eastern Finland

Docent Jyri Raitasalo, National Defence University of Finland

Opponent:

Professor Ilpo Helén, University of Eastern Finland

Layout: Taittotalo PrintOne

Cover: Reetta Korhonen

Acta electronica Universitatis Lapponiensis 339
ISBN 978-952-337-314-3
ISSN 1796-6310

URN http://urn.fi/URN:ISBN:978-952-337-314-3

ABSTRACT

The government of one and all in everyday digital security in Finnish Lapland
This study contextualises the gradual institutionalising of conventional concepts of cybersecurity by providing a more human-centric perspective. While discussion of cybersecurity can be encountered in daily news and in the workplace ever more frequently, its content and practical implications often remain abstract to everyday life. When cybersecurity is understandably addressed in highly technical and/or strategic terms, involving specific threat imageries and vocabularies, the mundane effects of the (un)successful securitisation of cyberspace can receive less attention. However, it is precisely these everyday effects that justify and undermine everyday cyber/digital security, and influence the respective security roles assigned to all citizens in emerging cyber-physical societies.

Drawing out commonalities and differences between human security and governmentality studies, this thesis critically examines the entanglement of digitalisation and cyber/digital security in Finnish Lapland: opportunities it provides and concerns it awakes in sparsely populated areas characterised by harsh climate, cultural diversity, long distances, and infrastructural issues, all of which relate to imagery of the Arctic as a developing region. It investigates the power relations and positions thus created, mainly through securitisation, development, and resilience. However, it also incorporates the related techniques of responsibilisation, human rights, commercialisation, surveillance and transparency, and, finally, techniques of the self, which aim at the assimilation of modern governmentality but also provide the means for its resistance. While digitalisation in Lapland is carried out with the stated aim of continuing service provision or improving it, it is efficiency and cost calculations that drive it.

Digitalisation and cyber/digital security are not generally examined together but as two separate trajectories. This thesis brings them together hence addressing both positive (freedom to) and negative (freedom from) security. It also provides localised research on the effects of digitalisation in the northernmost areas of Finland, Sweden and Norway, partially addressing a gap in the current knowledgebase. The research was carried out by problematising the mainstream framings of cyber/digital security from a number of individual security perspectives: applying human security to digitalisation and cybersecurity in the European High North, examining the interconnection of digitalisation and regional re-organisation of health and social services, studying the responsibilisation of the users of digital sharing economy platforms in contract law, and through a case study on the use of ICT and views on the requisite security roles amongst people living in Lapland. The synthesis re-problematises a human security approach to digitalisation through governmentality studies. This move visualises power relations embedded in human security that regardless of its emancipatory aim turn the approach to support modern governmentality through responsibilisation of individuals and communities for their own security and wellbeing. The theories and approaches covered in this thesis show that a multitude of human behaviours in digitality ought to be acknowledged and security practices able to accommodate it developed.

In the prevailing framings of cybersecurity, ICT corporations and states and/or societies are constituted as the main objects and subjects of security, whereas individuals are expected to behave in a digisavvy and safe manner and thus contribute to the overall effort of securing cyberspace. The main forms of public support in meeting the requirements of this kind of subjectivity are information provision, guidance and training, as well as societal accessibility policies. The aims of and values embedded in digitalisation remain unquestioned and increased connectivity is automatically expected to improve everyone's quality of life. However, digitalisation also leads to novel inequalities, power imbalances and dependencies – or aggravates the existing ones – and to a loss of self-sufficiency.

Digitalisation will not be turned around. However, as the power relations and positions it creates have not yet been firmly institutionalised, there is possibility to impact them, to turn them into networked relations that take people's needs, wants and wishes into account – instead of advancing digitalisation merely in the terms of technology and/or administration. Instead of approaching people as a vulnerability and hence in need of education and support, they ought to be viewed as subjects who can decide for themselves. At the heart of this struggle is the question of what kind of world we wish to live in.

Keywords: digitalisation, cybersecurity, digital security, human security, the individual, governmentality, the Arctic

TIIVISTELMÄ

Yksilön ja yhteisön hallinta arkipäivän digitaalisen turvallisuuden kautta Lapissa

Tutkin tässä väitöskirjassa kyberturvallisuuden tavanomaisia, vähitellen institutionalisoituvia käsitteellistyksiä ihmiskeskeisestä näkökulmasta. Samalla kun kyberturvallisuudesta on tulossa uutisten ja työpaikkakeskusteluiden vakioaihe, sen sisältö ja käytännön vaikutukset jäävät usein abstrakteiksi ja kaukaisiksi ihmisten arkipäivän kokemuksesta. Tekninen ja/tai strateginen lähestymistapa kyberturvallisuuteen jättää kyberavaruuden (epä)onnistuneen turvallistamisen arkipäivän vaikutukset suhteellisen vähälle huomiolle, mikä on aiheen teknisyyden ja turvallisuuspoliittisen merkityksen vuoksi ymmärrettävää. Samalla se kuitenkin tuo mukanaan tietyt uhkakuvastot ja sanastot aiheen käsittelyyn, mikä rajoittaa sitä, millaisia sisältöjä kyberturvallisuus voi saada ja millaisia politiikkatoimia siihen voi kohdistua. Siitäkin huolimatta, että juuri ihmisten arkipäivän kokemukset joko oikeuttavat tai kyseenalaistavat kyber-/digiturvallisuuden politiikkana ja ne turvallisuusroolit, joita kansalaisille kehittymässä olevissa kyber-fyysisissä yhteiskunnissa asetellaan.

Tarkastelen tutkimuksessa digitalisaation ja kyber-/digiturvallisuuden kietoutumista yhteen inhimillisen turvallisuuden ja hallinnan analytiikan teorioiden avulla. Keskityn digitalisaation avaamiin mahdollisuuksiin ja sen herättämiin turvallisuushuoliin Suomen Lapissa, jota luonnehtivat vähäväkisyys, kulttuurinen monimuotoisuus, haasteellinen ilmasto, pitkät etäisyydet ja infrastruktuurihaasteet. Edellä mainitut piirteet vaikuttavat siihen, että arktiset alueet mielletään usein kehittyviksi alueiksi ja niihin kohdistetaan tämän mukaisia politiikkatoimia. Mielikuvan mukaiset puhetavat ja käytännön toimet luovat valtasuhteiden ja valta-asemien verkoston, mitä havainnollistan pääosin turvallistamisen, kehityksen ja resilienssin tekniikoiden kuvauksen kautta. Kuvaukseen sisältyvät myös edellisiin liittyvät vastuuttamisen, ihmisoikeuksien, kaupallistamisen, valvonnan ja läpinäkyvyyden tekniikat, samoin kuin itsetekniikat, joilla pyritään modernin hallinnallisuuden sisäistämiseen, mutta jotka samalla mahdollistavat sen vastustamisen. Vaikka Lapin digitalisoitumisen julkilausuttu tavoite on ylläpitää tai parantaa palveluiden tarjontaa, sitä edistävät ensisijaisesti tehokkuus- ja kustannuslaskelmat.

Digitalisaatiota ja kyber-/digiturvallisuutta tutkitaan yleensä kahtena erillisenä kehityskulkuna. Väitöskirjassa tuon nämä kehityskulut yhteen ja tarkastelen niin positiivista (vapaus johonkin) kuin negatiivista (vapaus jostakin) turvallisuutta. Lisäksi kontekstualisoin tutkimuksen Suomen, Ruotsin ja Norjan pohjoisimmille alueille, joilta vastaavanlaista tutkimusta on suhteellisen vähän. Tutkimuksessa problematisoin kyber-/digiturvallisuuden valtavirran käsitteellistykset yksilöturvallisuuden eri näkökulmista: soveltamalla inhimillisen turvallisuuden lähestymistapaa digitalisaatioon ja kyberturvallisuuteen Euroopan pohjoisimmilla alueilla, tarkastelemalla digitalisaation ja alueellisen terveys- ja sosiaalipalveluiden uudistuksen välisiä kytköksiä, tutkimalla jakamistalouden digitaalisten alustojen käyttäjien vastuuttamista sopimusoikeudessa sekä tapaustutkimuksella Lapin asukkaiden tietotekniikan käytöstä ja näkemyksistä kyber-/digiturvallisuuden roolituksista. Väitöskirjan synteesi problematisoi inhimillisen turvallisuuden lähestymistavan uudelleen hallinnan analytiikan avulla. Tämä teko visualisoi inhimillisen turvallisuuden sisältämät valtasuhteet, jotka voimaannuttamispyrkimyksistään huolimatta ajautuvat tukemaan modernia hallinnallisuutta vastuuttamalla yksilöt ja yhteisöt heidän omasta turvallisuudestaan ja hyvinvoinnistaan. Väitöskirjan sisältämät teoriat ja lähestymistavat painottavat inhimillisen käytöksen moninaisuutta digitaalisuudessa, mikä pitäisi tunnistaa ja kyetä huomioimaan turvallisuuden käytännöissä.

Kyberturvallisuuden valtavirran käsitteellistyksissä tieto- ja viestintäteknologiayritykset sekä valtio ja/tai yhteiskunta ovat turvallisuuden pääasialliset viittauskohteet ja toimijat. Yksilöiden oletetaan toimivan taitavasti ja turvallisesti siten tehden oman osansa kyberavaruuden turvallistamisessa. Pääasialliset julkisen tuen muodot tämänkaltaisen toimijuuden saavuttamiseksi ovat tiedon tuottaminen, ohjaaminen ja harjoitukset, sekä erilaiset saavutettavuuspolitiikat ja -ohjelmat. Digitalisaation tavoitteita tai sen edistämiä arvoja ei kyseenalaisteta. Sen sijaan parempien viestintäyhteyksien oletetaan automaattisesti parantavan jokaisen elämänlaatua. Digitalisaatio kuitenkin tuottaa myös uudenlaista epätasa-arvoisuutta, vallan epätasapainoa ja riippuvuutta samalla kun se vahvistaa aiempia epätasa-arvoisuuksia ja riippuvuuksia sekä heikentää itseriittoisuutta ja omaehtoisuutta.

Digitalisaatio ei ole kehityskulku, joka on käännettävissä ympäri. Niin kauan kuin sen luomat valtasuhteet ja -asemat eivät ole vahvasti institutionalisoituneet, niihin voidaan vaikuttaa. Tavoitteena tulisi olla valtasuhteiden verkosto, joka huomioi ihmisten tarpeet, tavoitteet ja toiveet sen sijaan, että digitalisaatiota edistetään ainoastaan teknologian ja/tai hallinnon ehdoilla. Sen sijaan, että ihmiset hahmotetaan haavoittuvuutena ja siksi koulutuksen sekä tuen kohteena, heidät pitäisi nähdä toimijoina, jotka päättävät omasta puolestaan. Tämän valtataistelun keskiössä on kysymys siitä, millaisessa maailmassa haluamme elää.

Avainsanat: digitalisaatio, kyberturvallisuus, digiturvallisuus, digitaalinen turvallisuus, inhimillinen turvallisuus, yksilö, hallinta, hallinnallisuus, Arktis, arktinen

Prologue

Since beginning my Master's studies, I have been interested in how 'things' come to being. In that regard, having been able to participate in and study the introduction of cybersecurity to Finnish national and societal security discourses and arrangements has been a thrilling opportunity. The same has taken place with regard to cyber/ digital security in the Arctic.

The first time I encountered cybersecurity was in 2012, when I was asked to co-edit a book on the topic. Offense dominated discussion on cyberwarfare and our book was to highlight the importance of defence. "The Fog of Cyber Defence", co-edited with Jari Rantapelkonen, came out in 2013 and was downloaded from the website of the National Defence University over 800 times in the first 24 hours.

The same year I began working for Stonesoft, a Finnish cybersecurity SME, on another project. The first book on cybersecurity written in Finnish, "Kyberturvallisuus", was to be completed with Jarno Limnéll and Klaus Majewski. The goal of the book was to explain in an understandable manner what cybersecurity entails and how it can be managed in organisations. Finland was at the time developing her first national cybersecurity strategy and its implementation programme, so there was a clear need for such an opening. The book came out in 2014.

Next, I worked on an employee training package on cybersecurity for a Finnish conglomerate and developed research methodology for SaferGlobe, a peace and security think tank, which was partnering in the IECEU (Improving the Effectiveness of Capabilities in the European Union Conflict Prevention) project. In addition, the Finnish Defence Research Agency granted me a project on future warfare with the opportunity to work with a number of experts in the fields of digitalisation and cybersecurity. In 2016–18, I was co-investigating the strategic management of and the overall national arrangements for cybersecurity in Finland as a member of Aalto University's research team. The studies were carried out in collaboration with the University of Jyväskylä for the Prime Minister's Office.

In February 2016, I was asked to give a presentation on cybersecurity at the Arctic Centre of the University of Lapland. The twist was that I should give it from a human security perspective and contextualise it to the Arctic. I knew nothing of the Arctic and had associated human security with conflict zones and development studies. The presentation, however, went rather well for next we began developing a funding application, which success led to the ECoHuCy (Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North) project. The project was led by Kamrul Hossain, Director of the Northern

Institute for Environmental and Minority Law at the Arctic Centre, between 2017 and 2019. It was funded by NordForsk in cooperation with the Economic and Social Research Council (UK). Participants included UiT – The Arctic University of Norway, Swansea University (UK) and the Institute for Security and Development Policy (SE).

When the funders gave the green light to our project[1], I switched my original topic for a doctoral thesis, commercialisation of security, to human-centric cybersecurity. All articles and book chapters included in this thesis have been written for the project. One of the project's main outcomes was a book titled "Digitalisation and Human Security: A Multi-Disciplinary Approach to Cybersecurity in the European High North" co-edited with Gerald Zojer and Kamrul Hossain. It saw daylight in summer 2020.

In about ten years, cybersecurity has developed from a niche of information science and security studies to a more mainstream concept picked up by a number of disciplines and researchers in Finland (for an international reference, see Dunn Cavelty and Wenger, 2020). Within the same time period, the concept of cybersecurity has become more clearly defined and increasingly institutionalised. I have had the opportunity to follow this development from a number of interesting positions – which has not eased the task of completing a doctoral thesis on the topic.

The clarification and institutionalisation of concepts, their normalisation, takes place in theoretical and practical power struggles. It also generates particular relations of power and positions in them. "In brief, power is not homogeneous but can be defined only by the particular points through which it passes" (Deleuze, 1999, 23; also, Foucault, 2009b, 2). Therefore, it is not irrelevant whether cybersecurity is framed as a question of warfare, national security, business, continuity management, employee training, contract law, international law, wellbeing, or human and basic rights, as all these framings embed a different network of power relations and networked nodes. The synthesis part of this thesis scrutinises the conceptual manifoldness of cybersecurity in Finland, particularly in Lapland; its varying institutionalisations; and the power positions thus created, while the articles focus on digitalisation and cybersecurity from a human security perspective in the European High North. Particular attention is paid to the subjectivation of digisavvy individuals able to carry out their cyber/digital security responsibilities amidst the overarching digitalisation of everyday life.

The main observation of this thesis is that cyber/digital security and its subjects become mutually constituted in the discursive and material practices, through the techniques of security, which expand the dispositive of security to cyberspace and try to make the conduct of conduct governable in emerging cyber-physical societies.

[1] Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North (ECoHuCy) project was funded under NordForsk contract number 81030.

The conduct of behaviour is a strategic, goal-oriented activity that seeks to manage individuals and populations in the most efficient way, that is, by instructing and guiding them and facilitating their self-government towards a model perceived desirable for the aim of securing the society. These practices also constitute their own counterpart, that is, resistance to the attempts to govern behaviour in and with regard to cyberspace in the particular way. How all of the aforementioned takes place in the Arctic areas of Finland and produces individual subjectivities in cyber/digital security become described in this thesis.

According to Michel Foucault (1991, 194), "[w]e must cease once and for all to describe the effects of power in negative terms: it 'excludes', it 'represses', it 'censors', it 'abstracts', it 'masks', it 'conceals'. In fact, power produces; it produces reality; it produces domains of objects and rituals of truth." Moreover, "rather than assuming a generally acknowledged repression, and an ignorance measured against what we are supposed to know, we must begin with [...] positive mechanisms, insofar as they produce knowledge, multiply discourse, induce pleasure, and generate power; we must investigate the conditions of their emergence and operation, and try to discover how the related facts of interdiction or concealment are distributed with respect to them" (Foucault, 1998, 73).

Thus, in this thesis, the objective is to analyse the construction of certain forms of knowledge and truths regarding cyber/digital security in terms of power (after Foucault, 1998, 92) and producing particular kind of individual subjectivities. Power is understood "as the multiplicity of [...] relations immanent in the sphere in which they operate and which constitute their own organization"; as processes which transform, strengthen or reverse these relations; "as the support which these [...] relations find in one another [...] [or as] the disjunctions and contradictions which isolate them from one another"; and "as the strategies in which they take effect" (ibid., 92–93). Language is an essential component of knowledge and intertwines with power. Even if it "no longer bears an immediate resemblance to the things it names [...] [it continues] to be the locus of revelations and to be included in the area where truth is both manifested and expressed" (Foucault, 1994, 36, 42–43). "[L]anguage occupie[s] a fundamental situation to knowledge: it [is] only by the medium of language that the things of the world [can] be known" (ibid., 296).

Therefore, the first part of the title of this thesis is a quote from workshop discussions that I organised in the municipality of Enontekiö for data collection for article IV. Loosely in English: "So these are these our cyber attacks". In my view, it well captures the contextualised, everyday nature of cyber/digital security which this thesis is about.

While writing this thesis, and on top of climate change, the Arctic has been hit by two additional crises: Covid-19 and the Russo-Ukrainian War. The effects of neither have been considered in this thesis. On March 3, 2022, the seven other Arctic states condemned "Russia's unprovoked invasion of Ukraine and note[d] the grave impediments to international cooperation, including in the Arctic, that Russia's actions have caused". As a result, their "representatives will not travel to Russia for meetings of the Arctic Council" and the "states are temporarily pausing participation in all meetings of the Council and its subsidiary bodies". – Joint Statement on Arctic Council Cooperation Following Russia's Invasion of Ukraine[2]

[2] Ministry of Foreign Affairs of Finland (2022) Joint Statement on Arctic Council Cooperation Following Russia's Invasion of Ukraine on March 3, 2022. https://um.fi/current-affairs/-/asset_publisher/gc654PySnjTX/content/joint-statement-on-arctic-council-cooperation-following-russia-s-invasion-of-ukraine [March 21, 2022].

Acknowledgements

I would like to thank kindly the funders who have enabled the completion of this thesis: NordForsk, Suomen Marsalkka Mannerheimin Sotatieteellinen rahasto, Suomalainen strategisen tutkimuksen ja seurannan tukisäätiö (STRATU), and the University of Lapland Rector's grant. It would also not have been possible without good cooperation with the Municipality of Enontekiö and the institutional support provided by the Arctic Centre and the Faculty of Law of the University of Lapland.

I would like to express my deepest gratitude to all interviewees and workshop participants. Without your voluntary contribution this thesis would have remained a mere writing exercise.

The list of people to thank is long and non-exhaustive. First, my supervisors Tapio Nykänen and Mika Luoma-aho. Tapio in particular has had to bear my complex and wandering train of thought for some years now – and help organising it. Second, the pre-examiners Ilpo Helén and Jyri Raitasalo, who concluded that this thesis is worth defending; Ilpo for agreeing to be the opponent as well. Jan Hanska and Michael J. Laiho for crucial interventions when 'things' were not proceeding as smoothly as they could have. Jenna Päläs and Gerald Zojer for being 'brothers in arms' in the epic battles of thesis writing and book editing. Henri Wallén, Karolina Sikora, Laura Olsén-Ljetoff, Ilona Mettiäinen, Jussi Metsälä, Ilari Nikula, Ayonghe Akonwi Nebasifu, Adrian Braun, Dorothée Cambou, and Jan van den Broeke for the exchange of thoughts and hiking/skiing trips along the way.

Occasionally, seminars and conferences provide great conversations for rewiring thoughts for which I thank David Barnard-Wills, Jef Huysmans, Antoine Bousquet, Lukáš Likavčan, Christoph Humrich, and Heikki Huilaja. More often, fruitful cooperation develops over time for which I wish to thank Maria Mekri, Jarmo Pykälä, Mika Kerttunen, Eneken Tikk, Juha Saunavaara, Jouni Juntunen, Tuomas Kokkomäki, and Janne Autto. In addition, I owe a great deal to our ECoHuCy project partners Christer Pursiainen, Alan Collins, Michael Sheehan, Kristin Smette Gulbrandsen, and Johana Montalvan Castilla.

Without any less importance, I would like to thank Jari Rantapelkonen, Jarno Limnéll, Klaus Majewski, Ilkka Hiidenheimo, Timo Koivurova, and Kamrul Hossain for giving me a chance to prove that I know what I am doing – Elisabeth Rehn and Vilho Harle for telling me that I do when I myself doubted. Suvi Alt, Anna-Riitta Salomäki, Saara Särmä, Kaisa-Maria Tölli, Laura Valli, Saara Jantunen, Miikka Salonen, Jaakko Ailio, Christopher Lloyd, Clement Guitton, Andrew Carr, João Nunes, Antti Sillanpää, Christian Fjäder, Mika Aaltola, and Aki-Mauri

Huhtinen for early discussions on the topic. Marjo Lindroth for organising a PhD support group to the Arctic Centre.

Friends and colleagues at Stonesoft, the Arctic Centre and the Faculty of Law – thank you for the shared adventures inside, outside and in the borderlands of academia. Laurence Morris, Victoria Morris, and David Proctor for the essential escapes from thesis writing to the top of the world. Paula Partanen, Päivi Westerholm, Kaisa Kärkkäinen, and Susanna Jussila.

Finally, I would like to thank Mum and Dad for all their love and support. My brother Miika for saying the right things at the right time. Heli. Ella. Alku and Haiku.

Tromsø, April 17, 2022

List of Original Articles

The thesis is based on the following original articles, which will be referred to in the text by their Roman numerals I–IV.

I. Salminen, Mirva, and Kamrul Hossain (2018) Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record* 54(2), 108–118. https://doi.org/10.1017/S0032247418000268.

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.

III. Päläs, Jenna, and Mirva Salminen (2019) Alustan asiakkaan vastuusta ja vastuuttamisesta yksilöturvallisuuden tuottamisessa – sopimusoikeudellinen näkökulma kyberturvallisuuteen jakamistaloudessa. In: Päläs, Jenna, and Kalle Määttä (Eds.) *Jakamistalousjuridiikan käsikirja*. Helsinki: Alma Talent, 319–380.

IV. Mirva Salminen (2021) Arkipäivän digitaalinen turvallisuus Euroopan pohjoisilla alueilla: tapaustutkimus Tunturi-Lapista. *Media ja viestintä* 44(1), 158–180. https://doi.org/10.23983/mv.107305.

Articles I–IV are reproduced with the kind permission of their copyright holders.

Contents

1. Introduction

1.1 The power of metaphors: cooperation and competition

In late January 2019, the Northern Institute for Environmental and Minority Law (NIEM) in cooperation with the US Army Corps of Engineers organised a workshop "Governance for Cyber Security and Resilience in the Arctic" in Rovaniemi. The workshop was funded by the Emerging Security Challenges Division of the North Atlantic Treaty Organization (NATO) and brought together a number of scholars with varying backgrounds to discuss cybersecurity in the Arctic. One of the lessons learned was the power (and danger) of metaphors. In some of the statements, it was highlighted how information and communication technologies (ICT) were now rolled out to the Arctic and how the region could serve as a laboratory for technology testing for the rest of the world because of its harsh conditions and sparse population. Because, alongside serving as technology testbeds, the Arctic regions have been innovating in the use of ICT for their own needs since the 1960's and '70's, statements like these sounded slightly absurd (e.g. Hudson, 2015; Saunavaara et al., 2021). Reliable and affordable connections are missing merely in some Arctic areas with low population density (TFTIA, 2017, 10).

Similarly, a 2019 text on artificial intelligence envisions the development of the Arctic into a new frontier as "frontiers hold intrinsic potential for great conflict as well as great benefits, either of which could be accelerated by technology" (Lin and Allhoff, 2019, 193). Moreover, "the lessons here can inform the responsible development of other frontiers, such as outer space" (ibid., 194). Yet, the Arctic is not an extra-terrestrial no-man's-land waiting to be occupied, but an integral part of the Earth inhabited by people and animals who in the age of awakening global sense of responsibility ought to have a stake in the development of their life environment (e.g. Sharp, 2019). Furthermore, according to a news report, Nokia, alongside 13 other corporations, has already received funding from the National Aeronautics and Space Administration (NASA) to build a 4G network to the Moon (Laitinen and Keski-Heikkilä, 2020; see also Mikkonen, 2018). Statements like the aforementioned gain their meaning, however, against historical metaphors that constitute the Arctic as a frontier, an unexplored wilderness, a laboratory, a bellwether, and so forth. These metaphors remain highly influential when people imagine the Arctic.

Kathrin Stephen touched upon the Arctic metaphors in 2012: "There are two overarching metaphorical descriptions of the Arctic, one referring to the Arctic in terms of 'resources, opportunity and development' and the other in terms of 'conflict, competition and threats'". Indeed, any article search on the Arctic provides a number of texts, both scholarly and popular, discussing, for example, the Arctic exceptionalism in terms of successfulness of cooperation and peacefulness or the scramble for resources and increasing strategic importance of the region. According to Ingrid A. Medby (2019), who is leaning on the philosophy of Ludwig Wittgenstein, these kinds of metaphors are part of language games played by all stakeholders participating in the spatialization of the Arctic. The Arctic takes on a meaning through the use and context of language in diverse social practices. In order to make sense in these practices one needs to follow the rules of the game, that is, the common conventions for uttering and reasoning on the topic. The Arctic, thus, becomes produced in social interactions with others. (Medby, 2019, 124–126). One could add that the same interactions produce also the stakeholders; provide them with the right to use certain language in a credible manner, the institutional sites from which certain discourses can be utilised, and the situations in which the stakeholders become determined (see Foucault, 1998, 11, 18; 2009a, 55–61). They also condition what cannot be spoken about (Foucault, 1998, 27, 53).

When I began attending Arctic research seminars and conferences back in 2016, ICT researchers and/or corporations were not present in plenty. Moreover, even if digitalisation was recognised to take place in the Arctic, cybersecurity seemed not to be an issue at all. Even in two Arctic security expert workshops organised by highly appreciated think tanks (2017[1] and 2019[2]) the topic was virtually absent. At the same time, all eight Arctic states were directing their intellectual power, time, and material resources to the development of national cybersecurity, and ICT corporations were rising in the ranks of most valuable corporations worldwide. Digital espionage, cybercrime, cyber operations, and information influence – amongst other threats residing in and/or utilising ICT networks and/or equipment – were on the rise. Even if the lack of Arctic focused cybersecurity discussion may seem to suggest that the Arctic exceptionalism has spilled over to cyberspace[3], the more likely explanation is that while digitalisation has been framed also as a regional development issue, the main framings of cybersecurity are technology and/or national security centred. Yet, since 2016 cybersecurity awareness has been arising alongside the claims for improved broadband in the Arctic regions. In October 2019, a panel NIEM

[1] RAND Europe organised "The future of Arctic cooperation in a chancing strategic environment" table top exercise on June 6 and 7, 2017 at the Norwegian Institute of International Affairs (NUPI) in Oslo.

[2] Konrad Adenauer Stiftung organised "Melting Security: How the speed of the Arctic's geographical transformation forces its new and old stakeholders to act" roundtables on September 23–25, 2019 at Radisson Blu Hotel in Tromsø in collaboration with UiT – The Arctic University of Norway and The Norwegian Atlantic Committee.

[3] "Cyberspace should be understood as a metaphor" and as a construction. It is "a physical construction produced by networking information technology" and "a social construction shaped by the way that people and institutions think, understand, and talk about this space". (Barnard-Wills and Ashenden, 2012, 111.)

organised on digitalisation and cybersecurity from a human security perspective in the European Arctic at the Arctic Circle Assembly in Reykjavik hosted a full room.

The very same metaphors of cooperation and competition are present in the discussions around digitalisation and cybersecurity. Their exact content differs, but they are nonetheless utilised in the spatialization of cyberspace in a similar manner as in the spatialization of the Arctic. In general, but particularly in the Arctic, digitalisation is equalled with digital development, which increases opportunities and efficiency in the use of resources. It also eases everyday life. ICT are perceived as general-purpose technologies that produce network benefits, which cannot be generated by other means (Ministry of Local Government and Modernisation, 2016). As general-purpose technologies they are also seen as somewhat neutral tools (cf. Salminen and Hossain, 2018, 111; Salminen, 2021, 162).

Network benefits require networked actors who generally benefit from the cooperation or value the cooperation itself more than its possible hindrances. Much of this interaction takes place on digital platforms, which do not solely facilitate and format networking activities, but become constructed in these everyday activities alike (van Dijck, 2013, 6–7). Social media platforms in particular "are tweaked in response to their users' needs and their owners' objectives, but also in reaction to competing platforms and the larger technological and economic infrastructure" within which they evolve (ibid., 7). According to José van Dijck (2013, 11–14), human connectedness as a social value and automated connectivity, that is, automated engineering and manipulation of relations between human beings and other 'things' into algorithms, both play a major role in the emerging culture of global connectivity. Digitalisation is hence valued for the opportunities it provides to different actors, but the values inscribed in these opportunities vary.

In the Arctic, digitalisation indicates double-development: digital development within regions that are considered as developing regions from the perspective of state/federation capitals and/or Brussels. In these perceptions, the Arctic manifests simultaneously as a threatening, disordered space that is going through rapid changes and an enchanted, idealised space of natural beauty and non-materialistic local aspirations (see Pupavac, 2010, 692, 707). Being able to tap into the crucial flows of information, knowledge, capital, human resources, commodities, material, tourists, and so forth seems to be the living condition of the Arctic regions. If failing to do this, these areas are believed to be doomed to regression. (See e.g. Castells, 2010; Aaltola et al., 2014.) Digitalisation is hence thoroughly securitised. I do not refer with securitisation to a specific school of thought in critical security studies, the so-called Copenhagen School (cf. Salminen and Hossain, 2018, 112), but to Michel Foucault's observations about the dispositive of security, including that the question of security is essentially a question of circulation.

According to Foucault, the societal aim of effective government is linked to the intensity of circulation of 'things', which can be improved by development and protected by minimising what is risky. ‘Things’ include people, goods, services, and material givens such as water and air, but also ways of acting and thinking, habits and customs, as well as events of different kind. Circulation of the acceptable kind of ‘things’ is supported while circulation of what is dangerous is slowed down, weakened, or temporarily stemmed. The aim hence is to control circulation by impacting the material on and with which it is provided. In addition, circulation is controlled by impacting its constraints and limits, facilities and encouragements, as well as the set of regulations that allow it to take place. (Foucault, 2009b, 13–15, 19–21, 64–67, 325–326; cf. Abrahamsen and Williams, 2011, 50.)

One of the technologies of such control is development understood “as attempting to contain the circulatory and destabilizing effects of underdevelopmen[t]” (Duffield, 2007, 19). The developmental discourse is very similar in national and regional strategies related to digitalisation (see Salminen and Hossain, 2018; Salminen, 2018a; Salminen, 2019). Yet, the challenge lies in financing. As “private investment may be difficult to attract to Arctic […] projects given the high cost of deployment and often small clusters of customers”, public-private partnerships and the continuity of government support in different forms are presumed (AEC, 2017, 3–4). This challenge has remained similar from an information infrastructure development project to another (see Hudson, 2015; Salminen, 2018a; Salminen and Hossain, 2018; Salminen, 2019; Saunavaara et al., 2021).

Another, related technology is resilience which includes the responsibilisation of individuals – but also of communities, organisations, regions, etcetera – for their own wellbeing and security. Resilience in and with regard to cyberspace is called for by the acknowledgement that all possible threats cannot be prevented or countered and disturbances will take place, which makes it essential to be able to continue operating even under great stress and/or when some components of the system are down. As important are the abilities to recover quickly and to learn from the experience. (Limnéll et al., 2014, 242.) In the Arctic, resilience refers to “the capacity of communities and systems to recover and restore themselves from various kinds of crises and disturbances” (Arctic Council, 2020). It incorporates the idea that individuals and communities are the first line of response for the sheer distances prevent, for instance, effective state response arriving from more populous areas on time. This Arctic conceptualisation of resilience has not seriously incorporated cyber/digital security so far.

The spatializations utilised in this thesis vary. At the metaphorical level, I use ‘the Arctic’ to awake the mental images that are most commonly hold of the northernmost regions of the Arctic states. This is necessary in order to draw attention to the differences within these states, albeit they are often discussed (and most commonly statistically produced) as homogeneous entities. Everyday life in Kaamanen (in Inari) is different from everyday life in Kulosaari (in Helsinki). The four articles written as part of the ECoHuCy project utilise ‘the European High North’ as their spatial anchor, for the project mainly discussed the northernmost areas of Finland, Sweden and Norway. In this synthesis, I focus on the government of individuals in the Finnish society and living their everyday lives in the Finnish Arctic, that is, in Lapland.

I have excluded from the analysis a number of international (e.g. the United Nations (UN) and the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), NATO), supra-national (e.g. the European Union (EU)), multinational (e.g. the World Wide Web Consortium (W3C)), and transnational (e.g. Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Society) actors and structures that play a role in the construction of digital Lapland. I have done this limitation for analytical reasons, that is, in order to be able to claim something sensible about a complex, global phenomenon that touches upon all aspects of life and virtually intrudes into all structures of society. Covering this development in all eight Arctic states or at all levels of global governance touching upon digitality would have been too much.

Moreover, I focus on the practices of digitalisation and its securitisation as cybersecurity and digital security. The technology-focused concepts like information security, network security, or data protection and privacy receive less attention as those are in my reading included in the aforementioned wider concepts that operate at the levels of individual, groups, population, society, and the state. Finally, all spatializations are about the construction of order; about relating things to one another so that they begin to make sense (e.g. Foucault, 1994, xx–xxii; 2009a, 30–32, 41). The contingent and fluctuating order that I am interested in is the multiplicity of relations between human beings and other 'things' in the dispositive of cyber/digital security embedded in everyday life in Finnish Lapland.

The theoretical mix in this thesis comprises Foucault's and Foucault inspired accounts of modern governmentality as well as a human security approach to digitalisation and cybersecurity in the European High North. The four articles constituting the empirical part of this thesis build on human security while this synthesis examines the government of society through the production of individual subjectivities in digitalising security practices. A human security perspective to digitalisation is in itself a critical approach towards the mainstream, technology and/or national security focused accounts of cybersecurity. As it will be explained in section 1.3 and articles I, II, and III, it moves the referent object of cybersecurity from information and information infrastructure and/or vital societal functions to individuals and communities, which transforms both the requisite threat imagery and the security measures available to counter the thus identified threats.

However, when studying for and writing the articles, I began to wonder what kind of societal order the aspired empowerment but consequent responsibilisation of individuals and communities in digitality produces. This pondering led me to governmentality studies and theorisation on the production of 'right kind of', governable individuals and populations, which, I believe, sharpens the analysis of the contemporary rationality of government that takes digitalisation as a self-evident, positive trajectory to which advancement people need to adapt. It is not enough to argue that people need to be educated and trained to use ICT or financially supported in acquiring the technology so that digital divides can be bridged and everyone's participation in cyber-physical societies ensured. The entire societal order built on digitalisation and comprehensive cybersecurity that requires an undefined level of digital literacy and awareness from people needs to be visualised and problematised instead. Therefore, the research question to which this thesis seeks to answer is: *How does the government of the emerging digitalised everyday life take place in Lapland through the production of individual security?*

The outline of this thesis is the following. In the introduction, I first touch upon the discursive and material practices in which digitalisation and cyber/digital security become produced in the Arctic, in Finland, and in Finnish Lapland. Then I begin discussing modern governmentality that serves as the analytical framework within which the scrutiny of the production of individual security in and with regard to cyberspace is carried out in the rest of the synthesis. I introduce the concept of dispositive and how security operates as a dispositive in modern governmentality.

The second part summarises the four articles that constitute the empirical part of this thesis. They all discuss the everyday security of individuals and communities amidst advancing digitalisation either from a human security perspective in the European High North or from a human security inspired governmentality viewpoint. The main argument of this synthesis is that while being a highly valuable critique of the mainstream framings of digitalisation and cybersecurity, human security still supports modern governmentality. Instead of seeking subject positions that adapt to or sustain digitalisation the way it is currently taking place, a more radical critique problematising the emerging cyber-physical societal order ought to be conducted.

The third part then is the main theoretical part of the synthesis. First, I immerse in governmentality as a governmental rationality directing the conduct of conduct in digitality through both government of the self and of others. Governing is understood as a ubiquitous compilation of techniques that influence the behaviour of both individuals and groups of individuals of which population is the widest. These techniques produce both objects and subjects of cyber/digital security of which my main interest lies in the production of individuals as knowable, skilled, obedient, and responsible digital citizens capable of participating in national cybersecurity arrangements – and in the emerging cyber-physical society in the first place. This section brings together a number of perspectives from governmentality studies that shed light on the discursive and material practices in which digisavvy citizens and cyber/digital security become produced and which were also brought forth by the aforementioned articles. However, it also discusses resistance to current forms of digitalisation that takes place in Lapland.

The fourth part of the thesis provides some concluding remarks from the overall effort. Its main contribution is tying the sprawling discussion about cyber/digital security from multiple viewpoints to the individual. In addition, it envisions ways to incorporate freedom in digitalisation as something more than the ability to choose between 'the right options' as a digisavvy, responsible, transparent, and resilient subject living in the developing Arctic.

1.2 Framing digital development and security in the Arctic

1.2.1 The Arctic Council and the Arctic Economic Council

The Arctic governance bodies[4] have gradually picked up the theme of digitalisation under the labelling of 'telecommunications' and digital 'connectivity' and, thus, participated in the production of the digital Arctic. The Arctic Council[5] chairmanships of the United States (2015–17), Finland (2017–19) and Iceland (2019–21) had connectivity in a format or another included in the agenda (see the United States Department of State, 2015; Ministry of Foreign Affairs of Finland, 2017; Government of Iceland, 2019). The Council also ran a Task Force on Telecommunications Infrastructure in the Arctic (TFTIA) between 2015 and 2017[6]. Its mandate was to "coordinate a circumpolar assessment of telecommunications infrastructure and networks. The Task Force would deliver a completed assessment to include, among other things, recommendations for public-private partnerships to enhance telecommunications access and service in the Arctic." (TFTIA, 2015, 1.) "In establishing the TFTIA, the Arctic Council recognized the importance of

[4] The Barents Euro-Arctic Council has been excluded from the analysis because its geographic reach extends the northernmost areas of Norway, Sweden and Finland that were on the focus of the ECoHuCy project.

[5] "The Arctic Council is the leading intergovernmental forum promoting cooperation, coordination and interaction among the Arctic States, Arctic Indigenous peoples and other Arctic inhabitants on common Arctic issues, in particular on issues of sustainable development and environmental protection[.] [...] The Council's activities are primarily conducted in six Working Groups and one standalone Expert Group that cover a broad field of subjects, from climate change to emergency response [and] mental health[.]" The Arctic Council (n/d) About the Arctic Council. https://arctic-council.org/about/ [March 9, 2022].

[6] Prior to this task force, the Arctic Council had discussed information and communications technologies in the early 2000's. See e.g. Hickel, Walter J. (2003) Closing the Digital Abyss: Options for Arctic Telecom. Workshop report. Anchorage (AK): Institute of the North. https://oaarchive.arctic-council.org/bitstream/handle/11374/584/ACSAO-IS02_9_Infrastructure_ICT.pdf?sequence=1&isAllowed=y [March 20, 2022]; The Arctic Council (2004) ICT in the Arctic. Discussion paper. https://oaarchive.arctic-council.org/bitstream/handle/11374/337/ACSAO-IS03_9_Discussion_Paper_ICT.pdf?sequence=1&isAllowed=y [March 20, 2022]; The Arctic ICT Network Drafting Committee (2006) Arctic Information and Communication Technology Assessment (AICTA). Proposal and Rationale. https://oaarchive.arctic-council.org/bitstream/handle/11374/677/ACSAO-RU03_9_1_AICTA.pdf?sequence=1&isAllowed=y [March 20, 2022].

telecommunications as a factor for sustainable development in the Arctic" (TFTIA 2017, 9).

TFTIA's work was continued by a Task Force on Improved Connectivity in the Arctic (TFICA) from 2017 till 2019, which mandate was to "compare the needs of those who live, operate, and work in the Arctic with available infrastructure, and to work with the telecommunications industry and the Arctic Economic Council to encourage the creation of the required infrastructure with an eye toward pan-Arctic solutions and to report […] in 2019" (TFICA, 2019, 13). "[T]he group focused on understanding user needs while it explored new technological solutions, commercial opportunities and industry best practices" (ibid., 11).

TFTIA's main findings included a need for contextualised multi-technology solutions for improving connectivity in the Arctic, where "dependence upon a single system or provider creates vulnerabilities"; a major difference in connectivity exists between more and less densely populated places; and reliable and affordable broadband is lacking in some of the most rural areas (TFTIA, 2017, 87). Connectivity is crucial for it "supports better access to education, healthcare, and commerce, as well as enhancing citizens' participation in civic life and improving delivery of services" and "is important to indigenous peoples in maintaining and preserving their cultures and livelihoods" (ibid.). It improves the opportunities for data collection, preservation and transfer; benefits airspace and maritime users and supports the safety of their operations; and "is essential to the conduct of search and rescue operations in the Arctic" (ibid., 88).

Moreover, improved connectivity supports economic development locally; especially, the growing tourism industry. However, it also requires that the Arctic states streamline regulatory processes and are willing to continue investing in infrastructure development one way or another. (TFTIA, 2017, 88–89.) In the future development of the Arctic information infrastructure, "the needs of indigenous peoples and local communities, and those operating in the Arctic such as businesses, tourism, and researchers" ought to be included alike (ibid., 89; see also AEC, 2017, 27).

Yet TFICA continued that "[b]uilding and maintaining infrastructure in many areas of the Arctic is challenging due to the terrain, harsh climate, vast distances, and dispersed populations. […] In addition […], a higher cost environment and challenges with staffing [affect] the deployment of network infrastructure […]. Specific issues cited [in stakeholder communications] were the costs of deploying and maintaining connectivity infrastructure in areas that lack road access and are not connected to an electrical grid. […]. [S]taffing can sometimes be challenging due to an insufficient availability of specialized contractors [and the] process of recruiting, training, and retaining local workers is […] often difficult." (TFTICA, 2019, 24.) Moreover, "clarity over the process and timelines is critical because, due to weather patterns, installation often needs to take place during narrow windows of opportunity" (ibid., 26).

TFTICA (2019, 38) also recognised "that improvements in Arctic connectivity are a long-term effort that will require continued and expanded cooperation and collaborations among the users in the Arctic and with the industry". It expected that "existing and emerging connectivity technologies […] become more widely available in the circumpolar regions" over the next few years; recognised that "[t]here is a new trend of data centers emerging in some Arctic states"; and highlighted the criticality of network redundancy in Arctic conditions (ibid., 46; see also AEC, 2017, 12–13). My own research (Salminen and Hossain, 2018; Salminen, 2018a; Salminen, 2021), findings of the ECoHuCy project (e.g. Salminen et al., 2020a; Trump et al., 2020; Zojer, 2019a) and research more widely (e.g. Hudson, 2015; Kilpeläinen, 2016; Lehto et al., 2019; Saunavaara et al., 2021) mention similar opportunities for and challenges to digitalisation in the Arctic as these reports.

Similarly, the Arctic Economic Council (AEC)[7] has worked on the topic of broadband from 2016 onwards and organised three subsequent "Top of the World: Arctic Broadband Summits" (Barrow [currently Utqiaġvik] in 2016, Oulu in 2017, and Sapporo in 2018). The AEC Working Group on Infrastructure: Telecommunications concluded its work in 2017 by publishing "Arctic Broadband – Recommendations for and Interconnected Arctic" report. The report was to "take stock of the current state of broadband in the Arctic, and to make recommendations as to how to facilitate broadband deployment and adoption", because "broadband has the power to transform society and enable new and more robust ways of interacting with one another" (AEC, 2017, 3). According to it, "[r]eliable broadband is necessary to promote and advance interconnectivity, which in turn facilitates improvements in national economies, education [distance learning], health [telemedicine], and may other sectors of society" (ibid., 5). More specifically, it facilitates the business models of e-commerce; new ways of enhancing citizen participation in politics and community involvement; and e-government as "the use of information and communication technology to enhance the range and quality of public services to citizens and businesses while making government more efficient, accountable and transparent" (ibid., 9–10).

Broadband also "enables new and more robust ways of conducting scientific research" and "is essential to trade and transportation in the Arctic" (AEC, 2017, 11). Furthermore, it "enhances individual's lives […], allowing them to interact and prosper (whether economically, educationally, politically or culturally) in ways not possible before" (ibid., 9). However, because of the "extreme challenges" posed

[7] The Arctic Economic Council, established by the Arctic Council and consisting of businesses operating in the Arctic, is "an independent organization that facilitates Arctic business-to-business activities and responsible economic development[.] […] [Its] goal is to share and advocate for best practices, technological solutions, and standards. [It] support[s] market accessibility and provide[s] advice and a business perspective to the work of the Arctic Council." The Arctic Economic Council (n/d) About. https://arcticeconomiccouncil.com/about/ [March 9, 2022].

by the Arctic conditions, the region was "in danger of being left behind" in the development of connectivity (ibid., 3, 5). The findings of the AEC working group hence support those of the Arctic Council task forces and wider research. Its work has been continued by the AEC Working Group on Connectivity, which mandate is "to facilitate improved connectivity and sustainable economic development for the people and businesses in the Arctic" (AEC, 2018, 2).

These lengthy extracts from the reports of the Arctic governance bodies serve as an example of the discursive practices, also describing the material practices, in which the digitalisation of the Arctic and its securitisation take place. Articles I and II of this thesis do the same with regard to national and regional digitalisation and cybersecurity strategies of Finland, Sweden and Norway. The framing in the pan-Arctic reports echoes the national and regional strategies as the main purpose of advancing digitalisation – through infrastructure development; regulation, for example, setting caps to consumer costs; and utilisation of digital means in the provision of public services – is to reduce administrative costs and to support sustainable economic development, but also to support social development. The latter entails improved opportunities for interaction across time and space, for sustaining indigenous and other local cultures, as well as for citizen participation and the flourishment of individuals. Equality in internet access and reliability of connections ought to be advanced as well. Thus, the pan-Arctic reports on connectivity align with the principles of human security in seeking to reduce everyday insecurities and improve human wellbeing (see e.g. Salminen et al., 2020a).

Improved access to information and basic services, support to information generation and research activities, criticality for airspace and maritime actors as well as for search and rescue, and communities' vulnerability due to thinness of the infrastructure serve as further justifications for continuous information infrastructure development in the Arctic. High development costs, natural constraints, challenges in human know-how, and unaddressed regulatory needs hinder the development of both infrastructural and social layers of the digital Arctic. The embeddedness of security in the framing is evident for the fear of being excluded from global digital development, and the requisite circulation of positive 'things', lurks on the background. However, the understanding of security comes closer to what in human security is regarded as 'freedom from want' and 'freedom from indignity' than 'freedom from fear' (for the definitions of these freedoms, see 1.3.4), which tends to dominate cybersecurity agendas (see Salminen and Hossain, 2018; Salminen, 2019; Salminen et al., 2020b; Zojer, 2019a).

Thus far the Arctic governance bodies have remained silent about cybersecurity and digital security. The likely explanation for this silence is that they are not mandated to take a stance on national security issues and lack technical expertise. Albeit sidelining the aforementioned security concepts, they also explicitly acknowledge the interconnection of connectivity and security and safety in the Arctic regions. For instance, according to the AEC Working Group on Infrastructure: Telecommunications "[a]ccess to secure broadband is critical to national interests such as state security and defense. [...] Given the likelihood of increased communications support requirements arising from [economic and military] operations, expanded broadband deployment should be a priority. More generally, the ability to easily locate and quickly exchange data [...] is essential to ensuring the security of the nation-state as well as the safety of citizens at home and abroad. [...] Broadband also provides a window into the activities of anti-government groups or individuals and supports numerous technologies critical to national defense." (AEC, 2017, 10–11.) Next to that, "[a]ccess to high-speed Internet facilitates communication and allows for more precise disaster planning and response. It [...] reduces the cost of operations and allows public safety officials to allocate scarce resources more effectively. [R]eliable broadband can assist in organizing and analyzing data in a meaningful way so that officials can make realtime decisions in "life and death" situations. [B]roadband [also] plays an important role is search and rescue [...] operations." (Ibid., 11–12.)

These kinds of interlinkages of digitalisation, cybersecurity, national security, and everyday safety were mentioned in discussions with the inhabitants of the Arctic alike, but the likelihood of, for example, a cyber event halting societal functions was perceived low and its consequences so damaging that it did not receive much everyday pondering like article IV testifies (Salminen, 2021, 171). The findings from empirical research thus verify a priori observations made by reading the technical and national security focused cybersecurity agendas: There is much more to everyday cybersecurity in the Arctic regions than fast broadband, national security and defence, disaster management, search and rescue, and undisturbed technical functioning of ICT.

1.2.2 The Regional Council of Lapland

In Finland, the Regional Council of Lapland (RCL)[8] published a digitalisation programme in 2013. It was assembled as a regional development project and laid out the development of digital Lapland by 2020. The programme's foreword points out how "the digitalisation of society changes the way we live our lives and do our work". It then highlights the need to gather information about user expectations in order to reconcile digital service formats and human ways of doing things. (RCL, 2013, 4.) Currently, information society is making a leap in Lapland, which is supported by a vision of digital Lapland that is based on Arctic know-how and the northern

[8] The Regional Council of Lapland is "a statutory joint municipal authority, the members of which are all of the 21 municipalities of Lapland". Its core tasks are "the strategic development of the region, planning and safeguarding the interests of Lapland at both the national and international level". "The highest decision-making body [...] is the Assembly of the Council, and practical work is overseen by the Board of the Council". The Regional Council of Lapland (n/d) About us. https://www.lapinliitto.fi/en/information/the-regional-council-of-lapland/ [March 9, 2022].

quality of life. Lapland's future profile consists of "innovative experimentation, smart specialisation, and agile solutions". Long distances and the sparsity of population ought to be seen as a competitive edge to develop open-minded, ground-breaking solutions supporting green technology and novel operating models. The regional goal is to become a "continuously regenerating powerhouse that keeps the Finnish knowledge society going". "Deliberation, creativity, quality of life, and easiness" constitute the common building ground. Lapland remains a technology testbed and aims to be a trailblazer amongst the Arctic digital societies. (Ibid., 5.) The discourse could not be further away from the statements presented at the very beginning of this introduction (1.1) which assumed that ICT are now finally rolled out to the Arctic. Instead, Lapland prepares to excel in global competition with the help of digital means.

The digitalisation programme for Lapland has five objectives. First, to recognise better gaps in the digital literacy of citizens, entrepreneurs, and officials and to provide education and training to improve know-how. The purpose is to ensure equal opportunities to everyone to societal participation and service use, as well as to invigorate the local cultures, communities, and villages via strengthening interaction and creating virtual environments that facilitate belongingness. Second, to engage local businesses of different size in the shared regional operational model, digital (service) development, and the generation of new business ideas. Third, to facilitate the development of educational and research institutions into forerunners of digital society, for example, with regard to distance learning, smart traffic, and tourism services. Fourth, to transform public administration so that running errands digitally becomes feasible. Public administration develops digital services and provides testing environments, but it should also question its own structures and procedures. Especially, digitalisation of municipal services is called for, which in many places requires cooperation across town and municipality borders. Local democracy and the forms of participation are to be renewed and accessibility of services improved. Fifth, information infrastructure must be developed further so that, for example, broadband is available to all citizens and businesses in Lapland. (RCL, 2013, 6–8, 13, 21–22.)

Even if the digitalisation programme clearly discusses development, it does not focus on connectivity like the Arctic governance documents, but on a dynamic societal change and making digitalisation work for the region, its businesses, and its inhabitants. The aim is to provide new solutions in content areas in which Lapland has potential to be amongst the best in the world. In addition, renewals are required in livelihoods and services because of, for example, weakening municipal economies, decreasing and aging population, reduction in places of training, and long distances. (RCL, 2013, 9–10.)

The programme for Lapland also stays silent about cybersecurity. However, like the Arctic governance documents, it perceives people's digital literacy a precondition for development; calls for the inclusion of the whole population and all cultural groups in digital development; sees the need to ensure the availability of skilled workforce; and aims to remove the obstacles caused by gaps in digital infrastructure, people's and organisations' attitudes, and operational models (RCL, 2013, 13, 16, 19, 21, 27). What needs to be secured is the continued provision of education, training and guidance; funding for infrastructure projects and hence the availability of affordable connections; accessibility of information and services; and environmental sustainability (ibid., 19, 22, 24, 27, 29). Alongside economic development, social inclusion is strongly emphasised – in the development of services and operational cultures, through transparency and improved participation in local decision making, by opening data, and as a way of preventing alienation (ibid., 13, 21–22, 24). Tailoring services to each individual's needs is seen as a way to ensure equality in everyday life. That is, through the individualisation of customers, everyone's wellbeing is believed to be best supported. The role of public administration is to remove obstacles and improve conditions, provide services, and contribute to the viability of local economy and ICT companies. (Ibid., 21–22.)

Security is thus embedded in the programme for Lapland as it is in the Arctic governance documents. Next to that, "[i]n the construction of novel know-how and service models all actors have their own roles. The programme's implementation depends upon citizens, the third sector, educational and research institutes, business, as well as state and municipal administration" (RCL, 2013, 11). Responsibility for ensuring successful implementation, and hence safeguarding the attainment of desired values, is laid on the shoulders of everyone as it is in the Finnish comprehensive (cyber)security model introduced in section 1.3.2.

The main items in the digitalisation programme for Lapland do not differ from those in the Arctic governance documents, but the discursive practices do. The fear for being left behind in development is not present, but the aim is to utilise the digital tools in making Lapland a leading region in its strongholds in Finland and in the circumpolar context. Possible explanations for this can be sought, for example, from the fairly well-developed information infrastructure, long-term experience with the utilisation of digital means to overcome challenges related to distances and low population density and with the development of digital solutions to local needs, and national policies that have supported digital development in Finland since the 1990's (see Salminen and Hossain, 2018; Salminen, 2019; Salminen, 2021).

However, the programme for Lapland stands in an interesting contradiction, for example, to the Ministry of Finance's survey on the digital municipal services in Finland conducted in 2020. The survey included only one town (Kemi) and one municipality (Savukoski) from Lapland, excluded health and social security services which digitalisation has been a priority in Lapland for years (e.g. Lapland Hospital District, 2007; Lapland Hospital District et al., 2011; 2016), and covered merely 15 municipal services which mainly related to licencing services; application, booking and enrolment; farm relief service; and e-library services. The study came to three main conclusions: (1) the bigger the municipality or town, the wider the digital service selection and the more advanced services, (2) when several towns and municipalities use the same service, the service is more advanced, and (3) when a service provider provides less services, the services are more advanced. (Ministry of Finance, 2020c, 2–7, 12.) In the national comparison, both the town and the municipality from Lapland placed slightly under the average of municipalities from mainland Finland regarding how advanced the municipal digital services are[9].

The Ministry of Finance began allocating financial support to the development of digital municipal services in 2019 when Government Decree on the Incentive Scheme for Digitalisation in Municipalities (893/2019)[10] took effect. In 2019, a consortium of 12 municipalities, a town, and the Regional Council of Lapland received support for automating financial administration and developing information management (Ministry of Finance, 2019). In 2020, three consortiums from Lapland (led respectively by the towns/municipalities of Rovaniemi, Salla and Posio) received digitalisation funding (Ministry of Finance, 2020d).

1.2.3 Digitalisation as defined in this thesis

In this thesis, digitalisation is understood as digital development that has two aspects: (1) the increasing use and dissemination of ICT in virtually all aspects of human life, which (2) begins to influence, shape and (re)structure not only life environment, but life itself (see Brennen and Kreiss, 2014; Salminen, 2019, 322, footnote 2; Salminen, 2021, 161–162). The first aspect roughly aligns with the Arctic governance documents, while the second aspect becomes highlighted in the digitalisation programme for Lapland. According to Mark Duffield (2007, viii), “development is a technology of security that is central to liberal forms of power and government”. While appearing as benevolent, it hides attempts to manage and contain disorder, but not to suppress it completely (ibid.). The development of the digital Arctic thus strives to establish a contingent order that is manageable by the means available. It extends modern governmentality to cyberspace in the Arctic. Only some of the available means are technical, while others are more mundane, for instance, (scientific) knowledge production and dissemination, policies, legislation, administrative procedures, financing and investment, education and training (see Salminen, 2019).

The central goal of government has become to support and optimise the collective life of a nation, which is carried out by training and guiding but also disciplining

[9] The level of advancement of municipal digital services is expressed as a percentage in the study. The average level of advancement amongst small municipalities (less than 10 001 inhabitants) in mainland Finland is 59,99 per cent, while Savukoski’s percentage is 58,93. The average amongst mid-size municipalities (10 0001–100 000 inhabitants) is 64,85 per cent, while Kemi’s percentage is 63,39. (Ministry of Finance, 2020c, 20–23.)

[10] Valtioneuvoston asetus kuntien digitalisaation kannustinjärjestelmästä. My own translation.

individuals. In other words, by governing one and all. (Duffield, 2007, ix; Foucault, 2009b, 11, 19, 43, 122, 128–129.) Life existing outside these support networks is expected to be self-reliant (Duffield, 2007, ix), which generates a problematic duality in Lapland. Increasing connectedness and reliance on information infrastructure may actually decrease the self-reliance of individuals and communities and increase their dependency on nation-wide and global networks and centralised services as brought forth by article IV (Salminen, 2021, 170, 173). This dependency intensified by advancing digitalisation is also acknowledged in the latest national cybersecurity document of Finland, Cyber Security Development Programme, published in 2021 (Paananen, 2021, 18). In addition, 'resilience', which is pivotal in Arctic governance and cybersecurity, but also in the Finnish model of comprehensive security, and at the very heart of modern governmentality, may either increase or decrease as a result of digitalisation carried out the way it has been (see Salminen and Hossain, 2018, 111; Salminen, 2021, 170–171, 173; more widely Rautiainen, 2018, 26). I will return to this entanglement of security, development and resilience in sections 1.3.4, 3.1.5 and 3.3.1. Next, I will discuss both the prevailing and the gradually emerging framings of cyber/digital security effective in Finnish Lapland.

1.3 Multiple framings of cybersecurity

1.3.1 Mainstream framings: strategic and technical

Whereas digitalisation provides potential for certain desirable values, cybersecurity is to protect the realisation of these values (Limnéll et al., 2014, 15, 158). For that purpose, cyber threats need to be prevented, pre-empted, detected, counteracted, and mitigated, which anticipates a competitive setting that can culminate, at worst, in an open conflict. Ben Buchanan (2016) elaborates this dynamic with the concept of cybersecurity dilemma. Security dilemma is an old concept in International Relations (e.g. Buchanan, 2016, 15–29; Bourne, 2014, 93–108; Booth and Wheeler, 2007), but it receives new nuances when applied to cyberspace (see also Dunn Cavelty, 2014; cf. Foucault, 2009b, 296–297[11]). Due to the human speed of operations (not the speed of light as sometimes suggested, see also Limnéll et al.,

[11] For Dunn Cavelty (2014, 702) cybersecurity dilemma is awoken when an actor's "actions geared towards gaining more security are (directly and indirectly) to blame for making both the virtual [and] the real world less and not more secure". Foucault (2009b) does not use or define a concept of 'security dilemma' but speaks of the developments in governmentality brought forth in the 17th century in Europe in which the emerging conceptualisation of 'states' also positioned them in a competitive relationship vis-á-vis one another. Thus, "[i]f states exist alongside each other in a competitive relationship, a system must be found that will limit the mobility, ambition, growth, and reinforcement of all other states as much as possible, but nonetheless leaving each state enough openings for it to maximize its growth without provoking its adversaries and without, therefore, leading to its own disappearance or enfeeblement" (Foucault, 2009b, 296–297).

2014, 63–65), a lack of momentum, powerfulness of persistence and advantages of preparing in advance, states have an incentive to develop cyber capabilities before they seem necessary (Buchanan, 2016, 41). If another state discovers the state's capability-building efforts, it faces a dilemma of interpretation: It needs to decide whether to interpret this capability-building threatening or not (ibid., 49). Moreover, even when developing defensive capabilities, the state may resort to intrusions to the other state's networks, because it "can enhance network defense efforts, gather actionable information, and uncover future risks" (ibid., 72).

However, an intrusion into a strategically important network of another state is likely to be inherently threatening, that is, always interpreted as dangerous (Buchanan, 2016, 76). This interpretation, again, will guide the selection of counter-measures that are available to the other state to a varying degree. The response, nonetheless, can cause an escalation of the tense situation. (Ibid., 97–98.) The significance of cybersecurity in the Arctic is often derived from the increasing strategic value of the region, that is, it is becoming ever more important for entities like the state, the military, the economy and particular industries (e.g. Lehto et al., 2019). If the reading of these actors' strategic positions vis-á-vis one another highlights competition, the cybersecurity dilemma tends to become the main framework for interpreting the situation.

Similar, conflictual discourse dominates technical framings of cybersecurity. The discussion is often, but not solely, about 'attacks', 'defence', 'reconnaissance', 'operations', 'weapons', 'intelligence', 'countermeasures', 'targets', 'kill chains', 'enemy', and so forth. For example, in reference to information systems security, Workman et al. (2013, 280–284) first distinguish between active attacks (designed to damage or disrupt a system or a service) and passive attacks (designed to intercept information without notice) and then provide "broad attack classifications" such as information system attacks, social engineering attacks, and mobile device attacks. With regard to network security, they further explain that "[p]assive types attack are those designed to be stealthy, and include eavesdropping, whereas active attacks are more like open warfare" and "the passive form of attacks are most difficult to defend against, partly because their stealth makes them hard to detect" (ibid., 335). The discussion then moves on to sniffers[12], (distributed) denial of service attacks[13],

[12] Sniffers are of different kind, but a packet sniffer, for example, "is a tool that intercepts data flowing in a network". Techopedia (2016) Sniffer. https://www.techopedia.com/definition/4113/sniffer [March 29, 2021]. Techopedia is an online IT education website that provides, for example, a dictionary of technology terms with definitions, articles on technology trends, as well as tutorials and webinars. See Techopedia (n/d) About. https://www.techopedia.com/about [June 20, 2021].

[13] DDoS stands for distributed denial of service, that is, "a type of computer attack that uses a number of hosts to overwhelm a server, causing a website to experience a complete system crash". Techopedia (2020) Distributed Denial of Service. https://www.techopedia.com/definition/10261/distributed-denial-of-service-ddos [March 29, 2021].

redirection of traffic[14], source routing[15], IP session hijacking[16], and HTTP hijacking[17] before touching upon the "enemy's modus operandi" from reconnaissance and attack preparation to target exploitation (ibid., 336–342).

In a similar vein, Kiravuo and Särelä (2013, 231) discuss "the care and maintenance of cyberweapons", that is, "the capabilities needed to create and maintain a cyberweapons arsenal, the components that make up a cyberweapon, and the operative processes for using such weapons". The European Union Agency for Cybersecurity (ENISA)[18], again, utilises in its Threat Landscape 2020 report, especially in the descriptions of the top 15 threats, the kill chain framework of Lockheed Martin[19] "to map each step of the [attack] process and [to] reference the tools, techniques and procedures used by the attacker" (ENISA, 2020; Lockheed Martin, n/d). Conflictual and martial analogies are hence firmly embedded in both strategic and technical cybersecurity understandings (Betz and Stevens, 2013, 157).

1.3.2 Comprehensive cybersecurity to protect vital societal functions

However, cybersecurity is also about ensuring the continuity of vital societal functions[20] in all security situations. For this reason, for example, Finland's Cyber

[14] Redirection of traffic takes place in different ways and also for legitimate purposes, but, for example, "[a]ddress resolution protocol (ARP) spoofing is a technique that causes the redirection of network traffic to a hacker". Techopedia (2017) Address Resolution Protocol Spoofing. https://www.techopedia.com/definition/25409/address-resolution-protocol-spoofing-arpspoofing [March 29, 2021].

[15] Source routing "is a specific routing process where senders can specify the route that data packets take through a network. [...] Source routing is an alternative to traditional routing where packets just move through a network based on their destination." Techopedia (2019) Source Routing. https://www.techopedia.com/definition/9472/source-routing [March 29, 2021].

[16] Session hijacking "occurs when a session token is sent to a client browser from the Web server following the successful authentication of a client logon. A session hijacking attack works when it compromises the token by either confiscating or guessing what an authentic token session will be, thus acquiring unauthorized access to the Web server." Techopedia (2012) Session Hijacking. https://www.techopedia.com/definition/4101/session-hijacking [March 29, 2021].

[17] HTTP hijacking or "Internet Protocol hijacking (IP hijacking) is a specific form of hacking that makes use of IP addresses to move data over the Internet. [...] Hijacked IP addresses can be used for various kinds of targeted activities including spamming and denial of service attacks." Techopedia (n/d) Internet Protocol Hijacking. https://www.techopedia.com/definition/27966/internet-protocol-hijacking-ip-hijacking [March 29, 2021].

[18] ENISA is the EU's "agency dedicated to achieving a high common level of cybersecurity across Europe" established in 2004. It "contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure." ENISA (n/d) About ENISA. https://www.enisa.europa.eu/about-enisa [March 27, 2022].

[19] A US business concern specialising primarily on weaponry, aeronautics, and space technologies.

[20] Currently, seven vital functions to society have been defined in Finland: leadership; international and European Union activities; defence capability; internal security; economy, infrastructure and security

Security Strategies (Security Committee, 2013; 2019) emphasise cooperation between all actors in society – ranging from the central government to the authorities, regions and municipalities, business operators, organisations, research institutions, and to citizens – that follows the comprehensive security model set in the Government Resolution on Comprehensive Security[21] (2012) and in the Security Strategy for Society (Security Committee, 2017a). Furthermore, cooperative arrangements between the state and the business sector are based on the Government Resolution on Security of Supply[22] (1048/2018).

In brief, comprehensive security is "a cooperation model in which actors share and analyse security information, prepare joint plans, as well as train and work together" (Security Committee, 2017a, 5). "The Government directs, supervises and coordinates the safeguarding of functions vital to society. Each competent ministry does the same in its own administrative branch. [...] The Security Committee[23] assists the Government in comprehensive security preparedness and in its coordination. [...] Regional administration, municipalities and business communities and organisations manage preparedness planning in cooperation with other authorities, business operators and organisations." (Ibid., 11.)

Moreover, with regard to cybersecurity, the Cyber Security Director (this position is located in the Ministry of Transport and Communications and its first holder began his work at the beginning of April, 2020) ensures "the coordination of the development, planning and preparedness of cyber security in society" and "acts as an adviser to the central government in cyber security related matters" (Security Committee, 2019, 6). The National Cyber Security Centre (NSCS-FI) (operating as part of the Finnish Transport and Communications Agency also under the Ministry of Transport and Communications), which establishment was one of the actions laid out in the first national cybersecurity strategy (Security Committee, 2013, 5, 7), "develops and monitors the operational reliability and security of communications networks and services" and "provide[s] situational awareness of cyber security" (NCSC-FI, n/d). The role and authority of both the Cyber Security Director and NCSC-FI are still in flux (for a further elaboration on national cybersecurity arrangements in Finland, see e.g. Lehto et al., 2017; Lehto et al., 2018).

of supply; functional capacity of the population and services; and psychological resilience (Security Committee, 2017a, 14–24).

[21] Valtioneuvoston periaatepäätös kokonaisturvallisuudesta. My own translation.

[22] Valtioneuvoston päätös huoltovarmuuden tavoitteista.

[23] "The Security Committee assists the Government and ministries in broad matters pertaining to comprehensive security. The Committee follows the development of Finnish society and its security environment and coordinates proactive preparedness related to comprehensive security". It stipulates discussion and collects information "by arranging seminars and public discussions with various organisations, the business community and other cooperation partners", as well as "prepares statements and recommendations on matters related to comprehensive security". The Security Committee (n/d) Security Committee. https://turvallisuuskomitea.fi/en/security-committee/ [March 1, 2022].

According to Valtonen and Branders (2021, 96), the roots of the Finnish comprehensive security model date back to the first decade after the independence in 1917 and the civil war of 1918. The basis for national security structures was laid in the 1920's and '30s, while the experiences from the Second World War led to the unification of the country and the establishment of the concept of 'total defence', which has evolved into 'comprehensive security' over the decades. A strong national will to defend the country, which surveys verify also today (e.g. Findikaattori.fi, 2020), "has built both confidence in authorities and a willingness to work together". (Valtonen and Branders, 2021, 97–98.)

However, during the Second World War the unity of defence and cooperation between administrative branches had had to be coordinated ad hoc in many aspects due to lacking planning and preparedness. A number of civilian branches had been subjected to military leadership, which was no longer perceived as a functional model after the war. Instead, the civil administration's preparedness and capacity to function under stress had to be ensured otherwise. During the 1950's, the fields of total defence became established as 'political and administrative', 'economic', and 'psychological' defence, as well as 'protection of the population'. All these fields were supported by 'communications'. (Salminen, P., 2021, 145–147.) Total defence was a cooperation model purposed to prepare for war, but it also guided the strengthening of preparedness in civil society. After the Cold War, when global security transformed drastically, and "[a]s for other Nordic countries, discourses emerged to suggest that Finland needed to have a more comprehensive approach to security". (Valtonen and Branders, 2021, 99–100.)

Concept development and practical arrangements for critical infrastructure protection then began in the early 2000's and a strategy for securing the vital functions of society was accepted by the Government in 2003. "That was the first strategy providing common planning instructions involving threat scenarios for vital functions that needed to be secured in any circumstances, including general guidelines for managing a diverse array of security incidents" in cross-sectoral coordination and cooperation at all levels of society. (Valtonen and Branders, 2021, 100.) The 2010 update of the strategy outlined the key aspects of a 'comprehensive approach'. The model is "based on an all-hazards principle, which place[s] central responsibility to the competent authority, placing all other relevant security actors in supporting roles". (Ibid.) At the regional level, the Regional State Administrative Agency for Lapland (AVI) and the Centre for Economic Development, Transport and the Environment for Lapland (ELY), together with the Regional Council of Lapland, develop and coordinate preparedness and response[24]. In practice, the "lack

[24] On June 29, 2021, the President of the Republic signed five acts that will transform the provision of healthcare and social security as well as rescue services across Finland. In this reform, the Regional State Administrative Agencies and Centres for Economic Development will be abolished and the regional

of resources in many areas in Finland has created innovative solutions [for burden sharing like the] collaboration model between the Border Guard, Customs, and Police developed in rural Lapland" (ibid., 103; cf. Salminen, 2019; 2021). Cybersecurity was introduced as an aspect of comprehensive security in Finland's Cyber Security Strategy 2013, which is a sub-strategy supporting the implementation of the Security Strategy for Society[25].

In Finland, cybersecurity is defined in the 2013 national cybersecurity strategy as "the desired end state in which the cyber domain is reliable and in which its functioning is ensured" (Security Committee, 2013, 1). Definition in the 2019 strategy follows the definition given in the Vocabulary of Cyber Security published in 2018[26]: "Cyber security is understood as a space in which the cyber environment can be trusted and its functioning is secured" (Security Committee, 2019, 4, footnote 1). The objective hence is the same, secured and functioning cyberspace, even if the wording has slightly changed. The principles of cybersecurity production follow those of the comprehensive security model as stated above.

However, even if "each actor or sector in society has distinct cyber security tasks" (Security Committee, 2013, 36), the 2013 national cybersecurity strategy utters little about the role of individuals. Individuals are perceived as potential victims or injured parties or targets (ibid., 1, 13, 18, 27), plaintiffs (ibid., 27), effective utilisers of cyberspace (ibid., 3), receivers of training and instructions (ibid., 9), vulnerability (ibid., 18), employees (ibid., 31), right holders (ibid., 13, 33–34), information sources (ibid., 13), persons whose digital competence needs to be improved (ibid., 31), protectees (ibid., 34), and establishers of ICT and network security solutions (ibid., 5) (cf. Dunn Cavelty, 2014, 703–704). The improvement of

administration will be organised into 21 wellbeing services counties in addition to which the city of Helsinki will organise wellbeing services to its residents. See Laki sosiaali- ja terveydenhuollon järjestämisestä [Act on Organising Healthcare and Social Welfare Services] (612/2021), Laki hyvinvointialueesta [Act on a Wellbeing Services County] (611/2021), Laki pelastustoimen järjestämisestä [Act on the Organisation of Rescue Services] (613/2021), Hyvinvointialue- ja maakuntajakolaki [Act on the Division of Wellbeing Services Counties and Counties] (614/2021), and Laki sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisestä Uudellamaalla [Act on the Organisation of Healthcare and Social Security Services as well as of Rescue Services in the County of Uusimaa] (615/2021). My own translations. Some of these laws took effect already in the beginning on July, 2021. The first county elections were conducted in January 2022 "to elect a county council for each wellbeing services county. [...] [T]he highest decision-making power in each county will be exercised by a county council." Ministry of Justice (n/d) County elections. https://vaalit.fi/en/county-elections [March 20, 2022].

[25] The national cybersecurity management model crafted after this introduction is well depicted in Lehto et al. (2018, 11–25).

[26] Vocabulary of Cyber Security (2018) was compiled as there was a need for uniformly defined concepts in cybersecurity. This was a collaborative effort between the Security Committee, the National Emergency Supply Association, and the Finnish Terminology Centre envisioned in the second implementation programme of Finland's Cyber Security Strategy 2013. The vocabulary is available through https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ [July 29, 2021].

cyber competencies through schooling, education, training, exercises, and research receives most of the attention given to individuals, which is in line with modern governmentality: The aim is to help people help themselves thus responsibilising them for cybersecurity (e.g. Renaud et at., 2018; Zimmermann and Renaud, 2019; Päläs and Salminen, 2019; Salminen and Päläs, 2021). The claimed rapprochement of states, businesses, and citizens in cyberspace fosters wellbeing, but also introduces novel risks, for which reason the strategy is to be seen as a constantly evolving, living document (Security Committee, 2013, 17, 39).

The 2019 national cybersecurity strategy has "development of cyber security competence" as its third pillar[27]. Today, "[e]ach individual is [...] an important cyber security actor who can improve cyber security through his or her actions on a daily basis and thus impact his or her own cyber security and that of others. At the national level, it must be ensured that everyone has sufficient capacity to operate safely in a digital environment" (Security Committee, 2019, 8). The individual has hence been subjectivated as a cybersecurity actor and responsibilisation of him or her for national cybersecurity could hardly be stated more clearly. In addition, it must be ensured that top talents will stay in Finland to contribute to the common effort (ibid.).

The implementation of national cybersecurity strategies has been guided by two implementation programmes (2014 and 2017) developed for the 2013 strategy and the Cyber Security Development Programme (2021) supplementing the 2019 strategy. The 2014 implementation programme recognised six pivotal areas of development and consisted of 74 measures altogether. These six pivotal areas included: establishment of National Cyber Security Centre (NCSC-FI), integration of services provided by the Government security network and encrypted information transfer, improvement of the Police capacities to counter cybercrime, development of Government's 24/7 information security activities, development of legislation related to cybersecurity and cyber operational environment, programmes for research and development, as well as strengthening of skills otherwise. (Security Committee, 2014, 2.) It focused heavily on the activities of authorities, even if it recognised that majority of production and services were on the private sector. "Safe and secure cyber operational environment [was] to be developed in a manner that strengthen[ed] the opportunities residing in information society for citizens, companies, and authorities and advance[d] the realisation of basic rights. Yet, every actor, from individuals to companies and public administration still [had] responsibility for their own preparedness against cyber threats." (Ibid., 3, my own translation.) The development of citizens' digital competence was listed as one of the means to support national preparedness, but at the time this meant primarily

[27] The other two pillars are "development of international cooperation" and "better coordination of cyber security management, planning and preparedness".

the strengthening of research and teaching in universities and universities of applied sciences, teaching of media literacy at schools, as well as training and communications through projects and campaigns (ibid., 14–15, 21, 46–49).

The 2017 implementation programme explained how it approached the development of national cybersecurity as a service entity comprising the state, counties, municipalities, businesses, and the third sector in which the individual citizen was a customer (Security Committee, 2017b, 4). Cybersecurity was to be built into activities and services, which meant safe and easy-to-use digital services and operational capability also under stress so that trust towards digitality could be sustained and strengthened (ibid., 5). The programme divided into three entities and consisted of 22 measures altogether. These three entities composed of achieving the vision of the cybersecurity strategy by defining and organising a national cybersecurity management model, safeguarding the society's digitalised vital functions, and facilitating digitalisation by improving the cyber competence of citizens, business and administration. (Ibid., 8–10.) The latter consisted of two measures. First of them focused on generating a safe environment for digital business, including the strengthening of privacy and other basic rights and the authorities' obligation to help citizens and communities to improve their information security. The second concentrated on planning and implementing digital skills education and training, for example, in teachers' training and through peer support, voluntary defence training and preparedness exercises. (Ibid., 20–22.)

The primary aim of the most recent programme, the national Cyber Security Development Programme (2021), "is to create a cybersecurity ecosystem in Finland that will provide vitality and growth, create jobs in the sector, increase necessary expertise and improve both the sustainability of digital society and its resilience to varying phenomena in cybersecurity environment" (Paananen, 2021, 5, my own translation). Such an ecosystem implicates an overarching economic order that above all seeks to sell security while also providing it in exchange for the generalised obligation to improve digital literacy. "High-level, national cyber security calls for [...] extensive participation across all levels of society" (ibid., 5, 11, my own translation), for which reason "[c]yber security ought to be seen as a natural part of the societal responsibility of each organisation and individual" (ibid., 8, my own translation). The aim is to secure the opportunities that digitalisation provides while diminishing cyber security risks (ibid., 10).

Top class expertise is one of the main themes in the development of national cybersecurity ecosystem (Paananen, 2021, 10). It entails that the providers of digital solutions and services "must be able to provide safe and secure services", as well as that the citizens "must have the skills to use the services provided by digital information society in a safe manner and to recognise the risks related to the use of equipment, products, and services" (ibid., 11, my own translation). While Salminen and Hossain (2018, 114) notes that digital services have moved from being a supplementary form of service provision to being its primary form, this cybersecurity development programme signals even more strongly that the citizens and residents have to acquire necessary digital competence. Without good enough digital literacy and skills one will be perceived as dangerous surplus or self-sufficient individual residing outside the curtailed safety net provided to the right kind of citizens.

In the programme, the role of the third sector and civic organisations in improving the digital literacy of the citizenry becomes emphasised. The task of the state is to enable and to support, for example, by institutionalising the role of these organisations and voluntary cybersecurity communities (Paananen, 2021, 11–12, 14). In addition, cybersecurity is to be integrated in basic and vocational education and strategic partnerships are to be encouraged between the state, businesses and higher education institutions (ibid., 13–14). It thus seems that the future government of cyberspace will closely follow the networked rationality of modern government as described in this synthesis. It will continue to modify the field of opportunities for all societal actors. Intensifying governmental activities in cyber/digital security bring up the question of (human) freedom.

According to Dillon and Logo-Guerrero (2008, 291), "[t]here could be no more central question for politics […] than that of the relation of freedom and security. […] [Security practices] do not simply insist on rendering life transparent to certain forms of knowing; such life which is in whatever way resistant to being known begins to pose a security problem[.] […] [The] purpose [of security practices] is in addition […] to weigh life […] in order to determine which life is capable of self-regulating itself in the cause of its self-improvement, adaptation and change[.] […] [S]ome forms of life may be less capable or incapable, and even hostile or resistant, to self-regulating themselves in the cause of their self-improvement and adaptation. All life in some degree or another may have to be coached in […] self-governance and some life may have to be subject to more than coaching." (Ibid.) In one particular area "this challenge of making sense of novel spaces and processes is especially pressing[:][…] the entanglement of the digital, the informational and the governmental" (Walters, 2012, 53). I will return to the question of freedom in digitality in sections 1.3.4, 3.3.2, 3.3.3, and 4.1.

1.3.3 Digital security in Finland

In 2020, Finland published yet another societal security concept related to digitalisation and following the comprehensive security model: digital security. This concept focuses on the security of digitalised public sector services. It aims "to protect citizens, communities and society in the digital environment from risks and threats that may affect personal data and citizens' services, as well as society's and authorities' processes, services and data" (Ministry of Finance, 2020b, 11). Thus, it widens the responsibility of the public sector for sustaining digital services beyond functions vital to society. Citizens have also been moved to the beginning of the list of ‘things’ to be secured after having spent years firmly at its very end. In practice, digital security encompasses the techniques of risk management, continuity management, information security, data privacy, and cybersecurity (ibid., 16).

In this thesis the main object of interrogation is digital security – as defined by the Ministry of Finance of Finland and from a human security perspective. The reason for this confinement is the aforementioned limited attention given to the role of individuals in the mainstream frameworks of cybersecurity, whereas the digital security frameworks take individuals as their referent object and are vocal about their government. In digital security, citizens are allocated the role of ‘active security actors’, although it is also noted that this role has been poorly recognised and undefined (Ministry of Finance, 2020b, 12, 20). Development of digital literacy within the entire society is brought forth as a strategic focal point. ‘Citizenry, personnel and know-how’ are one of the stated areas of development that is carried out through improving people’s skills, exercises, and facilitating the availability of expert services. (Ibid., 12–15.) Public service provision is ought to become ‘human-centred’ and based on individuals’ life events (ibid., 19). These moves are significant value choices in comparison to cybersecurity.

Furthermore, it is acknowledged that there are too few digital security experts in Finland and that acquiring, developing, and sustaining know-how are national challenges (Ministry of Finance, 2020b, 20). Within the public administration, skills development takes place varyingly and repeated information security breaches[28] testify that the minimum requirements for digital security are not in

[28] The most high-profile publicised information breaches in the Finnish public administration include digital espionage in the network of the Ministry of Foreign Affairs in 2013 and in the network of the Parliament in 2020. Both cases have been recognised as advanced persistent threats (APT), that is, “a cyberattack launched by an attacker with substantial means, organization and motivation to carry out a sustained assault against a target. An APT is advanced in the sense that it employs stealth and multiple attack methods to compromise the target [...][;] persistent because the attacker can spend months gathering intelligence about the target and use that intelligence to launch multiple attacks over an extended period of time[; and] threatening because perpetrators are often after highly sensitive information”. (Techopedia (2017) Advanced Persistent Threat. https://www.techopedia.com/definition/28118/advanced-persistent-threat-apt [June 20, 2021].) The former attack has not been officially attributed, but speculations about the intruder have named Russia, China, and the United States. The latter attack has been attributed to China. See, for example, Leppänen, Mikko (2013) ”MTV3: Suomen ulkoministeriö laajan verkkovakoilun kohteena vuosia” [MTV3: Ministry of Foreign Affairs of Finland targeted by a wide network espionage campaign for years], YLE News, October 31, 2013, https://yle.fi/uutiset/3-6911225; Halminen, Laura, Junkkari, Marko, Juntunen, Esa, Lehtinen, Toni, Pugin, Leo and Vanninen, Anna (2013) ”Ulkoministeriön verkko oli täysin ulkopuolisten hallussa” [The network of the Ministry of Foreign Affairs completely under external control], Helsingin Sanomat, November 1, 2013, https://www.hs.fi/kotimaa/art-2000002685298.html; Pietiläinen, Tuomo and Tarvonen, Hanne-Mari (2014) ”Supo: Ulkoministeriötä vakoili kaksi eri valtiota – ’materiaalia on viety runsaasti’” [Supo: Two different states were spying on the Ministry of Foreign Affairs – ’plenty of material has been extracted’], Helsingin Sanomat, July 2, 2014, https://www.hs.fi/kotimaa/art-2000002742996.html; Tolkki, Kristiina, Rimpiläinen, Tuomas and Konttinen, Matti (2020) ”KRP tutkii äärimmäisen harvinaista rikosta:

place everywhere. Difficulties in identification services and problems in identity management also erode citizens' trust. Therefore, "[t]he public sector must not pass its risks on for service users to manage, and security requirements must not prevent the intention of service users to be realised". (Ibid., 21–23; cf. Salminen, 2021, 170–172, 174–175.) "Citizens, enterprises and various other entities must be able to connect securely to the ordinary digital services provided by the public sector. The various parties must also be able to have trust and confidence in the functioning of services and ultimately in assistance being provided by the authorities in case of incidents." (Ministry of Finance, 2020b, 24.)

Moreover, "[c]itizens must have access to a secure digital environment where security equals their experience of the safety and security of the physical operating environment. Among other things, this means attacks being guarded against already in the information network, malware[29] being filtered, and denial of service attacks being prevented." (Ministry of Finance, 2020b, 25.) Thus, a more active security role is envisioned to the state with regard to citizens' safety than in the previous strategies and programmes. All in all, the society should clearly define the problem of digital security and responsibilities in its production (ibid., 24; also, Lehto et al., 2018). Finland's cybersecurity strategies and the concept of digital security can be perceived as an evolving continuum, in which the problematisations refine and security comes to occupy more room in the digitalising society.

The concept of digital security as defined by the Ministry of Finance clarifies Finland's Cyber Security Strategy 2019. Its development follows six principles: co-management of the security of digitalised society on the basis of situational awareness and risk evaluation; planning and monitoring of the effectiveness and cost of digital security in public administration; development of citizens' and employees' understanding of the impacts of security risks and responsibilities; advancement of digital security in cooperation between public administration, communities and citizens; influencing international and EU-level digital security and utilisation of the results of this cooperation; postulation of security in technologies and service production. (Ministry of Finance, 2020b, 9.) The addition of the concept of digital

Eduskuntaan kohdistunut tietomurto voi olla vakoilua ja kansanedustajien sähköposteja vaarantunut" [National Bureau of Investigation is investigating an extremely rare crime: Information breach in the Parliament may be espionage and emails of MPs may have been compromised], YLE News, December 28, 2020, https://yle.fi/uutiset/3-11715912; STT and Osipova, Elsa (2021) "Supo: Eduskuntaan kohdistunut vakoilu viittaa Kiinaan – poliisin mukaan verkkovakoilulla on yritetty kalastella tietoja vieraalle valtiolle" [Supo: Espionage targeting the Parliament points towards China – according to the Police network espionage has been used to fish information for a foreign state], YLE News, March 18, 2021, https://yle.fi/uutiset/3-11843261. My own translations.

[29] Malware, that is, malicious software "is any software that brings harm to a computer system. [It] can be in the form of worms, viruses, trojans, spyware, adware and rootkits, [etcetera], which steal protected data, delete documents or add software not approved by a user". Techopedia (2013) Malicious Software. https://www.techopedia.com/definition/4015/malicious-software-malware [June 20, 2021].

security to the palette of digitalisation related security concepts in Finland has not made the differentiation between them – information security, cybersecurity, digital security, and all additional technical conceptualisations – easy. Limits between the conceptualisations are also blurry for which reason, for example, "digital security and cybersecurity as security of the digital operational environment often mean the same thing" (ibid.). A good example of such overlap is the Digital Security 2030 programme of the National Emergency Supply Agency (NESA) (2021b) which despite its title addresses cybersecurity. I will return to NESA and its programmes in section 3.1.2.

Yet, the ownership of the two concepts is located in different ministries and agencies – Ministry of Transport and Communications and National Cyber Security Centre (NCSC-FI) for cybersecurity and Ministry of Finance and Digital and Population Data Services Agency (DVV) for digital security. This is a traditional duality in public information security responsibilities in Finland (see Security Committee, 2013, 20), which logic is not self-evident, but will likely become clarified in the future. The consequence of the current overlap of cybersecurity and digital security conceptualisations for this thesis is that I use the formulation cyber/digital security throughout the synthesis to refer to the dispositive under scrutiny.

In addition to cooperation internal to society, supranational and international cybersecurity cooperation takes place within the frameworks of, for example, UN, OECD, the Organization for Security and Co-operation in Europe (OSCE), the Council of Europe, EU, NATO, Europol and Interpol, between the Nordic countries (see e.g. Koivunen, 2013), as well as through bilateral arrangements (see Security Committee 2013; 2019). Framing of the issue differs in these frameworks. The ways in which a phenomenon is framed matter because they define "the problem involved in a particular way and [tell] us who should do what to tackle the problem so framed" (Finnemore and Hollis, 2016, 447). "[D]ifferent problematisations of security [comprise] different discourses of danger" revolving around different referent objects of security and "giv[ing] rise to different kinds of governmental technologies and political rationalities" (Dillon and Logo-Guerrero, 2008, 274). Problematisation of an issue is hence both a process in which the issue is defined as a problem to act upon and the examination of this process itself (see Foucault, 1998, 82; Koopman, 2013, 48). It thus matters that, for instance, cybersecurity is a subject of conversations in NATO, digital security in OECD, human-centric cybersecurity in UN, and data protection and privacy in EU. It also matters from which theoretical perspective the topic is addressed, as a human security approach to cybersecurity produces a different understanding from a realist approach to the topic.

In this thesis, I will not address the international cooperative arrangements even if, for example, both EU and NATO are active actors in the Arctic. Instead, I will concentrate on how individual security is produced as part of cyber/digital security in Lapland. The lack of regionally focused security arrangements, or even discussion about the topic, highlights how the states and ICT corporations are perceived as the main security players in the mainstream framings of the digital Arctic (also Security Committee, 2013, 6).

1.3.4 A human security approach to digitalisation and cybersecurity

Even if frames tend to sustain themselves well over time and they can be difficult to dislodge, reframings and novel framings do take place (Finnemore and Hollis, 2016, 447). As an attempted reframing, the ECoHuCy project, part of which the four articles of this thesis were authored, introduced an alternative, or more precisely a complementing, view to cybersecurity in the Arctic. It aimed at producing a new discourse around digitality (see Foucault, 1998, 30, 36, 44). Instead of focusing on technical security and/or the national security implications of the digitalisation of society, it examined the everyday digital security of individuals and communities living in the European High North. Human security served as the project's theoretical framework and its aims were threefold: (1) to redefine cybersecurity from a human security perspective, (2) to depict both enabling and threatening potentials residing in the regional digital development from the perspective of the everyday life of local people, and (3) to substitute the human being for information, information infrastructure and/or vital societal functions as the referent object of cybersecurity.

This approach required contextualisation of digitalisation and cybersecurity to the European High North and discussions with the local people, as well as rethinking of what digital security in the Arctic entails. The pool of stakeholders participating in the definition of both positive and negative aspects of digitalisation, desired ends for the development, the related security concerns and means for security production, as well as the roles of different stakeholders, was extended from security and ICT experts, administrators and politicians to general population as depicted in article IV. The locals were thus included in the processes in which digital security becomes defined and framed (see e.g. Gulbrandsen and Sheehan, 2020; Olsén-Ljetoff and Hokkanen, 2020; Salminen, 2021). Shortly, the objective of the ECoHuCy project was to problematise the mainstream understandings of cybersecurity and turn them into a more inclusive dispositive that would also incorporate people's everyday concerns related to the digital transformation of society (see Koopman, 2013, 18).

Human security becomes extensively discussed in the four articles that constitute the empirical part of this thesis. In brief, a human security framing of digitalisation and cybersecurity focuses on human wellbeing (measured by, for example, the Human Development Index (HDI)[30]) and emphasises three freedoms for both individuals

[30] "The Human Development Index (HDI) is a summary measure of average achievement in key dimensions of human development: a long and healthy life, being knowledgeable and have a decent standard of living". United Nations Development Programme (UNDP) (n/d) Human Development Index. http://hdr.undp.org/en/content/human-development-index-hdi [June 21, 2021]. For further information, see HDI's Technical notes http://hdr.undp.org/sites/default/files/hdr2020_technical_

and communities: freedom from fear, want, and indignity. These freedoms entail "protection of individuals from risks to their physical or psychological safety", wellbeing, and dignity, which "affords individuals the possibility to lead stable, self-determined lives" (Tadjbakhsh and Chenoy, 2009, 3). Thus, human security combines the notions of safety and security and extends them from mere survival to life worth living (ibid., 9). It is about identification of thresholds, below which welfare, dignity, and survival should not fall (ibid., 17).

According to Shahrbanou Tadjbakhsh (2014, 2), security is freedom from danger and/or a threat, which definition "depends invariably on the context". Threats to survival can be, for example, about "physical abuse, violence, persecution or death"; threats to livelihoods about "unemployment, food insecurity, [and] health threats"; and threats to dignity entail "lack of human rights, inequality, exclusion, [and] discrimination". (Ibid.) In article II, these threats have been applied to digitality consisting of fears "related to the unfamiliarity of [ICT], inexperience in their use, doubt in one's own skills[,] and concerns of being excluded due to lacking knowledge and skills" (Salminen, 2019, 330). "Freedom from want entails that people do not fall victim to cybercrime […] and that they are able to provide themselves, for example, by applying for jobs online […] [or] claiming social security online". Freedom from indignity then adds in not to be named and shamed online without evidence, treated as inferior, or harassed, and to have equal access to services. (Ibid., 330–331.)

Human security aims to ensure that "all individuals [can] enlarge their human capabilities to the fullest and to put those capabilities to the best use in all fields" in a free and safe manner (UNDP, 1994, 13, 23). In other words, it aims to secure individuals' and communities' free choice "and that they can be relatively confident that the opportunities they have today are not totally lost tomorrow" (ibid., 23), also in and with regard to cyberspace. Human security is hence to support human development understood as "a process of widening the range of people's choices" (ibid.). As a consequence, "[t]he idea of human security has prompted the development and security communities to intersect" (King and Murray, 2001, 589) and claims have been presented for an international cooperation framework integrating security, human rights, and development (e.g. Churruca Muguruza, 2017, 15).

notes.pdf [June 21, 2021]. For a critical evaluation of the use of benchmarking as a technique of human security, see Homolar (2015). Human security approaches have often abstained from defining wellbeing, but, for example, King and Murray (2001, 593, italics removed) wish "to include only those domains of well-being that have been important enough for human beings to fight over or to put their lives or property at great risk". They also note that "different formulations of the concept include those that can be categorizes as subjective mental states […], or the degree of objective satisfaction of subjective desires and objective states" (ibid., 592–593). Wellbeing, like security and freedom, thus entail both subjective and objective evaluations of the situation in which one finds him- or herself.

Human security incorporates positive (freedom to something) and negative (freedom from something) security[31] and strives for human empowerment (Hoogensen Gjørv 2012, 836; Homolar, 2015, 844) – understood as everyone's increased ability to influence the developments taking place in his or her living environment. With regard to digitalisation, the aforesaid entails not only that individuals and communities are free to choose between, for instance, preset digital platforms for running errands or creating digital communality, but also that they can participate in defining the alternatives that digital development brings forth in their lives. No threat or obstacle ought to restrict their ability to participate in the digitalising society to the extent they wish to. In addition, human security takes into consideration chronic threats such as continuous undermining of privacy on digital platforms, as well as "sudden and hurtful disruptions in the patterns of daily lives" (UNDP, 1994, 23) such as unexpected disclosures of sensitive personal information or ransomware locking one's phone or laptop. It also aims to address structural violence[32], that is, indirect violence that lacks a subject that acts (Galtung, 1969, 170–171) but has been coded into the digital architecture (see Lessig, 1999).

Furthermore, human security integrates both objective and subjective security as well as objective and subjective freedom. The former have been defined by Arnold Wolfers (1952, 485) in the context of national security as "the absence of threats to acquired values" (objective security) and as "the absence of fear that such values will be attacked" (subjective security). Subjective security hence is to an extent an emotion. Similarly, objective freedom, according to Tuckness and Wolf (2017, 36–37), depends on the situation in which the person is in, whereas subjective freedom prevails if the person believes him- or herself to be free. Yet, a person who believes him- or herself to be free may in objective evaluation be seen to error (ibid., 36). The entanglement of security and freedom becomes discussed again in sections 3.3.2, 3.3.3 and 4.1.

Importantly, "[e]nsuring human security does not mean taking away from people the responsibility and opportunity for mastering their lives" (UNDP, 1994, 24). Instead, "people should be able to take care of themselves", which will set them free and enable them to make a full contribution to "their own development and that of their communities, their countries and the world" (ibid.). Alongside being the referent object of security, individuals and communities thus actively participate

[31] 'Freedom from something' and 'freedom to something' come close to what Tuckness and Wolf (2017, 41) have introduced as Isaiah Berlin's conceptualisations of negative liberty, that is, "freedom from others' interference" and of positive liberty, that is, "the freedom to act on a wide range of available choices".

[32] Galtung (1969, 168, italics removed) conceptualises violence "as the cause of the difference between the potential and the actual, between what could have been and what is". Furthermore, "when the potential is higher than the actual is by definition avoidable and when it is avoidable, then violence is present" (ibid., 169, italics removed). As violence hence prevents or hinders individuals from reaching their full potential, it is what human security strives to eradicate.

in the definition of security, security threats and suitable means for encountering them (see e.g. Salminen et al., 2020b, 30–32, 46; Salminen, 2019; Salminen, 2021). The gaze also moves from ostentatious events to mundane practices and spaces (McCluskey, 2019, 20). It is hence "essential to understand the moments in which individuals in their practices feel that they are (in)secure because of the relations and processes in which they have immersed" (ibid., 14; cf. King and Murray, 2001, 595). Threats thus defined may or may not be existential in their character, but cross a context-bound threshold and become accepted as security concerns by the audience to whom they have been addressed (Martin and Owen, 2010, 221; Salminen and Hossain, 2018, 112). Security then becomes produced in two-way processes running from top-down and bottom-up (Anttila, 2012, 31; Salminen et al., 2020b, 33, 35, 46).

Finally, human security extends security from the traditional national security sector to multiple other sectors such as health, environment, and economy (see e.g. UNDP, 1994; King and Murray, 2001, 588–589; cf. Buzan et al., 1998). As all societal sectors are currently becoming digitalised, and hence dependent on the smooth functioning of information infrastructure and ICT, cybersecurity is a human security question to the core. Next to that, human security questions located in cyberspace such as the realisation of the freedom of speech and the right to privacy online, but also the increasing concerns over hate speech, cyber harassment, mis- and disinformation, and cybercrimes of all sorts witness about the topicality of a human security approach to cybersecurity (e.g. Salminen and Hossain, 2018; Salminen et al., 2020b). Cybersecurity is a human security and a human rights question hence at two levels[33]: First, there is the question of 'digital rights', that is, the realisation of human rights online. Second, the realisation of human rights contemporarily depends on the functioning of (information) infrastructure in all conditions. (E.g. Salminen and Hossain, 2018, 112; Salminen et al., 2020b, 39–46; more generally about the relationship between human security, human rights and human development, see e.g. Churruca Muguruza, 2017.)

To conclude: As Myriam Dunn Cavelty (2014, 703) has noted, cybersecurity is "a heterogeneous set of discourses and practices with multiple, often contradictory effects". Cyberspace is "used by many different actors for a variety of things", for which reason security actions "come to bear on human lives in multiple ways" (ibid.; see also Foucault, 1998, 18, 26–27, 30, 33). Wolfers noted already in the 1950's that "the term 'security' covers a range of goals so wide that highly divergent policies can be interpreted as policies of security" (Wolfers, 1952, 484). As a consequence, after

[33] A potential third level is the claim that cybersecurity itself is a human right. For example, Scott J. Shackelford (2019) has argued that cybersecurity should be recognised as an emerging human right similarly to internet access. The same argument was presented by Luca Tosoni at XXXVI Nordic Conference on Law and Information Technology on November 9, 2021 in Oslo.

Colin Gordon (1991, 36), "[d]ifferent ways of posing and answering these questions compete and coexist with one another". What is important is the assemblage they constitute as a technology of government in people's everyday life.

The strands of cybersecurity research are manifold and trying to address them all in one thesis is not purposeful. Research, inter alia, on cybercrime and cyberterrorism, digital abuse, information influence, data gathering and surveillance, cyber and hybrid operations, as well as online activism or activism supported by digital means, in some aspects come close to or address individuals' and communities' everyday life – also in Lapland (see Salminen, 2018a; Päläs and Salminen, 2019; Salminen, 2021). However, my enquiry follows the approach of the ECoHuCy project, in which the juxtaposition of the overall, national cybersecurity framing with a human security framing generated novel problematisation concerning the placement, role, rights, and responsibilities of individuals in everyday digital security. Human security is, of course, not the solely international security approach focusing on the individual (see e.g. Bubandt, 2005; Booth, 2007; McCluskey, 2019; Jarvis, 2019) and due to its acknowledged theoretical ambiguity, I chose to support the framework in this synthesis with Foucault's and Foucault inspired observations about the dispositive of security.

1.4 Government of digitalising everyday life

1.4.1 Security dispositive

Building on the thinking of Michel Foucault, I examine in this synthesis the dispositive[34] of security in the context of digitalisation in the Arctic. As "[t]he

[34] There are a number of readings of dispositive concerning its comprehensiveness and whether it should be understood in singular or in plural. In this thesis, I rely primarily on Foucault's remarks about dispositive in his lectures 1977–1979 (2009b and 2010), in *The Will to Knowledge: The History of Sexuality: 1* (1998), and in commentary literature that discusses dispositives in plural (e.g Bussolini, 2010; Raffnsøe, 2008; Raffnsøe et al., 2016; Dean and Villadsen, 2016; Callewaert, 2017; Villadsen, 2021). According to Callewaert (2017, 37), Foucault approaches dispositive differently on the final pages of *Discipline and Punish: The Birth of the Prison* (1991) than in his aforementioned governmentality lectures. In the former, dispositive entails a "model of socialization invented by and for the prison [...] which [...] has pervaded the whole society", whereas in the latter, it refers to "the exercise of power by governmentality" (ibid.; also, Villadsen, 2021, 476–477). However, even in the former reading Foucault implies that the model developed in and for the prison "will by a number of dispositifs be transferred to the whole society"; *not in its compact form* that exists in the prison, *but so that only some of its mechanisms will spread to the society* hence normalising, for example, punishment (Callewaert, 2017, 38; also, Helén, 2016, 33, who emphasises Foucault's interest in studying how these mechanisms function and generate different effects). (Cf. the spread of the mechanisms of pastoral power over its religious boundaries and their consequent transformation in Foucault, 2009b; Walters, 2012, 22–25.) Raffnsøe et al. (2016, 276, 284) associate "the common penchant for pinning down certain consecutive historical epochs that Foucault seems to discern from each other [...][,] separated by radical shifts that seem to turn everything upside down", as "all-embracing, unequivocal contexts that follow and replace each other, thus re-presenting society

exact meaning of the term 'dispositive' and its significance in Foucault's thinking remai[n] debated in the commentary literature" (Villadsen, 2021, 474), I try to utilise Foucault's own accounts as much as convenient in elaborating the concept. I understand dispositive[35, 36] as a compilation of discursive and material[37] practices in their mutual, changing relations. In other words, dispositive is a compilation of techniques[38] that constitute a recognisable entity and can be used in governing a

in general at a certain historical point" with Deleuze's influence in interpreting Foucault. For example, the era of sovereignty and law would then be replaced by an era of discipline. (See e.g. Deleuze, 1999, 23, 30.) In their reading of *Security, Territory, Population* (2009b), Raffnsøe el al. (2016, 275) highlight three "particularly significant dispositional prototypes", namely, the legal dispositive, the disciplinary dispositive, and the dispositives of security. They "all express distinct dispositional logics" but are "able to share common material" (ibid., 780). Raffnsøe (2008, 55–56) elaborates these three dispositives in greater detail (also, Villadsen, 2021, 477–478; cf. Whelan [2019, 48–50], who discusses legal dispositive, ethical dispositive, and utilitarian dispositive). Yet, dispositives do not historically follow one another, but co-exist embedding in and influencing each other (e.g. Bussolini, 2010, 90; Walters, 2012, 32; Raffnsøe et al., 2016, 282). Finally, Villadsen (2021, 474) traces the reading of dispositive as "an apparently expansive and controlling regime of power" producing "submission and compliance to the demands of governance" to an early study of dispositive published by Jackson and Carter (1998), which has more recently been contested. "The immediate similarity between prisons, schools, hospitals and factories cannot be ascribed to an underlying (disciplinary) 'regime' [...] or an 'ideological structure' which gives shape to organizations", because (1) "the interplay of several dispositives means that one cannot rule univocally in organizational practices" and (2) "a dispositive is not a self-coherent system, since it produces unintended effects that put it in contradiction with itself" (ibid., 278).

[35] The French term 'dispositif' has been translated varyingly into English, most commonly as 'apparatus' or 'deployment'. However, the use of 'dispositive' has become more common in English research literature recently. One of the reasons for this shift in terminology has been, for example, the work of Jeffrey Bussolini (2010), who highlights the nuances in terminology that ought to be carried with into translations (see also Raffnsøe, 2008, 44; Callewaert, 2017, 29, 45). When having utilised English translations that feature the term 'apparatus' without associating it to 'dispositif', I have checked from the French texts which concepts they contain. Finally, of the Finnish books I have utilised Alhanen (2007) also translates 'dispositif' to 'dispositiivi'. 'Apparatus', again, is in this thesis understood as a subset of dispositive (Bussolini, 2010, 93–94; see Foucault, 2009b, 99; Dean and Villadsen, 2016, 106–107).

[36] According to Raffnsøe et al. (2016, 277), 'dispositif' in everyday French implicates "an arrangement set up for a specific purpose" with an immediate effect. "Etymologically, [...] the notion derives from the Late Latin *dispositivus*, a substantive form of the adjective under the same name" and emanating from a verb implicating "'to set in order', 'to arrange or array', 'to dispose', or 'to form'" (ibid., italics original). (Cf. Whelan, 2019, 47.)

[37] While Foucault often used the formulations 'discursive' and 'non-discursive', I have chosen to use the pair 'discursive' and 'material' in this thesis to depict both ideational and material aspects of practices. The reason is that 'non-discursive' becomes easily understood as the unsaid (e.g. Peltonen, 2008, 75), albeit silence is an important factor in discourse for Foucault (e.g. Deleuze, 1999, 4; see Foucault, 2009a). In addition, 'material' concretises and anchors practices nicely in everyday life which is the context in which digitalisation and its securitisation are investigated in this thesis. Raffnsøe et al. (2016, 278) also juxtapose 'non-discursive' and that "of a more material kind". Foucault himself was not too occupied with making a distinction between 'discursive' and 'non-discursive' as his "problem [was] not a linguistic one" (Foucault, 1980, 198).

[38] A compilation of techniques implies a technology, in Foucault's phrasing a technology of power. However, as Foucault used the terms 'technique' and 'technology' sometimes, not always, interchangeably and because 'technology' in this thesis has a particular meaning as 'information and communications

phenomenon problematised so that it becomes manageable by the techniques available. (See Foucault, 1998, 95; 2010, 4, 19; Deleuze, 1999, 16; 2006; Alhanen, 2007, 104–106; Raffnsøe, 2008, 55–56; Bussolini, 2010; Villadsen, 2021, 475, 479; in reference to biopolitics also Dillon and Lobo-Guerrero, 2008, 273). Foucault investigated discursive practices extensively in The Archaeology of Knowledge (2009a) and the mutually affective construction of knowledge in discourses that evolve into different scientific disciplines in The Order of Things (1994). Material practices became elaborated, for example, as disciplining practices in Discipline and Punish: The Birth of the Prison (1991), History of Madness (2006), and The Will to Knowledge: The History of Sexuality: 1 (1998).

As my main object of enquiry in this thesis is not Foucault's writings but the production of everyday digital security in Finnish Lapland, I will not immerse in the theory of practices. Instead, I will satisfy with Kai Alhanen's (2007, 28–29) summarisation of practices as historically particular ways in which "a phenomenon in some regulated manner becomes an object of thinking and acting" (my own translation). Practices thus constitute their objects and subjects in the processes of objectivation and subjectivation to which I will return in section 3.1.1. "[D]iscursive practices direct thinking by regulating objectivation, subjectivation, the use of concepts, and the formation of theories in discourses" (ibid., 46, my own translation; also, Deleuze, 1999, 16). They are socially constituted ways of uttering that guide the making of new statements and define what can be said in a discourse – and what can be accepted as knowledge (Alhanen, 2007, 59–61, 88; also, Bussolini, 2010, 100; Callewaert, 2017, 36). (For further details, see Foucault, 2009a.) Ilpo Helén (2016, 18) sums up the forms of limitation that operate in discourse regulating what can and cannot be uttered as censorship, distinctions between rational and mad speech, and differentiating between true and false. In order to operate and to affect discursive limitations require institutions and societal practices for their implementation (ibid.).

Material practices then entail all other practices of interaction that direct human behaviour. For example, in the context of digitalisation the fact that service provision moves from physical offices to online platforms modifies people's behaviour as does the ability to follow reindeers on a phone application (see e.g. Salminen, 2021).

technologies' (ICT), I have chosen to violate the generally accepted hierarchical relation between technique and technology and use only technique(s) or compilation of techniques when discussing a dispositive. In Foucault's work, 'techniques' are occasionally more specific, localised and concrete than 'technologies' which refer to more abstract collections of techniques. When direct quotations from either Foucault or commentary literature entail 'technology' or 'technologies', I have not changed the wording to 'technique' or 'techniques'. According to Helén (2016, 89, my own translation), "the technological aspect [of biopolitics] entails the engagement of knowledge with the techniques with which phenomena are made governable". As "techniques generally refer to the organisation of practices in a consistent and systematic manner to affect people's lives", my collation of 'technology' with 'technique' to an extent hides this emphasis on knowledge which 'technology' in Helén's reading has.

Gilles Deleuze (1999, 9, 27) exemplifies material practices as "'instructions, political events, economic practices and processes'". Discursive and material practices are co-constitutive and intertwined, that is, they embed in one another but cannot be reduced to one another (ibid., 10, 27–29).

The combination of discursive and material practices in their mutual relations constitutes a technique of government for managing a phenomenon. The combination of different techniques used to manage that phenomenon forms a technology of power and, furthermore, a dispositive. Dispositive emerges as a response to an urgent need and, thus, has a specific, strategic[39] function in time and in place (Foucault, 1980, 195; Bussolini, 2010, 89). It exists in a constant stage of transformation due to its relational nature, openness, and activities of the 'things' that comprise it (ibid., 195–196; Bussolini, 2010, 90–92; Callewaert, 2017, 45; Villadsen, 2021, 476). Yet simultaneously, it is "a relatively durable network" sustaining itself and supporting and being supported by certain forms of knowledge (Foucault, 1980, 196; Bussolini, 2010, 92; Callewaert, 2017, 35; Walters, 2012, 27, 36).

The phenomenon under scrutiny in this thesis is the securitisation of the digitalisation of everyday life in Finnish Lapland. Its urgency arises from acknowledging the deep embeddedness of digitality in critical infrastructures enabling and sustaining circulation, vital societal functions, as well as service provision and commerce. I will not be able to provide a full account of the governing techniques used in capturing the digital Arctic or constituting cyber/digital security in Finland. Instead, I will focus on the practices of security depicted in pan-Arctic and regional digitalisation strategies, in national cybersecurity and digital security arrangements in Finland, as well as in my studies on digital security (as defined from a human security perspective e.g. in Salminen, 2018a; 2019; 2021; Zojer, 2019b) in the European High North. While the four articles of this thesis depict security concepts related to digitalisation in Lapland, this synthesis examines the implications of their use. Furthermore, the main object of enquiry are the techniques of individual security as those are the common nominator in all of the articles.

Deleuze (2006, 338) has described dispositive as a 'skein', which well capsules the complex entity. It then consists of the lines of visibility[40], utterance[41], power, and subjectivation, as well as the lines of breaking and ruptures (ibid., 339–342; see also Dean, 2008, 23). It is a compilation of changing relations between practices

[39] According to Foucault (1980, 196), the strategic nature of dispositive entails that "it is a matter of certain manipulation of relations of forces". Bussolini (2010, 86) highlights that a dispositive is both strategic and technical. The latter points towards a "plan according to which the different components are in actuality organized in a given apparatus" (Raffnsøe et al., 2016, 278).

[40] 'Visible' in Deleuze's reading of Foucault seems to mainly refer to material practices (e.g. Deleuze, 1999, 28–30).

[41] 'Utterable' in Deleuze's reading of Foucault seems to mainly refer to discursive practices (e.g. Deleuze, 1999, 28–30).

and institutions, which both embody the relative imperatives of power (e.g. Deleuze, 1999, 9–10). Dispositive has two sides: a programme/diagram/strategic imperative and action/actualisation/social apparatus. The diagram is an ideal, both discursive and material, which the dispositive strives to actualise (for instance, cybersecurity as “the desired end state in which the cyber domain is reliable and in which its functioning is ensured” as in Finland’s Cyber Security Strategy [Security Committee, 2013, 1]), but which also changes when the entity changes. (Dean and Villadsen, 2016, 106–107; Foucault, 2009b, 99; Deleuze, 1999, 30–32.) “Every society has its diagram(s)” (Deleuze, 1999, 31; also, Helén, 2016, 164), which are part of dispositives characterised by changefulness embedded in their strategic function, networked alliances, and mode of operation. Dispositive is hence always in the becoming; a future-oriented but never reachable wholeness prone to instability, failures and transformations. (Dean and Villadsen, 2016, 106–107; Foucault, 2009b, 99; Deleuze, 1999, 30–32.) Therefore, according to Maria Stern (2006, 191), “integral to the promise of an assured security is the concealment of the impossibility of fulfilling this very promise”.

Such fluctuations and evolvement are visible also in attempts to conceptualise security in the context of digitalisation (see sections 1.3 and 3). The (re)actualisation of the dispositive’s diagram takes place in a multiplicity of interrelated (through connection, but also through disconnection) discursive and material practices in which the phenomenon is produced, including its framing, and governed. It is also embodied in the institutions established and/or mandated for the management of the phenomenon. Cybersecurity and digital security hence come into being in the discourse(s) and silence(s) revolving around the digitalisation of society or the Arctic (see sections 1.2 and 1.3); in respective regulation(s) and strategic documentation, as well as in their implementation (see section 1.3, later in this section 1.4, and articles I, II and III); in the constitution and implementation of societal and organisational guidelines such as information and/or cybersecurity policies, (technology) standards, netiquettes, good practices and industry best practices (see article III); in ICT and network architectures; in institutions participating in or particularly established for the management of digitalisation such as the aforementioned DVV and NCSC-FI, but also, for example, NESO’s Digipool[42] and Mediapool[43], the

[42] NESO’s Digipool is a network of ICT and communications network industries and authorities such as Traficom i.e. the Finnish Transport and Communications Agency, the Finnish Defence Forces, and NESA. It consists of companies, a management team and working groups, as well as an office. It gathers a situational picture of security of supply within the industries, facilitates the gathering and dissemination of a cybersecurity situational picture, suggest development projects and monitors preparedness in the industries, and organises education and training. NESA (n/d) Poolit. https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/poolit [February 28, 2022].

[43] NESO’s Mediapool is a network of media companies and authorities and similarly structured as Digipool. It supports the technical preparedness of communication industry to crises and hence ensures the freedom of speech in all security situations, advances cybersecurity in media companies, monitors

Data Protection Ombudsman[44], the National Human Rights Institution (NHRI)[45], intelligence bodies and their supervisors (see section 3.2.2), ICT corporations and industry organisations such as FiCom[46] and Finnish Information Security Cluster (FISC)[47], civil society organisations such as Effi[48], as well as research and educational institutions; in people's behaviour and thinking; and so forth. The behaviour of

information influence and social media events, guides and monitors preparedness in the industry, and organises education and training. NESA (n/d) Poolit. https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/poolit [February 28, 2022].

[44] "The Data Protection Ombudsman is a national supervisory authority which supervises the compliance with data protection legislation. [...] [It] is an autonomous and independent authority who are appointed by the government. [...] The Data Protection Ombudsman and deputy data protection ombudsmen form the Sanctions Board tasked with imposing administrative fines in accordance with the General Data Protection Regulation. [...] The Expert Board [...] is tasked with issuing statements on significant questions related to the application of the legislation governing the processing of personal data [...]". Office of the Data Protection Ombudsman (n/d) The Office of the Data Protection Ombudsman safeguards your data protection rights. https://tietosuoja.fi/en/office-of-the-data-protection-ombudsman [February 28, 2022].

[45] "The Human Rights Centre, its Human Rights Delegation and the Office of the Parliamentary Ombudsman together form the Finnish National Human Rights Institution (NHRI). [...] NHRI are autonomous and independent institutions, established by law and with a task to promote and protect human rights. [...] [In Finland,] [it] seeks to contribute to safeguarding the implementation of human rights by monitoring and evaluating, when necessary also critically, the actions of [civil society, human rights research institutions and government], by assisting them to implement human rights better and by making society more conscious of and amenable to human rights". Human Rights Centre (n/d) National Human Rights Insitution (NHRI). https://www.humanrightscentre.fi/about-us/national-human-rights-institutio/ [February 28, 2022].

[46] "Finnish Federation for Communications and Teleinformatics, FiCom, is a lobbying organization for the ICT industry in Finland [...]. [Its] members are companies and other entities that operate in the ICT sector [...]. [Its] task is to promote business opportunities for its members and to enhance their competitiveness [by] influenc[ing] ICT related regulatory issues, promot[ing] the development of information and communications technology, manag[ing] ICT statistics and business indicators, openly communicat[ing] current professional issues to various target groups and contribut[ing] the ICT industry's and digital sector's public image." FiCom (n/d) In English. https://www.ficom.fi/english/ [February 28, 2022].

[47] "Finnish Information Security Cluster (FISC) is an organization [of] major Finnish information security companies to promote their business and operations in national and international context. [...] [Its] main target [...] is to improve cybersecurity and support [...] member organizations' activities in the following areas: increase cross-border activities, promote public-private-partnerships, conduct market surveys, enable national depth and width of high-level education and dialogue with national and international regulatory bodies." FISC (n/d) About us. https://www.fisc.fi/about-fisc/ [February 28, 2022].

[48] Electronic Frontier Finland, Effi ry., is an association tasked to advance the realisation of basic rights and democracy on internet as much as in society at large; in particular, to protect freedom of speech and privacy, as well as to promote balanced IPR system, open access to knowledge, and transparency in administration. In doing so, it conducts research and publishing; organises meetings, training and guidance, and excursions to its members; provides statements on bills; influences political decision making; networks with other similar associations internationally; grants stipends for research; as well as provides legal advice and helps with legal costs when necessary. Effi (2013) Effi ry:n säännöt. https://effi.org/yhdistyksen-saannot/ [February 28, 2022]. My own translation.

individuals and groups of individuals (of which population is the widest) especially is the locus of security.

People are internal to dispositives and act in them (Deleuze, 2006, 345; Foucault, 2009b, 42–44) – hence a dispositive is "a modality of collective participation" (Panagia, 2019, 721) – which becomes easily forgotten in technology focused and/or systemic national security studies of cybersecurity (e.g. Aradau, 2010, 491). Moreover, dispositive does not dominate or coerce, but disposes, arranges and assemblages 'things' in their mutual relations so that a plurality of suitable ends can be achieved (Foucault, 2009b, 96, 99; Bussolini, 2010, 86; Raffnsøe et al., 2016, 274; Panagia, 2019, 716–717, 721). As mentioned earlier in this section, 'things' entail people, goods, services, and material givens, but also ways of acting and thinking, habits and customs, as well as events such as accidents, misfortunes and epidemics (Foucault, 2009b, 19–21, 96–97)[49].

In the dispositive of security, 'things' are calculated and their relations arranged into series of possible events that can be managed through estimates of probabilities. Trajectories perceived as positive are supported while the negative ones are nullified, counteracted, and mitigated. In its most efficient form such control is able to cancel out the inherent dangers of social phenomena by working on the so-called 'natural' processes 'found' embedding in the phenomena. For example, naturalness in population can be 'found' by examining its habitat, socio-economic distributions, regulations to which it is subjected, customs, values, and means of subsistence. The variables on which population depends make it an impossible target of government by direct orders and actions. Instead, its government is only possible through indirectly steering transformations within it, that is, through working on the population's conditions of life, for example, by digitalisation. Moreover, population is made up of different individuals whose behaviour cannot be accurately predicted regardless of how good digital algorithms become, but who all have desires that can be played to generate a collective interest. Finally, population is a set of elements in which constants and regularities are identifiable even in the case of accidents, which again serves as the building ground for both public and private insurance[50].

[49] In comparison, Foucault provided a listing of 'things' in their mutual relations that constituted a heterogeneous ensemble referred to as dispositive in a highly referenced interview in 1977. This listing included "discourses, institutions, architectural forms, regulatory decisions, laws, administrative measures, scientific statements, philosophical, moral and philanthropic propositions – in short, the said as much as the unsaid" (Foucault, 1980, 194). (Cf. the listing in Callewaert, 2017, 35.) However, I would not read this listing as an exhaustive inventory of 'what the dispositive has eaten' but as an exemplary illustration of the way dispositive should be thought of. Bussolini (2010, 92) raises the same point by stating that "[t]he dispositive is not so much the individual elements which make it up [...] as it is the particular arrangement and relations between them". Its dynamic, changing form is decisive. Furthermore, "the same 'elements' or institutions can be part of more than one dispositive". (Ibid , 89, 92; also, Raffnsøe, 2008, 47, 58–59; Raffnsøe et al., 2016, 272–273, 278–280; Callewaert, 2017, 45; Villadsen, 2021, 476.)

[50] Private cyber insurance is an emerging, yet relatively unmatured market. Currently, it is offered as both

(Foucault, 2009b, 19–21, 33, 42, 64–66, 70–75, 325–326; 1998, 25–26; 2010, 16–17, 31–32; Helén, 2016, 64–66, 71–74) It needs to be highlighted in this context that population itself "is not a natural entity but the effect of particular forms of knowledge, the invention of new statistical techniques, sciences like demography, state policies on reproduction, healthcare [etcetera]" (Walters, 2012, 16; Foucault, 2009b, 349; Helén, 2016, 64–66).

1.4.2 Modern governmentality

As security is one of the technologies of power at the disposal of government, the theoretical perspective of the synthesis is modern governmentality[51], that is, a particular rationality guiding the government of the state and society through the capacities and freedom of people. It shapes people's field of possible action, that is, the options available to them, and hence their freedom, but the governed remain free in their ability to act and think in a variety of ways. (Foucault, 2009b, 10; Dean, 2008, 13; Duffield, 2007, 6.) Modern government thus refers to 'the conduct of conduct', that is, "a form of activity aiming to shape, guide or affect the conduct of some person or persons" so that the governed remain willing subjects. (Gordon, 1991, 2–3, 10, 15, 48.) It consists of both self-government and the government of others and is entangled with "a way or system of thinking about the nature of the practice[s] of government (who can govern; what governing is; what or who is governed) [...] capable of making some form of that activity thinkable and practicable both to its practitioners and to those upon whom it [is] practiced" (ibid., 3, 12; Foucault, 2009b, 2, 88; Dean, 2008, 16).

In the ethical sphere, modern government entails the attempts "to make oneself accountable for one's own actions and the practices in which human beings take their own conduct to be subject to self-regulation" (Dean, 2008, 11; Foucault, 2009b, 43–44; Helén, 2016, 78–79, 159–160, 177). In the political sphere, it implies some sort of calculation concerning what is enough intervention in people's behaviour

standalone service and add-on to other insurances. (Kshetri, 2020, 1, 3). Coburn et al. (2018, 235–236) categorise the available products as (1) standalone commercial cyber insurance, (2) errors and omissions insurance, (3) commercial property all-risk insurance, and (4) personal lines insurance. The latter may be included in some homeowner policies or contents insurance products and cover a cyber attack on home computers and/or compensation for compromised personal or financial data. The products varyingly cover losses and costs for the first party i.e. those "incurred directly by your company", and/or the third party i.e. "the compensation that you may have to prove for another individual or organization as a result of your company suffering a cyber incident" (ibid., 236–237). "The main alternatives to buying a cyber insurance are for a company to self-insure or to form an insurance captive" (ibid., 243). Public cyber insurance is discussed shortly in section 4.1.

[51] Raffnsøe et al. (2016, 281) also emphasise the connection between security and governmentality in Foucault's writings (cf. Dillon and Lobo-Guerrero, 2008). Yet, "Foucault never systematically explain[ed] exactly how the notions of biopolitics, security, and governmentality relate to each other" (Raffnsøe et al., 2016, 281).

but not too much, so that the desired ends can be achieved (Foucault, 2009b, 5, 66; 2010, 11–13, 19, 28; Dean, 2008, 10–11.) According to William Walters (2012, 13), it is this understanding of "the interplay between the technologies of the self and the technologies of governing a people, a state or a society" that makes Foucault's approach distinctive and original.

In his lectures, Foucault (2010, 2) referred to governmentality as "the art of governing, that is to say, the reasoned way of governing best and, at the same time, reflection on the best possible way of governing". In addition, "one only governs a state that is already there [...] but also [...] as an objective to be constructed" for which reason "the art of governing must [...] fix its rules and rationalize its way of doing things by taking as its objective the bringing into being of what the state should be" (ibid., 4). Governmentality is hence both present- and future-oriented, but also bound by the past (e.g. Foucault, 2009b, 109–110). The state is then "the correlative of a particular way of governing" (Foucault, 2010, 6).

Modern governmentality is essentially concerned with "the introduction of economy into political practice", governing "in the form of, and according to the model, of economy" (Foucault, 2009b, 95). To govern the state then means "the application of economy [...] at the level of the state as a whole", that is, supervising and controlling "its inhabitants, wealth, and the conduct of each and all" (ibid.). The evolvement and adoption of modern governmentality led to the governmentalisation of the state, that is, "the might of the state came to be based on its ability and skill to govern society and its members as well as to make them governable" in a manner that optimised state intervention to rightly scaled, targeted, and timed actions across societal sectors (Helén, 2016, 133, my own translation, 142; Foucault, 2009b, 106, 108–109; 2010, 10–13, 32). I will examine governmentality in greater detail in section 3.1.

Contemporarily, governmental rationality strives to make cyberspace governable and turn the state to digital and virtual. More precisely, it strives to govern people (re)designing and (re)building this artificial space, acting and inacting in it and in relation to it, acting in organisations controlling its development (or the development of parts of cyberspace), and disassembling it. Therefore, and regardless of the wordings in national and regional digitalisation and cybersecurity strategies, the object of governing is never solely cyberspace, information, infrastructure, functions vital to society, administration, corporations or civic organisations, but always also the behaviour of groups and individuals (see e.g. Foucault, 2009b, 105–106, 122, 129; Gordon, 1991, 3). This aim does not change even if the referent object of security is shifted from information (information security) to infrastructure and/or functions deemed critical for the society (cybersecurity), to individuals and communities (digital security as defined in the ECoHuCy project [Salminen, 2018a; 2021; Zojer, 2019b] or as a human security perspective to cybersecurity; in a parallel manner also as human-centric/human-centred cybersecurity [e.g. Ani et al., 2019; Ceesay et al., 2018; Chong et al., 2019; Deibert, 2018; Renaud and Flowerday, 2017]) or if the referent object comprises all of the aforementioned, that is, digital security as defined by the Ministry of Finance of Finland. The latter concept serves as a good example of the fluidity of the terrain in which this thesis operates: Even if having been utilised by OECD (2015) for longer, the Ministry of Finance of Finland only picked digital security up in 2018–19 (Ministry of Finance, 2018) and properly defined it in 2020. For that reason, it has not been discussed in the articles of this thesis, but become mentioned only in this synthesis.

1.4.3 The individual in digital security

National digital security in Finland is developed together with the implementation of the Ministry of Finance's programme to advance digitalisation in the society. The programme has three main objectives to be reached by 2023: (1) Sterling digital public services are available to both citizens and businesses, (2) many of the public services to businesses are available only in the digital format, and (3) support to the use of digital services is available throughout the country so that the skills of service users can be improved and digital exclusion prevented (Ministry of Finance, 2020a, 4, 12). Digital public services have hence shifted from supportive form of service provision to primary form of service provision over the past three decades (Salminen and Hossain, 2018, 114; Salminen, 2019, 335). In addition, the programme strives to improve the accessibility of public services and the equality of citizens, for example, through sufficient support services and ensuring the realisation of linguistic rights[52]. A parallel programme aims at generating functional digital identification services (Digital Identity project) independent of the identification services provided by banks. (Ministry of Finance, 2020a, 3.)

[52] According to the Constitution of Finland (731/1999), chapter 2, section 17: The national languages of Finland are Finnish and Swedish. The right of everyone to use his or her own language, either Finnish or Swedish, before courts of law and other authorities, and to receive official documents in that language, shall be guaranteed by an Act (Kielilaki [Language Act] (423/2003)). The public authorities shall provide for the cultural and societal needs of the Finnish-speaking and Swedish-speaking populations of the country on an equal basis. The Sami, as an indigenous people, as well as the Roma and other groups, have the right to maintain and develop their own language and culture. Provisions on the right of the Sami to use the Sami language before the authorities are laid down by an Act. The rights of persons using sign language and of persons in need of interpretation or translation aid owing to disability shall be guaranteed by an Act (Viittomakielilaki [Sign Language Act] (359/2015)). According to a language barometer published on February 9, 2021, there are problems in the realisation of linguistics rights: Service provision in Swedish has weakened, a significant share of the Sami cannot receive services in their mother tongue, and individuals using sign language often need to order translators by themselves. (Ministry of Justice (2021) Lakisääteisiä palveluja omalla kielellä ei käytännössä aina saa – tuoreet barometritutkimukset paljastavat monia käytännön haasteita. [In practice one cannot always receive statutory services in his or her own language – latest barometers reveal several practical challenges.] Press release, February 9, 2021. https://oikeusministerio.fi/-/lakisaateisia-palveluja-omalla-kielella-ei-kaytannossa-aina-saa-tuoreet-barometritutkimukset-paljastavat-monia-kaytannon-haasteita [February 18, 2021].)

Digitalisation and digital security as defined by the Ministry of Finance are prime examples of the modern government of individuals and population within the dispositive of security through digitality. For example, the digital security curriculum of DVV aimed at improving citizens' digital literacy now entails trainings on 'Digitally Secure Life' targeted at and open to everyone, free of charge, and available on the agency's website. At the time of writing, eight trainings (the duration of which is from 30 minutes onwards) are available and categorised either as "for organisation's entire personnel" (six courses) or as "for organisations' managers and digital security specialists" (two courses). They cover issues such as digitally secure working life, data management, data protection and privacy, digital security for local government officials and for county government officials, as well as risk management, and securing digital operations during incidents. In addition, anyone can download the 'Digitally Secure Life' mobile game to test his or her digital literacy in working life "as an employee of the imaginary Municipality of Tyrskylä". (DVV, n/da.) The object of government is thus nothing less than life itself (e.g. Foucault, 2009b, 165).

Moreover, the agency is coordinating and developing a nationwide Digituki (digital support) network consisting of municipalities, public administration, associations, multiple projects, and companies. Regional Councils, with financial support from the Ministry of Finance, are connecting entities providing digital support into regional networks, which constitutes a part of the national network. Providers of digital support can also enrol to the national network through an online form. Digituki entails support for individuals' independent and safe use of ICT and digital services. This entails in practice remote support through chat, video or phone; face-to-face support in service points, at home or by peers; and trainings provided, for example, online or by folk high schools. DVV as the coordinator organises a monthly network event for the member organisations providing information on the network development and presentations on digitalisation. In addition, it organises a monthly webinar to the personnel or volunteers of these organisations addressing, for example, the needs of different customer segments and other themes related to the practices of everyday digital support. (DVV, n/db.) Lapland was one of the pilot regions that began developing digital support in 2018[53]. In 2019, the network extended to 14 regions. (DVV, 2020.) At the time of writing, DVV is applying permanent funding for Digituki, which would begin from the beginning of 2023 (DVV, n/db).

In Lapland, the role of public libraries, folk high schools, and town or municipal halls and Virtu service points in developing people's digital literacy and/or providing

[53] The development of Digituki in Lapland is coordinated by the Regional Council of Lapland and carried out by the Centre of Expertise on Social Welfare in Northern Finland. Further information is available on the project website at https://www.sosiaalikollega.fi/hankkeet/lapin-digituki-hanke [December 16, 2020].

support either in the form of advice or equipment cannot be downplayed. According to the Act on Public Libraries[54] (1492/2016), all municipalities need to organise a public library and all public libraries are tasked, inter alia, to provide access to data, information and cultural content, as well as to provide information services, guidance and support in information acquisition and its use as well as for versatile literacy. In order to carry out its tasks, the library has to have appropriate facilities, up-to-date equipment and enough skilled personnel. In other words, public libraries are tasked to provide support also in running errands safely in cyberspace.

Folk high schools, again, "are educational institutions that offer liberal adult education in both general education and vocational education and training" as regulated by the Act on Liberal Adult Education[55] (632/1998). Most of the schools are private, but all of them get funding from the state. (Kansanopistot, n/d.) Anyone can study a variety of digital skills on different courses and/or in degree programmes provided by folk high schools throughout the country. Finally, town or municipal halls and Virtu service points provide equipment and to an extent support in running errands safely in cyberspace. "Virtu service points are local residents' places for electronic services" equipped for the use of internet and videophone services, as well as for printing, copying and scanning documents (see e.g. Virtu Service Point Manual, n/d). There are currently 22 service points across Lapland[56].

The production of security in digitality thus takes place primarily by removing the obstacles to circulation and through the simultaneous government of one and all on an everyday basis (Foucault, 2009b, 147–190, 192). The aim is to improve the overall digital literacy of the Finnish population by improving the digital skills and awareness of every individual. Improved digital literacy among the citizenry makes the population governable in an efficient and economic manner by the techniques that secured digitalisation provides. Government focuses on supporting the necessary human capacities so that the circulation of useful data and information in the society can be ensured and maximised (see Foucault, 2009b, 2, 13–15, 19; cf. supporting the wellbeing of population in welfare state e.g. Helén, 2016, 66–71). Government and security are inseparable, but there are problems in their application to cyberspace – as it will be discussed in section 3.2.

The Ministry of Finance's programme to advance digitalisation in society and digital security framework to an extend meet the demands for a widened and deepened understanding of cybersecurity put forward in the ECoHuCy project. For example, digitalisation and security in the digital sphere are now addressed together and their interdependency is recognised (e.g. Ministry of Finance, 2020b, 10), efforts to improve the equality of access to information and digital services continue, there

[54] Laki yleisistä kirjastoista.

[55] Laki vapaasta sivistystyöstä.

[56] See the listing of Virtu service points at https://virtu.fi/ [March 26, 2022].

is a practical attempt to diminish the pool of people without the necessary skills, and questions of sustaining cultural and linguistic diversity have been included in the discussion (cf. Salminen and Hossain, 2018, 111, 113–114; Salminen, 2019, 322, 324, 327; Salminen, 2021). The general observation that "the individual is often left alone to find ways to carry out his or her responsibility to secure him- or herself" (Salminen, 2019, 332) still holds, but now there is a nation-wide effort to coordinate the attempts to improve everyone's digital literacy (cf. earlier scattered attempts, e.g. Salminen, 2019, 336).

However, the main critique of not including individuals and communities in defining both digitalisation related opportunities and challenges for themselves and engaging them in decision making remains unaddressed. People are still objectivated as targets of development instead of being active subjects deciding for themselves (also Ministry of Finance, 2020b, 12, 20). Even when subjectivities are produced, individuals become objectivated mainly as troublemakers or mere rule followers – in any case, people whose behaviour needs to be contained, including increasing self-containment (Zimmermann and Renaud, 2019, 174–175; also, Chandler and Reid, 2016, 1; Macmillan, 2011, 5, 7).

Zimmermann and Renaud (2019, 173) detail how "the 'human-as-problem' mindset manifests in measures that exclude the human or constrain human behaviour by requiring compliance with security policies". Eventually, people are expected to make the 'right choices' and adapt to both digitalisation and the prevailing forms of its securitisation, which highlight the importance of resilience of all actors in society. Moreover, according to Stevens and Vaughan-Williams (2016, 2, 5), "despite [...] burgeoning expectations that citizens should become stakeholders in and indeed agents of national security, still relatively little is known about how citizens conceptualise and experience 'threat' and '(in)security' in the context of everyday lives [and] whether they are aware of, engage with, and/or refuse government attempts to enlist them in building societal resilience".

According to Chandler and Reid (2016, 1), actually, "[t]he promotion of resilience requires and calls forth a much degraded subject, one defined by much diminished capabilities for autonomy and agency [...]. [...] Rather than enabling the capacities of peoples and individuals for autonomy so that they can make their own decisions as to how they wish to live, the discourse of resilience understands autonomy as a threat to life". Subjectivation in digitalisation thus follows modern governmentality in identifying merits, subjecting to continuous networks of obedience, and compelling to self-confession (Foucault, 2009b, 184–185; 1998, 18–21, 59–61, 65–67, 85). I will return to the topic of subjectivities in the art of government embedded in digitality in section 3.3. Before that I will summarise the articles that constitute the empirical part of this thesis and discuss how human security serves to support modern governmentality in section 2.

2. Everyday digital security in the European Arctic

2.1 Introduction to the articles

The four articles of this thesis examine the intertwinedness of digitalisation and cybersecurity in the everyday lives of people in the European High North, principally in Finnish Lapland. Each of them provides a partial answer to the research question – *How does the government of the emerging digitalised everyday life take place in Lapland through the production of individual security?* – and serves a particular function in building the overall argument of this thesis.

First, Salminen and Hossain (2018) sets the framework for a human-centred cybersecurity understanding in the European High North by asking: What is a human security approach to digitalisation and cybersecurity? In answering to the question, it utilises both national and regional strategies related to digitalisation and cybersecurity, as well as a conversation with local stakeholders in Lapland at the Arctic Centre of the University of Lapland in 2016. Second, Salminen (2019) introduces an example of an inconsistency embedded in the processes of digitalisation that becomes securitised not as a question of security in the digital sphere but as a question of everyday security in the physical sphere. It relies on media reports discussing a healthcare related event in south-western Lapland that culminated in 2017 and depicts the tensions inherent in the structural reorganisations that digitalisation facilitates. Third, Päläs and Salminen (2019) focuses on the responsibilisation of individuals as a technique of security. It examines how in Finnish law an individual can retrospectively be interpreted as responsible for, for example, a crime committed against him or her through a reference to duty of care. Comprehensive societal security and national cybersecurity arrangements entail that everyone does his or her part in the production of security, which currently implies an undefined level of digital literacy. Finally, Salminen (2021) is an empirical case study from Enontekiö, which is located in north-western Lapland and one of the most sparsely populated municipalities in Finland. Under scrutiny are local people's accounts of digital security that were constructed in two workshops carried out in the municipality in 2018 and then organised with a thematic content analysis.

The main argument of this thesis is that the way the digitalisation of society has been carried out in Finland is not only providing new opportunities to people and communities, but also reinforcing and creating insecurities amongst them. These insecurities are less related to technical vulnerabilities embedded in ICT and/or strategic security threats listed on national security agendas than to people's experiences amidst digitalising everyday life. While the society has placed much effort in connecting all households and businesses, for example, through nationally and EU-funded technology programmes; improving the equality amongst digital service users, for example, through accessibility programmes; strengthening privacy, for example, through data protection regulation; and fortifying digitalised infrastructure, for example, through network and information systems regulation and safety standards, it has only partially recognised and addressed the everyday insecurities that people tell about. Simultaneously, security production in society has been decentralised to societal stakeholders ranging from an individual to the state, which has created an imbalance between what is expected of the security producers and what their requisite digital skills and cybersecurity awareness are. Such discrepancies suggest that the securitisation of societal digitalisation has succeeded only to an extent.

In other words, the digitalisation of society is an effort to set up and sustain an economically efficient and effective order of government that largely depends on individuals', communities' and populations' technology-mediated self-government. Connecting everyone and everything; making people dependent on digital services for running their daily errands, studying, having hobbies, communicating, and/or enjoining entertainment; as well as educating and training them to act in a safe and responsible manner in the digital sphere turns individuals and communities into a governable population. Such government does not take place through coercion, but through people's freedom, even if it may utilise the techniques of law and discipline in the attempts to control the flows of information that are necessary for it to function. It is thus not only the Arctic regions that need to tap into the crucial flows, but the society in its entirety. Resistance or indifference to societal digitalisation; lacking or insufficient digital literacy; and distrust towards digital platforms, services, networks, and equipment hinder the development of such a government system for which reason they are increasingly labelled as dangerous and addressed as security problems. Securitisation of societal digitalisation enables its government through enhanced control.

In this section 2., I summarise the articles I–IV by providing their research settings, questions and arguments, practical implementation, and conclusions. In the next section, I discuss them further in the light of Foucault's and Foucault inspired accounts on modern governmentality on themes that emerged in discussions with local people in Lapland alike. The reason for such theoretical duality is the aforementioned theoretical ambiguity of human security to which the governmentality perspective provides additional rigour by showing how well-meaning human security efforts tend to support modern governmentality thus narrowing human freedom instead of purely empowering individuals and communities.

2.2 Article I: Digitalisation from a human security perspective in the European Arctic

When preparing the ECoHuCy project, Kamrul Hossain and I co-authored an article[57] which for the first time imagined what a human security approach to cybersecurity in the European High North could entail. Article I is hence an applied theoretical piece combining human security, human rights, and securitisation frameworks in order to refocus cybersecurity research on individuals and communities' everyday experiences amidst overarching digitalisation. It critiques the majority of digitalisation and cybersecurity policies and research for, first, separating positive digital development and its negative side effects onto two separate agendas and, second, considering individuals and communities merely as passive receivers of security instead of acknowledging their active role as security providers, who ought to have a say in the development of their life environment (Salminen and Hossain, 2018, 111, 113). Third, it calls for better contextualised research on cyber-physicality because "regional challenges posit people and communities to either beneficial or detrimental positions in information society" (ibid., 110). Such challenges include, inter alia, the state of information and other infrastructures, socio-economic positions, demographics, levels of digital literacy, physical distances and climate (change), as well as cultural diversities (ibid., 113).

The theoretical framework within which article I builds its arguments combines human security, human rights, and securitisation theory in a reinterpreted form. Human security is characterised as a preventive and pro-active approach which entails a multilevel security structure incorporating actors inside and outside the state. It recognises multiple sources of instability that affect individuals and communities in their everyday lives making them vulnerable to a variety of threats. "Fulfilling the basic human needs for survival stands at its heart", which is "guaranteed by the means of enjoyment of universal human rights". (Salminen and Hossain, 2018, 111.) Regarding the relationship between human rights and cybersecurity, the article highlights how "[c]ybersecurity is a means to protect human rights offline" by protecting critical infrastructure and granting access to digitality (ibid., 112). In addition, human rights, such as "freedom of opinion, expression and assembly, and the right to privacy", need to be protected online, which attaches the approach to issues such as commercial information collection and its further utilisation (ibid.). Human security aims at emancipating and empowering people "to address urgent issues in specific situations" by exercising

[57] Because the article does not specify the author roles, I shall do it here. As the lead author, I was responsible for all other parts of the text except the theoretical piece bringing human security and securitisation together. For the theoretical part, Kamrul wrote a draft which I then modified further and fitted with the rest of the text.

choice and, thus, to “avoiding risks and improving the system of protection” (ibid., 111–112).

However, neither human security nor human rights can explain the process in which an issue becomes a security question. For that reason, securitisation theory is added to the theoretical mix of article I. (Salminen and Hossain, 2018, 112.) Security is then “claimed as a social construct by virtue of a speech act” (ibid.). When an issue is accepted as a security problem by the audience to whom the speech act is directed, it is removed from the standard political agenda and the use of extraordinary measures to return it to this agenda becomes possible. However, threats identified within human security follow another kind of securitisation logic. “The point at which a threat matures is unknown and undefined” making it possible for threats to “arise from everyday situations and nebulous sources”. (Ibid.) This expansion of securitisation theory enables striving towards “a redefinition of cybersecurity that takes regional particularities into consideration, and […] the aim of empowering people and communities seriously”, for it provides room for them to serve as securitisation actors (ibid., 112–113).

At the time of writing the article, the pivotal Arctic governance bodies were only gradually becoming interested in digitalisation as a transformative process in the Arctic either under the label of ‘telecommunications’ or ‘connectivity’. Digital development was instead advanced through national and regional programmes in Norway, Sweden and Finland. However, cybersecurity seemed not to be an Arctic issue but a concern in national policies and programmes. (Salminen and Hossain, 2018, 109.) Article I takes a different approach by examining the European High North “as an entity with particular characteristics and connections across national borders” (ibid., 108). Furthermore, it contextualises both positive security (freedom to something, the opportunities that digitalisation provides) and negative security (freedom from something, the mitigation of threats that it generates) to individuals’ and communities’ everyday lives (ibid., 108, 113, 115). The purpose of such a move is twofold: to introduce cybersecurity onto human security agenda and to expand cybersecurity research to human security issues. Thus, a more comprehensive research framework for examining everyday digitalisation and cybersecurity concerns also from the perspective of people and communities experiencing them can be established. (Ibid., 108–109, 111, 115.)

The starting point of article I is that neither digitalisation nor cybersecurity are neutral technical processes that treat all people, institutions, and locations in the same manner – unlike national policies and programmes assume. Instead, the so-called developing regions within the Nordic states struggle to have their interests and needs heard in national planning and implementation. (Salminen and Hossain, 2018, 108–109, 111.) The article utilises both national and regional strategies (16 recent strategies altogether; see ibid., 109), as well as national level statistics (see ibid., 114–115) to establish this contradiction, but concentrates on the commonalities in regional digitalisation agendas that report consultations with local stakeholders (ibid., 110–111). Data collection also included a meeting with the representatives of the Regional Council of Lapland, Lapland Hospital District, and the Centre of Excellence on Social Welfare in Northern Finland on August 15th, 2016 at the Arctic Centre in Rovaniemi.

The aforementioned commonalities in regional digitalisation agendas include, first, an emphasis on "the urgency of improving information infrastructure and connections [...] for the benefit of local people, communities, businesses and administration" and on "the role of [ICT] in the overall societal and economic development" of the Arctic regions (Salminen and Hossain, 2018, 110). Second, they entail "the need to fit digital services to user needs and the demand for [...] flexible", easy-to-use, and safe services that ease everyday life in the regions. Third, digitalisation ought to "facilitate the development of local businesses into skilled utilisers of digital opportunities" and educational institutions "should be allocated the resources necessary for self-development towards digital forerunners". Fourth, the digitalisation of public "administration requires reformed through and operating models". Finally, "solutions based on open data and open source code are to be favoured and supported". (Ibid.)

The role of regional administrations in digitalisation is significant for they develop infrastructure and digital services, channel state and/or EU funding to projects, and coordinate cybersecurity by applying national strategies locally (Salminen and Hossain, 2018, 109). The state's "main task is to provide good conditions for the utilisation of digital opportunities", which it carries out, for instance, "by reforming regulations, formulating clear policy goals, removing obstacles to positive development, funding research, promoting networks and connections, and protecting society from grave cybersecurity threats" (ibid., 110). Yet, because "[e]veryone's actions affect (in)security and (un)trustworthiness of the globally interlinked digital environment and everyone is affected by the activities of others", everyone also has been given "a role to play in the processes of digitalisation and its safeguarding" (ibid., 109–110). In terms of power relations, the public administration is to pave the way for individuals to make best out of digitalisation, but in a responsible manner.

The article strives to problematise, first, the prevailing understanding of the Nordic states as homogenously developed information societies and, second, the prevailing understanding of cybersecurity as the safeguarding of the functioning of society through critical infrastructure protection and information security (Salminen and Hossain, 108, 114). A national focus "masks regional digital divides, threats and fears, and their consequences in people's everyday life", alongside which "regional political, socio-cultural or economic tensions do not easily transmit to nationally focused decision making, as they are perceived to be marginal, concerning only a small number of people or a fragment of the market or economy" (ibid., 110). A narrow cybersecurity understanding focusing on the protection of information and infrastructure, again, misses out human security concerns merely as second- or third-order effects (ibid., 112).

As solutions to the aforementioned problems, article I suggests considering the northernmost regions of Norway, Sweden and Finland "as an entity in which digitalisation is supported and secured through a shared regional framework rather than three national ones" (Salminen and Hossain, 2018, 110). Alternatively, the existing national policies could be intensified and modified "so that regional particularities receive the deserved attention" (ibid.). Either of the solutions could "truly respond to the interests, need and fears of people and communities, while taking economic, socio-cultural and environmental characteristics into consideration" (ibid.). All in all, "a widened digital ownership [and stakeholdership] is required" (ibid., 114). As a topic to be included in the widened cybersecurity agenda, the article suggests, for example, digital divides such as the gap between people with proper access to ICT and those without or with limited access, but also divisions "along wealth, gender, geographical and social lines" (UNHRC, 2011, 17 cited in Salminen and Hossain, 2018, 114). While "digitalisation has the potential to address existing human inequalities", it may also enhance them (ibid., 114). The same applies to environmental concerns (ibid., 113). Of the topics found from the prevailing cybersecurity agenda, cybercrime and digital abuse, again, should find their ways onto human security agenda as well (ibid., 114–115).

In the conclusion, the article reiterates that digitalisation and cybersecurity programmes serving aggregated national and supranational interests have thus far paid inadequate attention to whether they "help realise the opportunities and/or mitigate the threats residing in regional digital development" (Salminen and Hossain, 2018, 115). "In order to address the existing gaps in knowledge" and improve the targeting and inclusiveness of policies, "a comprehensive study of digitalisation and cybersecurity from [a] human security perspective is crucial" (ibid.). It should be conducted in cooperation with individuals and communities living in the European High North. The current regional silence over cybersecurity can indicate "confusion over who should be doing what [...] and what cybersecurity entails at the regional level". (Ibid., 115–116.)

2.3 Article II: Individual security amidst the re-organisation of health and social services in Lapland

Whereas article I is a general appraisal of the specificities of human-centric cybersecurity in the European High North, article II focuses on two aspects of human security in particular: personal security and health and social security. It aims "to create room for bottom-up influence on the primarily top-down processes of security production" 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 [...] Finnish Lapland" (Salminen, 2019, 321). The article is a case study of a health and social security related event in south-western Lapland that escalated to a nation-wide political power struggle in 2017.

Personal security in article II is understood as "protection from harm caused by the state, other states, other groups of people, individuals and gangs" with additional attention paid to "threats at women, children and to self" in both physical and digital life environments (Salminen, 2019, 333). In fact, because ICT have penetrated the Nordic societies to the extent that "actions in the digital sphere affect the physical environment" and vice versa, the article uses the nominator 'cyber-physical' to describe people's everyday life environment (Salminen, 2019, 322; see also Salminen, 2018a; Salminen et al., 2020b). Personal security then covers issues such as privacy and data protection, personal integrity, access to and usability of services, digital literacy, and confidence to (in)act online (Salminen, 2019, 333–336).

Health security in the article is understood "as protection from diseases, malnutrition, unhealthy lifestyles and harmful environmental impacts. It also entails access to healthcare." (Salminen, 2019, 338.) Social security, again, relates to "one's ability to provide him- or herself and the family" and entails issues such as compensation for loss of income; "payments to the elderly, the permanently disabled and the unemployed; family, maternity and child allowances[;] and the cost of welfare services" (ibid.). The pivotal tension in the article lies between the Finnish Government's plans to restructure health and social service provision nationally inter alia with the help of digitalisation and local resistances to such plans in Länsi-Pohja[58] (ibid., 323).

The article has two primary tasks following the outline of the ECoHuCy project: First, to redefine cybersecurity from a human security perspective and as contextualised to the European High North and, second, to examine individual (in)security in the context of health and social services digitalisation as a component of regional administration reform in Finland. Digitalisation of services has been justified as a way to continue service provision or to bring it closer to customers in sparsely populated areas, whereas the counter-discourse perceives it as a way to withdraw services from these areas and to concentrate them to population centres (Salminen, 2019, 322–323; see also Salminen, 2021, 167–168, 170–171, 173–174). The main argument of the article is that poorly justified reform plans that fail to accommodate individuals' and communities' everyday insecurities lead to contested decisions and disputes. National programmes for service digitalisation and

[58] Länsi-Pohja is a region in south-western Lapland comprising the towns of Kemi and Tornio, as well as the municipalities of Keminmaa, Simo, Tervola, and Ylitornio.

withdrawal from areas that do not meet the nation-wide quotas of treatment sessions should be discussed openly and with all relevant stakeholders instead of dissociating them to closed agendas that may not intersect. (Salminen, 2019, 347–349.)

Article II begins by introducing the evolvement of national digitalisation and cybersecurity policies effective in the European High North. The northernmost areas of Norway, Sweden and Finland manifest an interesting duality for they are simultaneously both laggards (in terms of, for example, infrastructure) and forerunners (in terms of, for example, digital education and health and social services) in digitality. (Salminen, 2019, 322, 328.) Similarly to article I, article II then notes how digitalisation of society has generated a need for novel forms of security and discusses the prevailing understanding of cybersecurity, which "brings together responses to the vulnerability of [ICT] and national security concerns", that is, the protection of information and infrastructures (ibid., 324–325). Yet, the mainstream understanding recognises the human being mainly "as a major vulnerability [...] due to his or her gullibility or vengefulness" (as a potential malevolent, a risky employee, or a possibly digitally illiterate citizen unable to protect him- or herself online) and, thus, allocates inadequate attention to people (ibid., 325, 331). "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" (ibid., 326).

Considering cybersecurity from a human security perspective changes not only the referent object of security (from information, infrastructure, and critical functions to the human being), but also the perceived threats (from cyber threats to threats to human wellbeing) and the security measures at one's disposal (Salminen, 2019, 329). Because "both technical[59] and strategic[60] threat depictions remain fairly abstract and distant to people's everyday experience", there is a need to concretise and approximate the language. By doing so, room can be generated for bottom-up influence in cybersecurity production and knowledge-related power positions that favour experts and exclude laymen may be partially dismantled. (Ibid., 330.) Moreover, as the prevailing understanding of cybersecurity tends to neglect or only inadequately addresses positive, empowering security, the utilisation of a human security approach can rebalance the understanding (ibid., 331).

The prevailing cybersecurity understanding requires that people do their part in the production of comprehensive societal security. The problem is that

[59] The technical threat depiction "lists items such as malware, web based attacks, web application attacks, denial of service, botnets, phishing, spam, exploit kits, data breaches, and identity thefts" (Salminen, 2019, 329).

[60] The strategic threat depiction usually includes "cyber activism (or hacktivism), cybercrime, politically and/or economically motivated espionage, cyber terrorism and cyber operations (or warfare)" (Salminen, 2019, 329).

"[w]hile the existing societal (security) organisations are busy with finding solutions to the protection of [...] 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" (Salminen, 2019, 332). Without knowing the principles of cybersecurity such a responsibility may appear absurd, uninteresting, or as overreacting – or it may prevent one from using ICT altogether (ibid.). The problem relates to transparency and privacy, for in the name of security "people may be expected to live a [...] transparent life 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 [...] add to this transparency requirement". (Ibid., 333–334.) Yet, personal security and privacy are mutually constitutive, for example, in terms of wholeness of self-image and bodily integrity, as well as ability to controls one's social appearance and protect identity (ibid., 334). Often individuals decide in and with regard to cyberspace without recognising all security implications of their choices.

Human security also notes factors that empower individuals to improve their personal security in and with regard to cyberspace. It points out that digitalisation generally amends people's access to information and that the difficulty arises in deciding what information is relevant and/or accurate (Salminen, 2019, 337). In addition, it to an extent facilitates people's ability to check, correct, and control information collected of them. Moreover, "enhanced connectivity enables, inter alia, social interaction and running errands across time and distances" hence, for example, reducing the need for travel and improving emotional wellbeing. It also facilitates the publication and dissemination of information about wrongdoings. (Ibid.) However, the digital skills and awareness of individuals may not meet what is required in order to make best out of digitalisation, which, again, impacts their willingness, for example, to use digital services and platforms. "Advice and support [...] has been arranged, for instance, by municipalities, non-government organisations, volunteers, service providers and state authorities [...], but people utilise or do not utilised the provided support for a number of reasons", including shame, protest, frustration, learning difficulties, and indigence. (Ibid., 335–336.)

The final section of article II provides a digitalisation of health and social services related case study from south-western Lapland by the Swedish border. Under scrutiny is a dispute between the Finnish Government, two then existing healthcare districts in Lapland (Lappi and Länsi-Pohja), a private multinational healthcare corporation and its competitors, as well as two towns and four municipalities constituting the region of Länsi-Pohja (Salminen, 2019, 338). "The dispute centres on the threat of eliminating some of the [central] hospital functions" in the region, but continuing them in the other hospital district approximately 100 kilometres away (ibid., 339). It "embeds in two Finnish [G]overnment projects: one of [digitalising] a bigger share of public services and another of restructuring health and social [...] service" provision nationally (ibid.). Both projects had been carried out in Lapland for years prior to the dispute (ibid., 339–341). Nonetheless, the dispute centres upon the physical provision of health services, while digitalisation and social services receive relatively little attention (ibid., 347–348).

The case study is conducted by constructing a historical narrative of the events that culminated in late 2017 from news reports published by the local editorial staff of the national broadcasting company, YLE, on its web portal. "The data source was selected for its national coverage", even if regional and local newspapers were considered as well (Salminen, 2019, 341). "The pieces of news were collected by searching with different combinations of keywords" from the web portal in December 2017. This led to a sample of 79 news articles published between June 16, 2015 and December 22, 2017. Additional data collection on the digitalisation of public services in Lapland took place in a public discussion titled "Arctic Cafe: Digitalisation – An opportunity or a threat to people living in Lapland?"[61] organised on April 4, 2017 at the Arctic Centre in Rovaniemi and online.

Historical narrative is a common method, for example, in study of history, but I consciously apply it to a too small sample, because it is a good way of representing the case studied in the article. "There is no agreed definition of a historical or any other kind of narrative" (Salminen, 2010, 58), but as a thumb rule "narratives tell about events and how human beings experience them" – either their own experience or somebody else's (Hyvärinen, 2009, 1–2 cited in Salminen, 2010, 59). "Furthermore, narratives construct an order and [become] presented in a recognisable way in the medium that transmits them" (Salminen, 2010, 59). "A narrative consists of, at least, two events so that something can change [...] but it does not necessarily have to come to some kind of an end". "The process of relating events to one another is commonly called emplotment [...] [carried out] by using a priori known signs, rules and norms so that, for example, the combination of actors, ways of acting, circumstances, interaction and suggested results become recognisable and acceptable to the receivers" of the narrative. However, "narratives contain contradictions, conflicts, tensions, contingency and simultaneity [...] [and] are always told for some purpose", for which reason there are alternative narratives of the events. (Hyvärinen, 2006; 2009; Czarniawska, 2004 cited in Salminen, 2010, 59.) In sum, a narrative is "an emplotted presentation of suspected events in the past". It "has an author who selects an event as a starting point by attaching some value to it", which is then "followed by a group of selected and organised happenings as transformational elements leading to a selected end". (White 1975, ix – x, 5 cited in Salminen, 2010, 60.)

When preparing for the regional re-organisation of health and social services in Lapland, significant differences in the preferences of the two then healthcare districts became evident. "[T]he representatives of Länsi-Pohja felt that their concerns were

[61] "Arctic Cafe: Digitalisaatio - lappilaisten mahdollisuus vai uhka?" My own translation.

not addressed or even heard in the negotiations, but the representatives of Lappi were pushing for service centralisation [...]. Lappi responded by pointing towards requirements set by legislation and practical necessities [...]. On the background was mistrust felt towards the negotiating partner due to past experiences" and the main issues included the continuation of basic healthcare provision close to customers as well as the preservation of delivery ward and extensive emergency duties in Länsi-Pohja. (Salminen, 2019, 342.) While the negotiations were ongoing, the region's towns and municipalities reactivated the examination of alternative ways of organising health and social services. One of the options was an extensive outsourcing of health services to a private corporation, which was interpreted "as a means of pressuring the negotiating partner and the [G]overnment". (Ibid., 342–343.)

"In the spring 2017, the negotiations about the division of work between Länsi-Pohja and Lappi [...] ended without a result" and outsourcing of the services began to look likely (Salminen, 2019, 343–344). This state of affairs stirred calls for returning to the negotiating table and concern that "outsourcing would not safeguard services and jobs in the area" or that the profit motive would rule over the local needs (ibid., 344). By contrast, it was presented that outsourcing would be the only option to avoid decision making and service provision slipping away from Länsi-Pohja. Finally, the Government established a working group "to provide a compromise solution to the dispute" and put forward a bill to tighten the conditions for outsourcing. (Ibid., 344–345.) The latter move speeded up processes in Länsi-Pohja, which was countered by blaming the region for endangering health and social service re-organisation in entire Lapland (ibid., 345).

The dispute culminated in autumn 2017, for instance, in local demonstrations both pro and contra outsourcing (Salminen, 2019, 345). The towns and municipalities eventually decided for outsourcing and a co-owned company with a multinational healthcare corporation was established. Mud-slinging from all sides continued in media and investigations about the legality of the move took place, but local people "expressed fears for uncertainty regarding, for instance, the pricing and availability of services", familiarity of personnel at healthcare stations, treatment of individuals without the ability to decide for themselves, and child health services and school nurses. (Ibid., 345–347.) The outsourcing contract was signed before Christmas and came to force in the beginning of 2018 (ibid., 347).

Regardless of the then ongoing national digitalisation and restructuring projects, "[n]either social services nor digitalisation ever became a major item in the [media] discussion. Instead, the dispute centred on the location of physical healthcare [stations]. While digitisation changes both the reach and availability of [...] services, it was only mentioned, for instance, when [the future provision] of healthcare was envisioned", not as a factor in restructuring of the time. Not even if the healthcare corporation had also expressed interest in service digitalisation. (Salminen, 2019, 347–348.) Thus, people's everyday health and social security concerns do not seem to revolve around digitalisation, which nonetheless lays on the background of the restructuring of welfare services. (Ibid., 348–349.) "[T]here 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 be treated equally", and not become marginalised by digitalisation (ibid., 350). Only in that way the shift in responsibility from the public administration to the individual which digitalisation entails can be somewhat fair.

"It seems that the nation-wide re-organisation of health and social [...] services, including [their digitalisation], [still] 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 [provision], increased freedom of choice, and more customer say." "In people's perceptions, their everyday security does not revolve around digitalisation" but the physical location of service stations. (Salminen, 2019, 348.) Ultimately, article II "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." (Ibid., 351.)

2.4 Article III: Responsibilisation of individuals for cybersecurity in Finnish contract law

Article III, co-authored with Jenna Päläs, examines individual security in digital sharing economy from the perspective of consumer responsibility, responsibilisation, and risk allocation in Finnish contract law. Its pivotal argument is that legislation in force, similarly to such societal practices as labelling digisavviness as a 'civic skill', providing information and inducing guilt, presupposes a particular level of individual diligence, competence and understanding in and with regard to cyberspace, but this required level has not been unambiguously defined anywhere. Instead, it becomes established on a case-by-case basis in retrospective legal practice. (Päläs and Salminen, 2019, 321, 331–332, 348, 370–371.)

The theoretical framework of article III is modern governmentality and, in particular, the responsibilisation of individuals that embeds in it (see Päläs and Salminen, 2019, 324–325, 331–332). However, human security has guided the choice of perspective: individual security and consumer protection in everyday cyber-physicality contextualised by, for example, Finnish law, its application, sharing economy platforms, know-how of network users, state of infrastructure, geography, economic positions, and culturally-bound value systems (ibid., 331). Similarly to article II, article III focuses on individual security amidst the digitalising everyday life and concretises how ordinary, but complex, problem cybersecurity is. Self-evidently, people living in Finnish Lapland use sharing economy platforms as well, and are bound by the practices in which their security and the related subjectivities become produced. Often it is the individuals themselves who are expected to provide for their security (ibid., 370).

The article's starting point is consumer protection in modern sharing economy carried out by law by restricting consumer liability. However, law also poses obligations to consumers regarding their behaviour in cases of unauthorised use of means of payment, communications services, or methods of digital identification. These consumer obligations are related to diligence and prevention of risks. Ignoring them will lead to liability for risks and damages following from one's (in)action. (Päläs and Salminen, 2019, 322.) Thus, according to the findings of article III, the mechanisms of consumer protection also enable the responsibilisation of consumers on the basis of contract terms, industry practices, and so forth. The article examines under which conditions the consumer is liable for unauthorised use of his or her means of payment (including bank and credit cards, payment solutions related to mobile phone subscriptions and applications, and online banking credentials) and/or methods of digital identification. In addition, it investigates what kind of duties to act legislation related to unauthorised use sets to consumers, how those have been applied in legal practice, and how those concretise on digital platforms. The holistic aim is to evaluate the level of 'digital civic skills' that can be expected of the users of sharing economy platforms and whether it can be assumed that they recognise the threats and risks inherent in cyberspace. (Ibid., 323.)

Thus, article III focuses on the conduct of sharing economy platform users and the level of diligence required from them (Päläs and Salminen, 2019, 322). In practice, when the issue is unauthorised use, the holder of the means of payment and/or methods of identification is a victim of crime, but this does not affect the evaluation of his or her own responsibility (ibid., 323). While there is no specific cybersecurity law in Finland, the users' diligence and risk management abilities have been prescribed in the Payment Services Act (290/2010), the Consumer Protection Act (38/1978), the Act on Electronic Communications Services (917/2014), and the Act on Strong Electronic Identification and Electronic Trust Services (617/2009)[62]. Research on how individuals are responsibilised for cybersecurity took place by examining duty of care provided by the aforementioned laws.

[62] Maksupalvelulaki (290/2014), Kuluttajansuojalaki (38/1978), Laki sähköisen viestinnän palveluista (917/2014) sekä Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009). My own translations.

The method of analysis is phenomenon centric doctrinal legal research[63]. Doctrinal legal research is about synthesising principles, norms, rules, interpretive guidelines and values, which rationalises "a segment of the law as a part of the larger system of law" (Bhat, 2019, 145). In other words, it is about "[a]bstracting ideas from diverse [sources] and consolidating them through synthesis", that is, legal reasoning or rational deduction, in order to grasp the legal system's simultaneous constancy and change, which is also affected by social facts and historical genesis (ibid., 143–144, 145). It addresses both "the 'is' and 'ought' aspects of law", that is, the reality considered objective as well as "ideals and visions put forward through justificatory arguments" with the aim of generating "internal coherence and conceptual clarity required for a better understanding of the law and legal system" (ibid., 148).

Safety and trust are essential factors in value creation dependent on communications networks, which has integrated cybersecurity firmly in the structures of digitalising society (Päläs and Salminen, 2019, 319). Cybersecurity is both a desired end state and the compilation of means and procedures utilised to reach that end state. Since the human being is a component in information systems of which cyberspace consists, individuals have a number of subjectivities in digitality. They are targets of cyber threats, but also threat sources such as malevolent actors or systemic vulnerabilities. In addition, they serve as "providers of cybersecurity, because when acting skilfully and expectedly in the digital environment, individuals contribute to both security and trust". (Ibid., 327.) Cybersecurity, both as an objective state of affairs and as a subjective evaluation, is a precondition of trust needed for people to engage in digital activities (ibid., 320, 328–329). "Lack of trust in the digital environment becomes a problem, for example, in situations in which the service that the individual needs or wants is available only in the digital format and on a platform, which use he or she does not consider safe" (ibid., 329). Not to mention that he or she may in retrospect be judged as responsible for misconduct regardless of, inter alia, inadequate digital literacy.

The Payment Services Act (290/2010) regulates the contractual relationship and liability distribution between the user and the provider of a payment service. The premise is that carrying out a payment requires the consent of the payer – if the payer

[63] Ilmiökeskeinen lainoppi. My own translation. Phenomenon centric doctrinal legal research comes close to problem oriented doctrinal legal research (ongelmakeskeinen lainoppi, my own translation). The latter strives to combine different fields of law and different levels of defining a legal problem (a technical legal problem, a societal problem, and the means which the legislator has at its disposal to fix a societal shortcoming) in order to establish a comprehensive, systematic understanding of the norms relevant for the legal problem. It aims to systematise the legal order, not merely a particular field of law. (Kangas, 1982, 383–387; see also Päläs and Salminen, 2019, 322, footnote 12.) While the problem oriented doctrinal legal research operates within law, phenomenon centric doctrinal legal research begins with a problematisation adopted from another discipline, for example, social sciences and carries out doctrinal legal research on that basis, that is, interpretation and systematisation, concerning the relationship between law and the phenomenon in question. It does not strive to systematise all relevant norms, but focuses on this relationship. (See Päläs, 2022.)

has not given such a consent in a pre-agreed manner the payment is unauthorised. If the service provider nonetheless carries out the payment, it bears the responsibility to return the payment or compensate for it. (Päläs and Salminen, 2019, 333.) The service provider's liability is limited by, for instance, the payer's duty of care and precautionary requirements (ibid., 334).

The holder of the means of payment must use it according to the rules of the user agreement and look after it and the related methods of identification in a reasonable manner. This responsibility begins when the holder receives the means of payment and ends, for example, when he or she reports it as lost or used in an unauthorised manner. (Päläs and Salminen, 2019, 334, 338.) The holder of the means of payment is liable for its unauthorised use when he or she has consciously and voluntarily given it to such a use, neglected the duty of care, or neglected the duty to report the means as missing without an undue delay. In legal practice, the diligence of the payment service user is evaluated. (Ibid., 335.) The requisite retention obligations include, inter alia, that the means of payment and the related methods of identification are kept separately so that an outsider cannot connect them to one another. In addition, the holder must check every now and then that the means is not missing. (Ibid., 336–337.) Gross negligence is in question when the holder of the means of payment ignores security risks related to its retention and use (ibid., 338). When evaluating the seriousness level of negligence, the likelihood of risk and whether the holder has increased this likelihood by his or her own conduct is taken into consideration. Moreover, whether the holder has or whether he or she should have acknowledged the risk matters. (Ibid., 339.)

The aforementioned consumer obligations are relatively straightforward in the physical environment. However, bank and credit cards are increasingly used in digital platforms and novel means of payment such as mobile pay and digital purses have been developed – alongside novel forms of abusing or compromising such services – for which reason their application in the digital environment is worth pondering upon. (Päläs and Salminen, 2019, 342–343.) As a rule, it is the duty of the payment service provider to prove that the payer has given consent to the payment, whereas the user of the payment service may be requested an account of the events and his or her own conduct (ibid., 343–348). The circumstances of each case play a great role when judging the level of knowledge, understanding, and skills required from a diligent consumer – alongside the estimation of what one should have concluded on the basis of general knowledge and information provided (ibid., 348).

Neglecting the duty to act despite acknowledging the related security risk, carelessness, and facilitating the realisation of such risk stand at the heart of estimating consumer (gross) negligence. Remarks about security risk in user agreements or service providers' announcements seem to increase precautionary requirements. However, the user agreements that define customer liability are generally one-sided, non-negotiable standard agreements which the customer needs to accept in order to use the service. Often agreeing to the use of service under such and such rules is carried out without even reading the agreement but just clicking it as 'agreed'. It may thus be that the service user is bound to precautionary requirements and risk avoidance measures of which he or she is unaware. (Päläs and Salminen, 2019, 349–350.)

The Payment Services Act applies also to payments carried out by mobile phone that are charged in the phone bill. However, it does not cover payments in which the phone company serves as a payment broker for digital content or audio services. The Act on Electronic Communications Services (917/2014) applies to such situations instead. It regulates risk and liability sharing between the user of communications service and the telecommunications company with regard to unauthorised use and damages following from it. Providing evidence for unauthorised use may be difficult for the consumer due to the complex nature of communications services, for which reason the preparatory material highlights that the risk may not fall upon the service user due to the impossibility of providing evidence. (Päläs and Salminen, 2019, 351–352.)

The Act on Electronic Communications Services does not define content for the service user's duty of care. However, the Consumer Disputes Board[64] has outlined that unauthorised use of phone subscription is comparable to the use of bank and credit cards in terms of the risk of misuse and protection from it. Therefore, retention obligations and the obligation to check every now and then that the mobile phone and the related identifiers have not been lost are part of the service user's duty of care. In addition, the user has to ensure adequate information security on his or her equipment. (Päläs and Salminen, 2019, 352–353.) The service user is liable, inter alia, in case the loss of the equipment or its unauthorised use results from his or her greater than lenient negligence. The seriousness of negligence is, again, estimated on a case-by-case basis. What the consumer should have known or done weighs in the estimation, as does an evaluation of what could be expected of an average consumer in similar circumstances. Similarly, information provided by the telecommunications company and the contract terms play a role in the estimation. The service user's liability ends, for example, when he or she has reported the loss of equipment to the service provider and requests the service to be closed. (Ibid., 353–354.)

Using digital platforms generally requires some form of user identification. Methods of digital identification base on information and characteristics of a person's digital identity. Digital identity is a basic element, for example, in running errands

[64] "The Consumer Disputes Board is an independent and neutral arbitrator. It provides recommended decisions in judicial disputes between consumers and companies." "It operates in the administrative field of the Ministry of Justice and outside judicature as an alternative body for arbitration." Kuluttajariitalautakunta (n/d) Tietoa meistä. https://www.kuluttajariita.fi/fi/index/tietoameista.html [March 17, 2022]. My own translation.

and legal capacity in cyberspace. Methods of digital identification individualise the service user by comparing information provided by him or her with the information hold by the service provider. Such identification methods can be divided into weak and strong based on the certainty of individualisation. Strong identification is regulated by the Act on Strong Electronic Identification and Electronic Trust Services (617/2009), whereas weak identification relies on the terms of user agreements and the general principles of contract law. (Päläs and Salminen, 2019, 355–358.) Strong identification methods need to combine at least two of the following verification factors: (1) something that the service user knows, (2) something that he or she has at his or her disposal, and (3) a physical characteristic of a natural person. The basic principle of is that a trustworthy actor belonging to a trust network guarantees the identity of the service user so that the service provider or a third party can be sure about who the user is. (Ibid., 357.)

Unauthorised use of methods of identification concerns erroneous positive identification due to deceitful conduct or disturbance in the identification service. A person can then identify him- or herself as someone else and carry out legal transactions. The starting point is that the holder of the method of identification is not liable for such transactions. However, service providers operating online also need to be able to trust that the service user is who he or she claims to be. By breaching the obligations set in the Act on Strong Electronic Identification and Electronic Trust Services and in the terms of the user agreement of the identification method, the holder becomes liable for unauthorised use. (Päläs and Salminen, 2019, 359.) The retention obligations and duty to act are similar to those in the Payment Services Act (ibid., 359–360). The Act on Strong Electronic Identification and Electronic Trust Services specifically forbids handing over a method of digital identification to someone else's use consciously and voluntarily. The holder becomes liable also in cases of greater than lenient negligence that lead to, inter alia, the loss of the method and/or when he or she neglects the duty to report the method missing. (Ibid., 360.)

The act does not define the holder's liability or to whom he or she is liable. However, the decision KKO 2016:73 of the Supreme Court rules that the holder's liability compares to consumer liability in cases of unauthorised use of means of payment or credit. If the unauthorised use of the methods of identification is caused by the holder's negligence, he or she is also liable for the credit agreement thus committed. In other words, the holder is liable for the legal transactions carried out through unauthorised use, which extends the legal consequences beyond the contractual relationship between the service provider and the service user. (Päläs and Salminen, 2019, 361–363.)

In sum, user responsibility in all of the aforementioned laws is culpability, that is, neglecting duty to act defined in legislation and user agreements leads to liability. However, the liability systems differ from one another with regard to the extent of contractual obligations. (Päläs and Salminen, 2019, 364.) Therefore, the Finnish Competition and Consumer Authority[65] has called for examining whether different liability systems entail such contradictions and ambiguities that the consumer may have to bear disproportionate liability for unauthorised use. It may be difficult for the consumer to discern which legislation is applied in which case and how the requisite level of diligence becomes defined. (Ibid., 365.) Victims of unauthorised use have the right to be compensated by the wrongdoer, but the damage is paid by the victim if the wrongdoer cannot be reached or he or she is insolvent (ibid., 369).

Moreover, the increasing use of phone applications for payment and identification requires pondering upon the expectations towards consumers and whether the intertwinedness of service providers complicates liability chains too far. When estimating liability in and with regard to cyberspace, consumers conduct and risk awareness seems to become highlighted, but it is not self-evident what level of skills and understanding can be expected of them. (Päläs and Salminen, 2019, 366.) The continuous development of digitality demands respective adaptability from consumers (ibid., 367). In addition, it may be difficult, if not impossible, to determine in some situations which of the parties has neglected his, her, or its duties (ibid., 370).

2.5 Article IV: Everyday digital security in Fjeld Lapland

Article IV brings the study of digitalisation and cyber/digital security firmly back to the framework of human security and the European High North. It is an empirical case study on the opportunities, hopes, challenges, and concerns that digitalisation generates amongst the population in north-western Finnish Lapland (Salminen, 2021, 158). Its focus is hence on people's experiences related to the effects that digitalisation has on everyday life and the feelings of (in)security, (dis)trust, and participation it awakes (ibid., 159, 160). Under investigation are the questions: Which 'things' related to the quickly advancing digitalisation people find beneficial and which detrimental? Whether people think they can influence digital development? What kind of hopes and challenges relate to digitalisation and its effects on everyday life? (Ibid., 159.) Given the climate and geography,

[65] The Finnish Competition and Consumer Authority "ensures as fair and efficient market performance as possible for the benefit of the national economy and consumers". It "ensures a better balance for all consumers – also those in a more vulnerable position – in their relationship with companies" and "that companies' success in the market is based on their own merits rather than artificially restrictive practices or unfair advantages". Furthermore, it "ensures that public bodies do not exploit unfair competitive advantages arising from their position in their business". Finnish Competition and Consumer Authority (n/d) Well-functioning markets, more informed consumers. https://www.kkv.fi/en/information-on-the-finnish-competition-and-consumer-authority/ [March 17, 2022].

demographics, limitedness of livelihoods, economic pressures, infrastructure, and lifestyles in north-western Lapland, the article illustrates how "digitalisation and everyday security concerns related to it are always bound by time and place" (ibid., 158–159, 162).

Article IV begins by anchoring the case study to both physical and digital conditions prevailing in Enontekiö – a municipality serving as a representative of Fjeld Lapland[66] in the study. It moves on to human security and explains how 'digital security' in the article refers to factors related to societal digitalisation that arose in workshops organised in Enontekiö and that either improve or diminish everyday wellbeing (Salminen, 2021, 160). Improving the wellbeing of individuals and communities is the goal of human security. A narrow understanding of human security emphasises only the reduction of violence – direct and structural, physical and psychological. However, a broad understanding covers also the reduction of scarcity and facilitation of people's freedom and self-fulfilment. Individuals and communities are then defining their own security and threats against it. (Ibid., 160–161.) The article builds on this broader understanding. It also highlights how human security is based on basic and human rights. As the states may breach their citizens' rights, the latter should be primary. Moreover, human security should be understood as a threshold. When an issue crosses this threshold, it may turn into a security threat. What is pivotal, is the issue's urgency. Decrease in everyday insecurity and unhappiness, again, indirectly contributes to societal security. (Ibid., 161.)

Digitalisation is in the article defined as an increase in the availability and quality of telecommunications, as well as a broader societal transformation in which different walks of life become re-organised due to the increasing use of ICT (Salminen, 2021, 161). Like article I, article IV notes how ICT are often understood as a somewhat neutral transformative force that treats everyone in a similar manner. Yet, the relationship between human beings and technologies is socially constructed and varies between societies due to different historical layers of values, attitudes, beliefs, institutions, and practices. Technology is developed in response to everyday needs, but it also changes these needs and integrates technology-mediated human interaction in the society's institutional structure. (Ibid., 162.)

Security questions related to digitalisation are similarly socially constructed, which generates room for intervening in contents that security may encompass (Salminen, 2021, 160). Cybersecurity generally strives to protect the confidentiality, integrity and availability of information, as well as infrastructure deemed as critical, vital societal functions, or more broadly the functionality of society, including inter alia democracy and the realisation of human rights. The purpose of article IV is to resolve what kinds of contents digital security takes on in everyday life in Fjeld

[66] Fjeld Lapland consists of the municipalities of Enontekiö, Muonio, Kittilä, and Kolari. Enontekiö is located in Sápmi, by the borders of Norway and Sweden.

Lapland. It hence serves a dual purpose of developing the concept of 'digital security' from a human security perspective and of filling this concept with content provided by people living in Enontekiö. The aim is similar to articles I and II.

The case study was carried out by organising two workshops in late 2018 in Enontekiö (in two different locations, the municipality centre Hetta and the border village Kilpisjärvi) to discuss with the local residents about digital services and the ways they utilise and would or would not like to utilise ICT in their everyday lives. Inspired by the world café method[67], the workshops were informal group discussions over a cup of coffee and open to all interested. The discussions were guided by five groups of research questions that were all covered during the two-hour workshops. No background information was collected of the participants, nor was the sample controlled in other ways. Article IV also does not report in which of the workshops something was said. This was important for generating an atmosphere of trust in the discussions. In addition, due to the sparsity of population in Enontekiö, it was perceived as necessary so that the speakers could not be recognised from any discussion fragments. (Salminen, 2021, 163–164.)

The workshop discussions were recorded, transcribed, and rearranged with a thematical content analysis so that a wide overall picture of the effects that digitalisation generates in people's lives in Fjeld Lapland could be established (Salminen, 2021, 159, 163–164). Relationships between issues, their similarities and differences, guided the construction of themes in the analysis. It was also noted whether a theme was valued as positive, negative, or neutral; whether it received different values in different contexts; and to which other themes it was (un)connected. (Ibid., 164.) In article IV, themes arising from the discussions (n=31) were arranged and reported under structural themes (n=5), that is, themes drawn from the five groups of research questions. The article 'translates' the discussions into the language of security when needed and also reports 'survival strategies' that people resort to amidst digitalising everyday life environment. (Ibid., 165.)

The five structural themes consist of "Uses of ICT", "Digital opportunities for human security" / "Digital challenges for human security", "Factors that advance the desired kind of digital development and obstacles to it", "Individuals' abilities to influence the digital development", and "The roles of different actors in the production of digital security" (Salminen, 2021, 165). The analysis first points out the importance of phone as a multipurpose device, including its security function, in sparsely populated areas characterised by long distances. However, the security function of the phone is fully dependent on the operation of the communications networks of which it is a node. As people had experienced long service breaks, a false feeling of security generated by the phone and one's

[67] For an overview of the World Café method and its applications see http://www.theworldcafe.com/ [March 18, 2022].

own dependency on it were acknowledged. In addition, even if phone generates security, expectations of constant reachability were found strenuous. (Ibid., 165–166, 168–169.)

Second, age cohort was seen as a factor in the use of ICT as for the youth it provided novel opportunities, but a concern was presented on behalf of the elderly living alone and not being used to ICT and digital services. In addition, it was stated that the local characteristics of digitalisation ought to be recognised better in societal steering as well as by the companies providing digital services, solutions, and/or devices. (Salminen, 2021, 166.) The general attitude towards the use of ICT was more positive in Kilpisjärvi than in Hetta, which may be explained by the difference in experience: Whereas digitalisation has facilitated the withdrawal of physical services from Hetta, it has brought services closer to people living in Kilpisjärvi (ibid., 166–167).

Digitalisation provides a number of opportunities, but also generates several challenges for human security in Fjeld Lapland. It was pointed out that many digital services function well and the improved access to information facilitated forethought in multiple everyday situations. The main benefits mentioned were the decreased need for travel, more freedom in the use of time, increased efficiency, more hobbies and free time activities, and improved availability of commodities. Local applications, services, and uses of social media, in particular, were praised and told to enhance, for example, communality, economic security and traffic safety, as well as to facilitate the realisation of basic rights. (Salminen, 2021, 167–169, 173.) However, when 'things' did not proceed in an acceptable manner, insistence and claiming of basic rights were perceived as the only way, for instance, to receive equal treatment or service (ibid., 166, 170, 174).

Digital health services were perceived in a positive light. It was also envisioned that social media could be developed to a direction in which it served as a tool for aid and support instead of hate speech, blaze, and misinformation. Dissing and intervening in local matters from afar were perceived as having become easier due to social media and concerning immigration or Sámi issues in particular. (Salminen, 2021, 168, 172.) Finally, digitalisation had changed both education and work improving the chances for training and studying (without the need to move away from the municipality), distance work and shared work. Distance work and studying were, however, not always seen in a positive light as they also increased equipment requirements and expectations of constant availability. (Ibid., 166, 169.)

People acknowledged that smooth everyday life in Enontekiö to an extent depends on digital services. Nonetheless, the use of digital services was perceived as somewhat forced for physical service points located far away. Digitalisation also positions individuals in society in an inequal manner depending on, for example, their awareness and skills, economic wellbeing, and the location of their house or apartment which positions them differently in communications networks. In addition, not everyone was willing to learn the necessary skills or accepted all services or applications. It was pointed out that the actors who either forced digitalisation or provided the necessary services should have an ethical responsibility with regard to the usability of services, information collection and utilisation, information and data security, as well as for providing the customers with an opportunity to manage information collected of them. Centralisation of services in particular was told to having had decreased service quality, mainly because of the utilisation of chatbots, lacking local knowledge, long waiting times, and advancement of self-service culture in all sectors. (Salminen, 2021, 170–171, 173.)

Digital literacy was recognised as one of the biggest challenges in digitalisation. In addition to varying skills and experience, incertitude, lacking guidance, and individual attitudes were perceived as obstacles for reaping the benefits of digitalisation. Moreover, the right to privacy occasionally complicated counselling. (Salminen, 2021, 171.) People were familiar with information security, data security, and cybersecurity questions, which affected their online behaviour. It was told, for example, that one did not click on links on social media and paid attention to which websites he or she visited (ibid., 172). The question of surveillance, again, divided the workshop participants into those who were willing to give up privacy to an extent so that authorities could intervene in harmful trajectories and into those who stood strongly against unlimited surveillance. Doubts towards the authorities' abilities to keep information safe and secured were also presented. (Ibid., 171–172, 174.) Lastly, the lessening ability to repair equipment and devices due to their increasing digitalisation was mentioned as development that decreased self-sufficiency in Fjeld Lapland. In addition, the relationship between digitalisation and environmental security ought to be better acknowledged and scrutinised. (Ibid., 166, 172–173.)

When factors that either advance or hinder digital security eventually become normalised into societal structures, they also transform the understanding of what a desired kind of digital development entails. The main message from the workshops was that digitalisation should be steered towards a direction in which it becomes more humane and begins advancing human wellbeing. Services should not become fully automated and impersonal, but more reciprocal. (Salminen, 2021, 173–174.) Instead of becoming a 'digitalisation municipality', Enontekiö could also serve as a hideaway from too advanced digitalisation and a retreat from social media. Everyone does not wish for the same things, but somehow compromises need to be reached and everyone's participation, security and wellbeing in society ensured. (Ibid., 173.) However, influencing the direction of digital development was experienced as difficult – in addition to which not everyone had thought of whether he or she would like to have a say in it. One could mainly affect his or her own behaviour, conduct of the near ones, and to choose which applications and services he or she adopted. Changes were induced by someone or something else whereas one could mainly try to adapt to them. (Ibid., 174.)

With regard to the security roles in society, individuals were perceived as responsible for their online behaviour, but the responsibility for cyber/digital security was said to be shared between all actors in society. Moreover, some of the decisions would have to be taken even at the level of the European Union. (Salminen, 2021, 171, 174–175.) The fact that the importance of individuals' behaviour popped up in discussions every now and then indicates that responsibilisation of individuals for cyber/digital security has to an extent been successful. However, as responsibility and actions that improved human wellbeing were called for from ICT corporations and societal decision-makers, securing cyberspace is not solely a task of individuals making rational choices for their own benefit. People in Enontekiö hence both accommodated and resisted the contemporary forms of digitalisation and its securitisation.

2.6 Human security in support of modern governmentality

While the four articles of this thesis criticise the mainstream understandings of cybersecurity as too narrow and exclusive, this synthesis claims that regardless of its emancipatory aims, a human security approach (like the digital security approach of the Finnish state) reinforces modern governmentality. Indeed, human security and national security can be seen as mutually consolidating (Duffield, 2007, 111; Pupavac, 2010, 705; Anttila, 2012, 32; Salminen and Hossain, 2018, 113). Human security aligns with modern governmentality, for example, by highlighting the importance of bridging the digital divides through education, training, and peer support; raising individuals' security awareness; and calling for improved availability and accessibility of digital content and services. It wishes to equalise everyone's access to digitality and to ensure that digital development advances human wellbeing towards its unspecified fulfilment. Thus, it strives to produce digital citizens capable of harnessing the opportunities provided by digitalisation for the improvement of their quality of life. As the other side of the coin, it supports the production of population governable within the contemporary economic order that creates and sustains relations of power which benefit above all transnational corporations, but also autocratic governments capable of almost perfecting societal control through omnipresent surveillance and correction of human behaviour.

Interestingly, corporations and governments are also the main target of human security's criticism towards power relations that exclude, repress, mask, and conceal. It hence focuses on power in negative terms and discusses the productivity of power under empowerment and institutional support to people's freedom to choose for themselves. This criticism is to transform the prevailing relations of power to better address the interests, needs, and fears of individuals and communities.

For the production of skilled enough, but not too skilled, digital citizens, the main question is whether people internalise the guidance related to safe, secure, and unoffending behaviour in and with regard to cyberspace. In other words, how they adopt the practices that enable them to care for themselves – and hence for others – in the digitalising everyday life. (E.g. Foucault, 1998, 53–54, 61–63; Foucault, 2009b, 181–182; Helén, 2016, 76–77, 102–106.) This question does not only entail adopting the 'normated' and 'normalised' attitude but also working on the self, which takes time (Sheringham, 2006, 366). The preference is "for localised, diversified, 'bottom-up' kinds of knowledge formation that could perhaps transform public policies" (Dean and Villadsen, 2016, 56) but that, nonetheless, entangles with the dominant forms of knowledge constituted, inter alia, in power relations in the fields of science, politics, economy, military, and administration. As a consequence, human security fails to question the sensibility of all-encompassing digitalisation, but adopts its progressive ethos as development. A more radical approach celebrates resistance to both digitalisation and its securitisation as alternative forms of self-care (see section 4.1).

Human security thus fails to critically investigate the sensibility of securitising digitalisation and the changes it induces in everyday life as well. While securitisation serves the political aim of increasing the importance of issues and, thus, manages to draw attention to them (see Wæver, 1995), the issues it moves onto security agenda may have already been discussed on other agendas – without the related urgency, but possibly with wider participation and even better outcomes. This move brings in institutionalised security actors to discuss human wellbeing, which transforms the problematisation of wellbeing but also of human security (see e.g. Mäkinen, 2010; Turner et al., 2011). Thus, instead of making bold securitisation moves, it may be best to focus on people's everyday experiences, the ways of uttering they utilise when discussing digitalisation and security, and the daily material practices in which they mitigate insecurities and generate security (see McCluskey, 2019, 5; Prokkola, 2018, 4; Salminen and Hossain, 2018, 112; Salminen, 2021).

According to Emma McCluskey (2019, 9) security is "not an elite, exceptional, decisionist [political phenomenon] but a banal, routine practice of various professionals of security", who in the Finnish comprehensive security model encompass all actors in society (also, Barnard-Wills and Wells, 2012, 230; Prokkola, 2018, 4–5). Important are the ways "in which different bodies of knowledge are *labelling* security, examining the tensions and controversies between different actors in these labelling practices, as well as their wider effects" [...] and "the relationship between the construction of the security label and the boundaries of the security practices that may in fact be labelled by others as freedom, mobility, violence, privacy, or indeed human rights or hospitality" (McCluskey, 2019, 10, italics original). What McCluskey calls labelling, I have called framing in this synthesis. Securitisation is hence a multidimensional process compiling several discursive and material practices and engaging multiple actors in the production, dissemination, acceptance and alteration of threats and risks, as well as of experiences of danger (Prokkola, 2018, 5).

According to Foucault (2009b, 45), the apparatuses of security have a constant tendency to expand as new elements are integrated in them. As an example, the strategic securitisation of cyberspace took its early steps in the 1990's, but has become a major industry in the 21st century (e.g. Salminen and Kerttunen, 2020). Simultaneously, digitality is gradually expanding its standing in security across societal sectors (Rajavuori and Huhta, 2020). While it is of great importance that the human security approach to cyber/digital security envisioned in the articles of this thesis pays attention to individuals' and communities' broad concerns amidst digitalising everyday life, by doing so it also contributes to the expansion of security. Because the everyday insecurities related to digitalisation still largely go either unrecognised or non-investigated, the expansion is welcome. Yet, even if the apparatuses of security 'let things happen', instead of regulating everything as disciplinary apparatuses tend to do, they seek a firm control over events, which reduces, for example, human freedom to freedom of choosing between acceptable alternatives (Foucault, 2009b, 45). Thus, the goals of human wellbeing and fulfilment always escape the practices of human security.

The importance of digitalisation and cyber/digital security lies in the effects they constitute in everyday life. All strategies and policies discussed in this thesis agree on this at some level. Even if eventuality, disturbances and emergency situations, weighs heaviest on national cybersecurity agenda, it acknowledges that the basis for operating in exceptional circumstances is laid in normal conditions (see Security Committee, 2013; 2017a; 2019). The same principle applies to technical cybersecurity. While examination of the everyday is a theoretical strand of its own (see e.g. de Certeau, 1988; Sheringham, 2006), in this thesis it becomes highlighted, firstly, because of the attention that human security pays to it. Human security leaves the everyday untheorized, but basically it refers to the life environments of individuals and communities.

Secondly, the everyday experience was also in the focus of Foucault's investigations. What was important to him was "a direct link to ordinary people's problems, especially people who are incarcerated or disempowered" in some way(s) (Dean and Villadsen, 2016, 51). The complexity of problems such as security in and with regard to cyberspace appears in connection with people's lives, not as an abstract play of thought (ibid., 49). Indeed, modern governmentality as the 'conduct of conduct' takes people's entire life in all its multiplicity as the object of government striving to guide every aspect and every moment of it (Foucault, 2009b, 165; also e.g. Foucault, 1991, 140–141). Thus, "[f]ar from being dominated by the sameness, the everyday is an arena of endless difference" (Sheringham, 2006, 22) or multiplicity (Foucault, 2009b, 11, 21). Theorising on the everyday evolved "by finding ways of teasing out the complex imbrication of the positive and the negative, alienation and freedom, within the weave of everyday life", which itself embeds "the possibility of its own existential or ontological transformation" (Sheringham, 2006, 12, 34–37).

Thus, it may also entail the means for resisting the art of government embedded in omnipresent digitality, even if "[c]yber security concerns all walks of life" (Security Committee, 2013, 33).

The next section of this synthesis provides Foucault's and Foucault inspired accounts of the techniques with which everyday cyber/digital security in Finnish Lapland becomes produced. It focuses on techniques that were brought up by the articles of this thesis. It also continues the discussion on digitalisation and cyber/digital security techniques effective in Lapland, Finland, and in the Arctic which I began in section 1.

3. Government through cyber/digital security

3.1 Governmental rationality embedded in digitalisation

3.1.1 Objectivation and subjectivation of 'things'

With modern governmentality Foucault referred to a certain rationality that guides the acts of government aimed at producing an efficient and economic order within society (e.g. Walters, 2012, 30; see e.g. Foucault, 2009b, 95, 98–99). It combines different forms of power (sovereign, disciplinary and pastoral powers) and knowledge[68] and the requisite techniques for the government of life (biopower), while simultaneously changing these forms of power, knowledge, and their techniques (see Foucault, 2009b; 2010). Foucault used 'government' in both a wide and a narrow sense (Gordon, 1991, 2; Walters, 2012, 11; Helén, 2016, 131), which to me in Finland entails the acts of representative political bodies, the functions of bureaucracy, the activities of actors and bodies trying to influence formal decision making, as well as the operation of economy and civil society and the conduct of citizens vis-á-vis each other, other 'things' and themselves. According to Gordon (1991, 2–3), while Foucault took interest in the interconnections between the different forms of government, his lectures, in which governmentality was principally addressed, focused on government in the political sphere (see e.g. Foucault, 2009b, 87–114, 286–287)[69]. Self-government

[68] Power and knowledge are tightly intertwined and "it is in discourse that power and knowledge are joined together" (Foucault, 1998, 100). Discourses are the basic elements of knowledge that aims to produce truths, that is, Foucault was primarily interested in scientific discourses and the emergence of 'things' within them. "Discourse [as well as silence and secrecy] transmits and produces power; it reinforces it, but also undermines and exposes it, renders it fragile and makes it possible to thwart it" (Foucault, 1998, 101). Therefore, for example, with regard to sex, the question to be studied was: "In a specific type of discourse on sex, in a specific form of extortion of truth, appearing historically and in specific places [...], what were the most immediate, the most local power relations at work? How did they make possible these kinds of discourses, and conversely, how were these discourses used to support power relations?" (Foucault, 1998, 97.) Foucault thus "rejects the idea that universal objects exist and opposes the arguments that there are any constants in human history" (Walters, 2012, 16). Instead, "objects must be allowed to become a site of historical emergence in its own right". They have "'not always existed' but [are] 'nonetheless real' and 'born precisely from the interplay of relations power [...]'". (Ibid., 17.)

[69] Walters (2012, 12–13) makes the same notion. Furthermore, he distinguishes between three forms of governmentality in Foucault's writings. "In its broadest sense governmentality is a heading for a project that examines the exercise of power in terms of the 'conduct of conducts'". In narrower senses, it is a particular domain of government – government of and by states – or serves almost as a synonym to "the conduct of a liberal approach to [government]". (Ibid., 11–13, italics removed, 30.) Yet, Walters (2012,

and governmental practices diffused within society became addressed under other labels such as biopolitics, ethics and aesthetics.

Government entails attempts to shape behaviour according to particular norms for a variety of shifting ends. Such attempts take heterogenous range of ‘things’ as their objects, for which reason the referent objects of cyber/digital security also vary. (Dean, 2008, 10–11.) Governmentality thus entails multiple aims advanced in a number of dispositives so that the society as a whole becomes a compilation of diffused (even contradictory) aims and governmental techniques (e.g. Helén, 2016, 141–142). The same phenomena become simultaneously governed in different dispositives. Yet, what is notable is that ‘government’ or ‘power’ do not only operate in the political sphere or constitute a kind of order of domination in which the powerful suppress the powerless, but become constituted in the relations between people and people and other ‘things’ in all their existence (e.g. ibid., 18; Foucault, 2009b, 65–66). These very same relations then construct people and other ‘things’ through the practices of objectivation and subjectivation. The forms of subjectivity hence “intersect with the modes of government of the self and others” (Macmillan, 2011, 4).

Objectivation entails the ways of turning a matter or a phenomenon into an object of thinking, acting and influencing (Alhanen, 2007, 21). On one level, this thesis is a study on the objectivation of digitalisation and cyber/digital security in particular in its various framings, policies, and institutionalising practices that are gradually taking shape. Objects come to being and exist in discourse, as well as vanish from it, through a network of rules that define relations between ‘things’ and conditions for objectivation in that particular discourse. The aim is not to reveal the true nature of ‘things’, but the discursive practices that enable speaking of the object in the way it is spoken of at the time and in the place (ibid., 64–65). These ways of thinking and speaking guide the formation of material practices – and vice versa.

According to Alhanen (2007, 16, 22, my own translation), the question of how individuals have become objects of their own thinking, that is, “how practices objectivate people into different kind of subjects” is at the heart of Foucault’s writings. This subjectivation entails the ways in which “the subject who thinks of and acts towards objects is set, defined and modified” (ibid., 21, my own translation). It also includes the techniques through which people’s thinking, behaviour and acting are influenced by following a certain model (as in prison, at school, in military, in asylum, and so forth), as well as the techniques of directing people to think and observe themselves as thinking, desiring and acting subjects (the so-called techniques of the self) (ibid., 22–23). On another level, this thesis is then an investigation of subjectivities available to individuals in cyber/digital security and the production of those subjectivities.

6, 39) warns against conflating governmentality and liberalism as the latter does not exhaust the former. In this thesis, I do not distinguish which form of governmentality I am discussing when. Instead, I use governmentality varyingly in its both wide and narrow senses.

Discourses create different kind of subject positions, which people acting in the discourse can occupy and which change as the discourse changes. These positions are not defined by the thinking subjects' ideas and acts but by the rules of the discourse. (Alhanen, 2007, 67–69.) Subjectivities are hence always intersubjective and constituted in social interaction directed by the rules of discourse. Power and knowledge embed in the relations between people and people and 'things' and, therefore, the different framings of cyber/digital security objectify objects and subjects differently and provide subjects with different positions to think, speak, act, and influence (see section 1.3). However, differences in objectivation and subjectivation do not necessarily indicate different rationalities of government but the different framings of cyber/digital security may well support the same governmentality as section 1.4 already emphasised.

Modern governmentality, which simultaneously individualises and totalises, is thus "about finding answers to the question of what it is for an individual, and for a society of population of individuals, to be governed and governable" (Gordon, 1991, 36; see also Foucault, 1982, 782–784; 2009b, 184–185). This making thinkable and practicable takes place in both discursive and material practices that compile into techniques of government that, again, constitute particular dispositives. In this thesis, I am especially interested in the government of people within the dispositive of cyber/digital security that aims to produce digisavvy citizens capable of carrying out their role in the arrangements of comprehensive security in digital Lapland and participating in the emerging cyber-physical society in the first place.

The governing practices "presume some conception of an autonomous person capable of monitoring and regulating various aspects of their conduct" and try to "shape in some way who and what we are and should be" (Dean, 2008, 12). While digital literacy has been turned into a civic skill in Finland, the level of skills and awareness required from digisavvy citizens remains undefined at the general level and becomes decided on a case-by-case basis, for example, in courts (Päläs and Salminen, 2019; Salminen and Päläs, 2021). The state of affairs contributes to people's everyday insecurity by reducing predictability and legal safety, which, nonetheless, are improving again when more cases are processed in courts and other judicial bodies establishing a norm of some kind. However, some characteristics of digisavviness can be deducted from strategies and programmes introduced in sections 1.2, 1.3 and 1.4, as well as from the four articles of this thesis.

The preferred kind of citizens are harnessed with particular capacities and hence capable of behaving in a responsible manner in cyberspace. For instance, they have the economic capacity to acquire the necessary equipment, connections, and software and they know how to use ICT. They wish to connect and value the state of being connected over disconnectedness and use ICT to gain other values they perceive as desirable. They are happy to use digital services and market places, conform to self-service and service in other languages than their mother tongue, and learn to modify their behaviour to accommodate the restrictions in and the modifications of code. They wish to decide for themselves, but only within the limits set by commercial, non-profit and public service providers. They care for privacy and abstain from sharing sensitive information online, but they do not feel uncomfortable with 'necessary' information gathering about them and their activities or the opening of this data for commercial service development. Moreover, they recognise vulnerabilities embedded in technology and human behaviour and voluntarily increase their awareness and skills so that they can act in cyberspace in a safe manner. Yet, their skills stay within an acceptable range of variation so that neither the skills (see the threat depictions e.g. in Dunn Cavelty, 2014; Salminen, 2019; Päläs and Salminen, 2019) nor their absence (i.e. the lack of expertise mentioned in the aforementioned governance documents and programmes) constitute a threat to society. Above all, they do not resist digitalisation or refuse to adapt to it. Government through digitality then becomes feasible and economic for all parties involved.

In a similar vein, Paul Henman (2013, 1410) describes the governmental expectations towards citizens using Web 2.0[70] services: Citizens are imagined as active utilisers of open access public data and as active feedback givers. They are praised as "agents of their own destiny in making their own choices, actively using government data intelligently and co-constituting their usage of government services perhaps in junction with other citizens", while, in fact, governmental policies are merely managing people's experience of being relatively powerless citizen-consumers (Henman, 2013, 1412; also, Siltaoja et al., 2015, 450; Salminen, 2021, 170, 173–174).

3.1.2 Government of critical information flows

In addition to governing individuals, modern governmentality concerns groups of people, other 'things', and societies at large. In societal cybersecurity, there is an embedded duality. On the one hand, for the state and when titled as 'cybersecurity', the ICT problem is about safeguarding critical information and its flows, societal functions depending on these information flows, and the infrastructure which enables and supports these functions from (existential) threats. The logic follows that of national security to which a number of actors in different fields, and across the blurry line between public and private, are tied through collaborative arrangements. The approach hence concerns primarily the government of 'things', which role in the dispositive of security, according to Claudia Aradau (2010, 493–494), was greatly ignored still a decade ago. Instead, materiality should be considered as co-constitutive

[70] Web 2.0 refers to interactive internet. Instead of only consuming information people are able to generate, modify, upload and disseminate information regardless of the form of this information (text, audio, video). Thus, "Web 2.0 represents a web where information transfer is a two-way street". Techopedia (2020) Web 2.0. https://www.techopedia.com/definition/4922/web-20 [May 9, 2021].

of social order that is also agential. Like other objects and subjects, information and critical infrastructure emerge out of discursive and material practices and influence these practices. (Ibid., 494–496, 498.)

While Foucault did refer to both discursive and material practices as the basic elements of the dispositive of security, he did not much theorise on their relationship (Aradau, 2010, 497). However, according to Thomas Lemke (2015, 9), in discussing the government of people and other 'things' Foucault did not rely on a foundational sorting of active human subjects and passive material objects but employed a relational approach. 'Things' like people are then both objects on and towards which techniques of government are directed and subjects called upon to conduct themselves (ibid.; Foucault, 2009b, 42–43). The same can be applied to information, infrastructure or societal functions, which all condition human behaviour and life in digitalising societies (e.g. Aradau, 2010, 492–493). The digitalising everyday life in Lapland becomes increasingly modified by code, ICT design and architecture, networks, appliances and applications (see Salminen, 2021). It becomes a field of intervention embedded in "a multiplicity of individuals who [...] only exist biologically bound to the materiality within which they live" (Foucault, 2009b, 21). Agential power hence "originates in relations between humans and non-human entities" (Lemke, 2015, 10).

Furthermore, Foucault's formulation makes it possible to presume that human beings are governed as 'things' and hence ordered like other 'things' in order to achieve particular ends – no longer as 'souls' or 'bodies' (Lemke, 2015, 10–11; also, Macmillan, 2011, 6). The common nominator is, like the discussion on human rights and human security reveals later in this synthesis (3.1.4 and 3.1.5), that information, critical infrastructures, development, resilience, and rights are linked with sustaining a defined minimum level of law and order, welfare, and economic life (Aradau, 2010, 508).

In Finland, alongside the cooperative arrangements briefed in sections 1.3 and 1.4, the National Emergency Supply Agency (NESA), which is located in the administrative field of the Ministry of Economic Affairs and Employment and operates from a market perspective, aims to prepare for crises and disturbances and to safeguard the continuity of functions vital to society in all security situations (Aaltola et al., 2016, 13) – practically, through preserving circulation in economy and society. 'Information society' is one of the focus areas of NESA[71], which task is to coordinate the preparedness of a voluntary network of businesses and other organisations operating in Finland and evaluated as critical for the functioning of

[71] NESA has altogether seven focus areas: information society, energy supply, financial sector, logistics, industrial production, healthcare, and food supply. See the landing site of NESA at https://www.huoltovarmuuskeskus.fi/ [March 15, 2021]. These are broadly described in the Government Resolution on Security of Supply (1048/2018).

society – the so-called National Emergency Supply Organisation (NESO). Many of these businesses own, run and/or maintain critical infrastructures. (E.g. ibid., 16.) NESA cannot dictate what the stakeholders do, order them or compel them, but it can support their preparedness, for example, by providing information, connections and networks, and advice which support continuity management in these organisations (e.g. Lehto et al., 2017, 14–15, 48). It does this on the basis of the Act on Security of Supply[72] (1390/1992) and following the Government Resolution on Security of Supply (1048/2018). In exchange, the Government should be able to rely on the operability of business and hence the functionality of society in all security situations.

The history of security of supply in Finland dates back to the first decade after the independence – like the history of comprehensive security model as mentioned in section 1.3 – and the 'supply disaster' during the First World War that contributed to the outbreak of civil war in 1918 (NESA, n/da). Yet, the experiences during the Second World War, that is, the lack of groceries and material, were particularly important for the build-up of national security of supply (see Aaltola et al., 2016, 23). In the 2000's, the threat imagery directing the operations of NESO has changed from war and blockage of foreign trade to a multiplicity of disturbances that impede societal functions. At the same time, its operations have move from securing material supply to upholding of critical functions and services. (NESA, n/da.) In addition, NESA channels resources to the National Cyber Security Centre (NCSC-FI), owns Suomen Huoltovarmuusdata Ltd.[73], and supports Suomen Erillisverkot Ltd.[74] in its operations. NESO hence operates as the arm of modern governmentality that strives to preserve the right order of other 'things' supporting circulation, particularly in the economic field[75], in all circumstances.

NESA has organised consecutive programmes to improve national cybersecurity, especially in the business sector. Between 2011 and 2016, it collaborated with industry, NCSC-FI and VTT (a research institution owned by the state of Finland) in KYBER-TEO project portfolio aimed at improving information security in industry (NESA, 2021a, 8; see also Ahonen et al., 2017). Next, it ran Kyber2020

[72] Laki huoltovarmuuden turvaamisesta. My own translation.

[73] A data centre designed to ensure that the information systems critical for the security of supply and located in the centre are available and secured in all security situations. Suomen Huoltovarmuusdata Ltd. (n/d) Suomen Huoltovarmuusdata Oy. https://www.suomenhuoltovarmuusdata.fi/ [March 16, 2021].

[74] A state-owned provider of communication networks and services that supports the activities of authorities and remains operational in all security situations. Suomen Erillisverkot Ltd. (n/d) Erillisverkot. https://www.erillisverkot.fi/ [March 16, 2021].

[75] Military security of supply has its own structures under the Ministry of Defence and the Defence Forces, but it leans on the overall security of supply framework. Its goal is to ensure that resources necessary for the operational capability of the Defence Forces and the maintenance of the requisite technical systems are available during emergencies and disturbances comparable to emergencies (Ministry of Defence, 2016, 5).

programme from 2017 to 2020 to improve cybersecurity in businesses critical to security of supply in order to ensure the business continuity of these organisations during emergencies and disturbances in normal conditions. In this programme, it collaborated with NCSC-FI and the Digipool of NESO[76]. (NESA, 2021a, 5–6.) From 2021 onwards, NESA, in collaboration with NCSC-FI and the business sector, is running Digital security 2030 programme to "improve societal resilience against cyber disturbances". The programme is part of the implementation of the strategic objectives of NESA as well as of the national cybersecurity strategy. (NESA, 2021b, 4.)

Kyber2020 programme ran along two tracks: (1) improving cyber capabilities supporting the businesses critical to security of supply and (2) improving the preparedness of these businesses themselves. Its success hinged on the achievement of increased cooperation and mutual trust between authorities and businesses, resilience and a model for disturbance management, and the development of national cyber capabilities. (NESA, 2021a, 4–5.) The programme was divided into eight development areas, including inter alia national detection capabilities, cyber competence and cyber capabilities, trust in cyber risk management, cybersecurity in industries, resilience of media against information influence, and international cooperation (ibid., 6, 10). Cybersecurity metrics were developed as part of the programme, but it also became evident that "precise measuring is ambiguous given the dynamic operational environment prone to changes caused by a number of external factors" (ibid., 7, my own translation). In 2017 and 2019, the Digipool of NESO implemented maturity mappings of different industries (covering over 100 businesses in 12 industries[77]) and regular renewals of these mappings were perceived as a way to measure programme success. Unfortunately, the locations of mapped businesses are not disclosed for which reason providing a number or a share of them in Lapland is impossible. Pivotal lessons learned included that cooperation across industries and administrative branches improved information exchange and understanding of the criticality of communication. International cooperation in the field of digital security of supply was found to be challenging. (Ibid., 7–9.)

The ongoing Digital security 2030 programme, again, has four headings: (1) preparedness for cyber disturbances, (2) operational capability under stress, (3) cooperation between different actors in society and the business sector (networks), and (4) foresight for future phenomena. (NESA, 2021b, 4, 7–9.) Cybersecurity of

[76] NESO is organised into seven sectors which coincide with the aforementioned focus areas of NESA and sector specific pools that are responsible for operative preparedness in industries and businesses (NESA, n/db).

[77] See National Emergency Supply Agency (NESA) (2020) Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot. [Cybersecurity in different industries – pivotal findings of the mapping.] https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf [July 27, 2021].

the functions vital to society and foresight for the solutions to everyday cybersecurity stand at its heart. It strives to help businesses create sustainable cooperation structures and models, nationally viable trade, and networks in which businesses and authorities work together. (Ibid., 4.) The goal is that the vital functions withstand cyber disturbances so that (1) businesses know what to prepare for and how, resist cyberattacks, and recover from them quickly; (2) businesses and authorities have a common will, cooperation networks, and shared operational models to protect critical functions; and (3) international cooperation supplements national competence and capabilities to detect and defend against threats that are central to security of supply (ibid., 5). Integral to preparedness "cybersecurity know-how must be a solid and cross-cutting part of the competence of business management, expert groups, and other personnel". Development of this know-how can be facilitated, for example, by providing information and tools for evaluation. (Ibid., 7–8, my translation.)

3.1.3 Responsibilisation for cyber-physical wellbeing

On the other hand, when addressed in terms of 'digital security' and when discussed in the workshops in Enontekiö for article IV, securitisation of digitality comes closer to the logic of welfare state. The expectations towards and alternatives for action available to societal actors are then quite different from those in the national security framing. According to Mikael Nygård (2015, 138, 161), social policy is contemporarily justified mainly with its significance to economic growth and international competitiveness – exactly like societal digitalisation. In most conceptualisations, welfare embeds the idea that the state plays a pivotal role in the production of citizens' wellbeing. Yet, active state interference has been criticised for slowing down growth or constituting an obstacle to it. This contradiction has facilitated a reconceptualization emphasising the responsibility of communities and individuals for the production of their own wellbeing.

Changes in thinking have been followed by reforms in welfare systems: Equality has begun to indicate the equality of opportunities instead of outcomes and the state to invest primarily in social policies that support desired future trajectories. (Ibid., 139, 144, 153–154, 160; also, Pupavac, 2010, 692, 707.) The state has moved from 'rowing' to 'steering' by focusing on coordination instead of production and responsibilising social actors of all kinds (Abrahamsen and Williams, 2011, 60–61, 63–64). However, one cannot "assume a priori that the state is in a position of controlling and directing" these social actors, who also have their own interests and powers, even if it remains a central actor in the governing network (ibid., 69, 83–85; Krahmann, 2010, 73–74; Siltaoja et al., 2015, 446; regarding surveillance see also Huysmans, 2016, 75). For example, the state may adopt a hands-off policy and act merely as a customer instead of actively directing the development (Krahmann, 2010, 74).

Catlaw and Sandberg (2018, 6) make a similar argument by stating that "[i]n breaking from social-welfarist efforts to govern social processes through expertise, [modern] government emphasizes individual choice, autonomy, responsibility and the logic of the market". It strives to extend market-type relations to ever new areas. (In great detail, see Helén, 2016, 167–218.) Digitalisation of society, however, transforms modern governmentality and becomes characterised by (1) 'active citizenship' understood as continuous and effective generation of data; (2) Web 2.0 and wearable technologies as prime vehicles for data generation and circulation; (3) transformation of social government to 'connected government' following from reciprocal data generation and data sharing between citizens and administration (cf. articles II and IV about the lacking reciprocity in information sharing between citizens and administration); and (4) a persistent instrumentalization of data generated by people to ends that may be inconsistent with those of the data generators. (Catlaw and Sandberg, 2018, 6–7.)

Digitalisation facilitates welfare reforms and requires citizens to take a significant share of the responsibility for inter alia managing their appointments, keeping their records straight and reporting on their activities in digital service portals, as the extracts from pan-Arctic, regional, and national documents presented in sections 1.2 and 1.3 and article II testify, but the justifications given for digitalisation have not always convinced their audiences. As a consequence, unhappiness with the withdrawal of physical service points and their replacement with digital ones has been demonstrated (see articles II and IV). Most people still expect that the state provides basic security and protection to its citizens.

The level of (un)happiness related to digitalised services, however, varies. The article IV, for example, pinpoints local people's general satisfaction with digital health services (Salminen, 2021, 168). The development of these services began in the mid-1990's in Lapland (Lapland Hospital District, 2007, 4). The initial task was to create an overall system consisting of "videoconferencing technology, data security, an emergency medical service system, an electronic referral/feedback system, digital imaging, image transfer and archiving" and a related operational model for the use of municipal health centres and hospitals across the region (ibid., 4, 7). This included improvements in information infrastructure together with the municipalities. Adoption of the new system was supported by personnel training. The purpose was to bring specialised healthcare services closer to customers across Lapland. (Ibid., 4–5.)

The project dedicated to this stage of health services digitalisation had six goals: promotion of the wellbeing of Lapland residents, safeguarding of Lapland's health services, networked public healthcare, comprehensive services which take advantage of the new technology, increase in and utilisation of ICT competence, and creation of a compatible infrastructure (Lapland Hospital District, 2007, 6). It succeeded inter alia in turning videoconferencing into a familiar routine for both education and consultation, improving information security, and advancing the adoption of referral/feedback system and digital x-ray system (ibid., 10–19). As a result, heath services could be safeguarded to all residents, saving time and travel and reducing the related traffic risks were possible, and operations became more efficient, less costly and regionally more equal. However, challenges were observed with the quality of transmitted sound and image, network capacity, price of the equipment and connections, and competence (ibid., 21, 26–27).

The follow-up project extended service digitalisation to social services, widened its regional coverage to Länsi-Pohja healthcare district, and included digital services for both professionals and customers. In addition, it "coordinated the connection of the region to the national ePrescription service" and created an online training environment for and a handbook on data protection. (Lapland Hospital District et al., 2011, 4, 25–26.) "The main areas in regional development for promoting wellbeing and ensuring the availability and equality of basic services include[d] development of electronic services, promoting entrepreneurship and social innovation in the wellbeing sector, and increasing the appeal of working in wellbeing services and ensuring the availability of personnel" (ibid.). For doing so, "[t]he project aimed at developing procedures for internal and cross-organisational use and increasing citizens' participation in their care and services" (ibid., 5).

The project had four objectives: increasing citizen's participation; developing digital consultations and services between professionals, customer guidance, and cooperation among different operators; promoting the availability of customer data across organisations; and creating "opportunities for providing high-quality location-independent wellbeing services" (Lapland Hospital District et al., 2011, 6). As a result, the virtual social and healthcare centre, virtu.fi, was created for both professionals and customers to access online services safely and around the clock (ibid., 8). It included such services as online family and social service consultations, online health services, electronic forms, appointment booking online, text messaging services to facilitate queue management and data collection, and videoconferencing (ibid., 10–23). At the time, it was seen as an alternative service channel. If digital services were to "replace traditional services, it [had to] be ensured that special groups, such as the elderly and disabled [...], are supported so that they do not become marginalised and excluded" (ibid., 27). The vision was to develop virtu.fi further into "a central node for the provision of electronic social and healthcare services" (ibid.), which is currently on its way (see e.g. Lapland Hospital District et al., 2016).

In 'human security' or 'digital security' thinking, digitalisation is to enable, first, connectiveness and, second, continued provision of (public) services; even to bring some of these services closer to customers. Similarly, it entails the training and education of people to use digital interfaces, and ICT in general, in the preferred, 'safe' manner. People, again, request for a more humane cyberspace, which would be able to address the problems of loneliness, sickness, exclusion, and skill gaps in a 'safe' manner, that is, without one losing the ownership of his or her personal data or becoming victimised through crime or any sort of abuse (Salminen, 2021, 172–174). The language of fundamental/basic/human rights and 'digital rights' is often utilised in the latter framing. People request for a firmer state interference to root out the negative, harming, threatening, and unpleasant effects of interaction between people and people and 'things' in and in connection to cyberspace.

Of such negative effects, the question of inequality in access to cyberspace, information and digital services has also been recognised by the state of Finland. For example, internet accessibility programmes[78] and information society programmes[79] have been running since the mid-1990's and nation-wide broadband programmes since the early 2000's[80]. Finland treats internet access as a basic right and Government Report on Human Rights Policy (compiled by the Ministry of Foreign Affairs[81]) and National Action Plan on Fundamental and Human Rights 2020–2023 (compiled by the Ministry of Justice[82]), which both were in a renewal process at the time of writing, are now investigating the realisation of these rights in the context of digitalisation[83]. In practice, the national security discourse and

[78] Internet accessibility programmes have evolved into policies and regulation on the accessibility of digital services. Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies has received its national implementation through the Act on the Provision of Digital Services (306/2019). Its aims inter alia to advance everyone's ability to participate equally in the digitalised society, to provide minimum standards for the accessibility of digital public sector services, and to improve the quality of these services. The Regional State Administrative Agency of Southern Finland advices on and monitors the implementation of accessibility requirements throughout the country. See Aluehallintovirasto (n/d) Saavutettavuusvaatimukset. https://www.saavutettavuusvaatimukset.fi/ [March 24, 2022].

[79] Information society programmes have evolved into digitalisation programmes in the 21st century.

[80] The contemporary broadband programme, effective since early 2021, supports the build-up of fixed broadband connections which minimum speed for download is 300 Mbit/s and for upload 100 Mbit/s. Support can be applied for projects that are perceived as commercially non-profitable but justifiable, for example, because of permanent housing or holiday homes in the area. Laki kiinteän laajakaistan rakentamisen tuesta [Act on the Support for Fixed Broadband Construction] (1262/2020) and Valtioneuvoston asetus kunnan maksuosuudesta ja nopean laajakaistayhteyden vähimmäisnopeudesta laajakaistahankkeessa annetun valtioneuvoston asetuksen muuttamisesta [Government Decree Changing the Government Decree on the Municipality's Share of Payment and on the Minimum Speed of Fast Broadband in Broadband Projects]. (1148/2021) My own translations.

[81] See Government of Finland (2021) Valtioneuvoston ihmisoikeuspoliittinen selonteko. [Government Report on Human Rights Policy.] Valtioneuvoston julkaisuja 2021: 92. [Publications of the Finnish Government 2021: 92.] http://urn.fi/URN:ISBN:978-952-383-971-7 [March 23, 2022].

[82] See Government of Finland (2021) Valtioneuvoston perus- ja ihmisoikeustoimintaohjelma 2020–2023: Perus- ja ihmisoikeuksien toteutumisen seurannan kehittäminen. [National Action Plan on Fundamental and Human Rights 2020–2023: Developing the monitoring of fundamental and human rights.] Valtioneuvoston julkaisuja 2021: 59. [Publications of the Finnish Government 2021: 59.] http://urn.fi/URN:ISBN:978-952-383-630-3 [March 23, 2022].

[83] I attended these renewal processes as a member of the Human Rights Delegation, which is one of the three pillars of the Finnish National Human Rights Institution (NHRI). "The Delegation functions

the welfare state discourse entangle with one another (and with the other framings of cyber/digital security as mentioned in section 1.3) constituting a complicated assemblage of cyber-physical[84] security with the requisite attempts to govern it. Thus, unlike it is sometimes assumed, rights and security neither are two ends of a continuum nor require a balancing act but support one another (Salminen, 2019, 333; Salminen and Hossain, 2018, 115; also, Stevens and Vaughan-Williams, 2016, 4; cf. e.g. Hildebrandt, 2013; Taddeo, 2013; Stalla-Bourdillon, 2014).

3.1.4 Digitalising rights in the service of modern governmentality

Rights and security may still indicate differing relationships to freedom as, according to Foucault (2010, 9–13; 2009b, 91–95), rights and law set an extrinsic limitation to state government whereas the limitation set by security and economy is intrinsic to it. Furthermore, law can be understood either "as the expression of will" or "as the effect of a transcription that separates the sphere of intervention of public authorities from that of the individual's independence" (Foucault, 2010, 41). The former implies "a juridical conception of freedom: every individual originally has in his [or her] possession a certain freedom, a part of which [s]he will or will not cede" constituting his or her basic rights. In the latter, freedom is conceived "as the independence of the governed with regard to government". (Ibid., 41–42.) The two understandings may intertwine, but "are essentially heterogeneous and disparate" due to their different historical origins. "[W]here [...], how, and in what form [human] rights are claimed", then shows whether they are perceived as "the juridical question of rights [or as] a question of [the] assertion or claim of the independence of the governed vis-à-vis governmentality". (Ibid., 42.)

According to Louiza Odysseos (2010, 747–749, 755), human rights produce a particular kind of subjectivity amenable to self-government and supportive to modern forms of government aligning with the principles of economic efficiency. Governing along these lines requires from individuals an ability "to exercise freedom along structured paths and fields of action" (ibid., 751), that is, it calls for particular kinds of citizens – digisavvy citizens in this thesis. "Human rights as moral rights

as a cooperative body in the field of fundamental and human rights and helps to intensify information flow between the different actors". Human Rights Centre (n/d) Human Rights Delegation. https://www.humanrightscentre.fi/about-us/human-rights-delegation/ [March 16, 2021].

[84] 'Cyber-physical' is a concept relatively commonly used in cybersecurity and critical infrastructure research to refer to the interconnectedness of ICT devices and other components, so that "disruption of one component may have a negative, cascading effect on others" (Clark and Hakim, 2017, 1). Cybersecurity hence does not only entail threats associated with ICT but also physical threats to critical infrastructure (ibid.). As "critical infrastructure, such as transportation networks, electricity generation distribution networks, sophisticated communication systems, water and gas distribution networks, has increasingly relied on the Internet and networked connections for its operations", such systems have become frequently referred to as cyber-physical (ibid., 14). In this thesis, I use cyber-physicality to emphasise this interconnectedness of 'the physical' and 'the digital' spheres.

exist regardless of their legal and political acknowledgement by sovereign power" and prior to their codification into law, which entails that "they represent a claim against the state" demanding that it respects individual freedom and enshrines it in positive law (ibid., 755; see the first of Foucault's two perspectives to rights in a previous paragraph). However, these rights are "imbued with [...] the stricture to not 'govern too much'" and engender a self-governing subject contributing to modern governmentality (ibid.; also, Duffield, 2007, 7). The latter takes place through discursive practices in which individuals "become aware of their humanity and are sentimentally encouraged and educated to think of others as equal moral agents with innate freedoms and rights" (Odysseos, 2010, 756).

'Authoritative' agents like think tanks and supra-state organisations – or Ministries of Foreign Affairs and Justice as noted in the previous section – then work on these sentimental claims: analyse individuals as subjects of human rights and produce 'valid' knowledge on these claims to be considered in decision making. Furthermore, these agents provide knowledge on the basis of which communities "can reflect on how [they are] constituted by moral subjects and how the codification and enforcement of rights can assist" them (Odysseos, 2010, 759). Individuals and communities can then call upon "states and other international actors to recognise the moral worth and freedom of human beings and furthermore to legally acknowledge them" as right bearers, which constitutes a new legal subject (ibid., 761). Finally, an operational framework of rights needs to be established to create and regulate freedom, that is, the disposition of 'things' so that conditions of freedom are enhanced (ibid., 162).

"By creating, managing and expanding the legal framework of human rights", social discontent and the management of social ills is carried out through rights. It also places the responsibility for making claims of social discontent and for social change on the shoulders of individuals and provides a pathway through which this can be done. (Odysseos, 2010, 762–763; cf. Siltaoja et al., 2015, 453.) Thus, "the self-governing subject who exercises freedom by first demanding and then exercising its human rights" emerges, which enables the minimisation of state commitment to the cost-effective juridical endowment and protection of rights (Odysseos, 2010, 764, 766). As mentioned earlier (section 1.3.4), human right claims in digitality can contemporarily be two- or three-fold: claims for the acknowledgement of and respect for digital rights, the observed necessity of digitalised critical infrastructure protection as a precondition for the realisation of human rights, and, potentially, the acceptance of cybersecurity as a human right.

Odysseos's remarks coincide with my suggestion in section 2.6 that a human security approach does not interrogate modern governmentality far enough even if it questions the primacy of information and critical infrastructure or vital societal functions as the referent objects of cyber/digital security. Resorting to human and basic rights as a means of resisting the prevailing forms of societal digitalisation helps grinding some of the sharp edges of modern governmentality in everyday life.

Nonetheless, it does not lead to 'empowerment' but the manifestation of 'helpless victim' with rights that he or she cannot enact. (Odysseos, 2010, 765; also, Henman, 2013, 1412–1413.) In a similar manner, people who attended the workshops for the Fjeld Lapland case study in article IV pointed out that there are problems in the realisation of basic rights for those who do not have ICT or connections available or who do not actively and persistently claim their rights. However, possible counter-conducts were also envisioned, for example, the advancement of 'digifree' municipality and declining from participation in the digital society to any further extent than absolutely necessary. (Salminen, 2021, 171, 173.)

Basic and human rights are an integral part of human security, which therefore has been criticised in a similar manner for serving as a technique of modern governmentality. It has been argued that failure to achieve human security risks circulation that threatens global order and, thus, security (Duffield, 2007, 112). "[T]he permanent emergency of non-insured or self-reliant life and the surplus population it continuously throws off" threaten security globally and call for state intervention, as well as for the promotion of individuals' and communities' self-reliance, in areas perceived as underdeveloped and dangerous (ibid., 111, 121–124; also, Pupavac, 2010, 704, 707). While human security has been criticised for its vagueness as a concept, according to Duffield (2007, 114), this vagueness is what enables it work as a technique of governmentality reworking the relationship between development and security.

Yet, in order for human security to achieve its goals – empowered individuals and communities – it "should not operate as if its subjects are helpless and incapacitated" but facilitate local autonomy as self-government and self-determination organised around multiple understandings of security (Richmond, 2011, 44; also, Chandler and Reid, 2016). Achieving this end requires engagement with 'local-local' understandings of security, recognition of difference, as well as enablement of agency and autonomy (Richmond, 2011, 44) – similar to what, for example, Stern (2006), Prokkola (2018) and McCluskey (2019) have argued or what stands at the heart of so-called 'vernacular security studies'[85]. Moreover, as human security is a component

[85] Vaughan-Williams and Stevens (2016, 44) have analysed the difference between 'vernacular' and 'everyday' security approaches. The vernacular security approach has (1) "focused on how *particular* individuals and groups articulate their attitudes and understandings", (2) worked within such dichotomies as high/low or elite/everyday, (3) "align[ed] emancipatory and cosmopolitan potential with a 'bottom-up' perspective", (4) utilised widely methods like ethnography and focus groups that seek empirical engagement, and (5) "taken the linguistic constructions of citizens' accounts of threat and (in)security in their daily lives as [the] primary object of analysis" (ibid., 44; italics original). The everyday approach, which "roots in French cultural thought of the 1980s", (1) seeks "to trace *both* (in)securitizing moves and arenas in which these moves are negotiated and resisted by individuals and communities" and hence (2) refuses the high/low or elite/everyday dichotomies, (3) perceives "the everyday as a site for progressive politics while at the same time emphasizing that it is not a somehow passive or inert realm", and (4) tends to "privilege security practices negotiated in the context of citizenship more generally" (ibid., italics original).

of global governmentality seeking to "govern populations in the borderlands" (Doucet and Larrinaga, 2011, 129), it can be asked whether it helps preserving the kind of metaphorical images of the Arctic introduced at the beginning of this synthesis (1.1).

3.1.5 Conditioning of human behaviour

Unlike in this thesis, in which the prevailing images of the Arctic areas as developing regions within developed countries are invoked to critically engage with digitalisation as digital development, development is often theorised as activities taking place "over there" in order to improve security "over here" (see e.g. Duffield, 2007; 2010; Pupavac, 2010; Stern and Öjendal, 2010). The theoretical move of the ECoHuCy project to examine human security in the digitalising European High North, however, visualised how societal digitalisation generates contradictory trajectories within Finland as well. Digitalisation to an extent reinforces but also redraws the lines demarcating inclusion and exclusion in society and helps legitimate, for example, the withdrawal of physical welfare services from sparsely populated areas for their provision in the digital format is more cost-efficient (Salminen and Hossain, 2018; Salminen, 2019; 2021). The related infrastructural issues and questions of digital literacy resemble those commonly associated with places "over there".

For example, in accordance with Duffield (2010, 61), modern governmentality continues to see people living in so-called developing regions "as somehow incomplete of lacking the necessary requirement for a proper existence", which means that "life cannot be lived properly". Development, for instance through support and training, "premises to make incomplete life full and wholesome" by changing behaviour and attitudes, that is, by governing these others. Development hence operates as a technique of security and it does this through privileging local and adaptive self-reliance in the name of human security or resilience. (Ibid.) It is "concerned with how life itself is [...] supported and promoted, the conditions for community existence and the limits within which people are expected to live" (ibid., 64). Whereas in the developed countries in general, including Finland, life-related risks "are compensated for through a mixture of fiscal measures [including] private insurance, contributory social insurance and taxation", supporting "public and private welfare bureaucracies, benefit entitlements and social safety-nets" and intermeshing with a range of critical infrastructures (Duffield, 2010, 64; with regard to Finland, see e.g. Lehtonen and Liukko, 2010), this does not fully hold true in the digital sphere where individuals are to a great extent left to worry about their own security (e.g. Renaud et al., 2018; Päläs and Salminen, 2019; Salminen and Päläs, 2021). Even less so in Lapland, where information infrastructural concerns exist, even if welfare services are becoming digitalised to ever greater extent (Salminen and Hossain, 2018; Salminen, 2019; 2021).

Yet, at the same time people tell about changes decreasing self-sustaining lifestyles caused by digitalisation and increasing dependency on ICTs and connectivity (Salminen, 2021, 170–171, 173), which according to Duffield (2010, 65) are marks of developed societies. Thus, and while Duffield (2010, 61, 65) notes that development should not be conflated with state-led modernization but that the life-chance divide striates developed consumer societies as well, digitalisation and the requirements set for individuals by cyber/digital security are transforming subjectivities in Lapland. As modern governmentality is based on protection and improvement of "the essential processes of life associated with population, economy and society [...] in the name of people, rights and freedom" (Duffield, 2007, 4, 6), it establishes "[a] paradoxical position of life both as an autonomous domain and as an object and objective of [...] administration" (Dean, 2008, 99). As a result, the modes of existence and lines of change should be those acknowledged as safe and appropriate, instead of seeking "adaptive self-reliance as radical autonomy" (Duffield, 2010, 67–68, italics removed). For example, whereas the early hacker culture cherished pranking in such forms as website defacement or denial of service and skills testing in networks, much of this kind of behaviour has since been criminalised.

With regard to cyberspace, criminalisation of certain acts, expressions, and behaviours is the strongest form of censorship, which also has other, more subtle forms such as moderation of online discussion fora and blocking of social media users and content (see e.g. Salminen, 2021, 172). In the Criminal Code of Finland (39/1889), inter alia, offences against privacy, public peace and personal reputation (chapter 24); terrorist offences (chapter 34a); sex offences (chapter 20); violation of certain incorporeal rights (chapter 49); and criminal damage (chapter 35) distinguish the illicit from the permitted also in the digital sphere. Internationally, the Council of Europe Convention on Cybercrime (ETS No.185/2001) serves as the prime tool to bridle behaviour in and with regard to cyberspace. Article 9 of the convention concerns offences related to child pornography as content-related offences and Article 10 deals with offences related to infringements of copyright and related rights. Article 15, again, provides safeguards for the adequate protection of human rights and liberties incorporating the principle of proportionality. However, governing human behaviour through criminalisation succeeds only up to a point. Constantly evolving cybercrime continues to be the dominating form of malicious activity in cyberspace (e.g. IBM, 2022, 29) and, for example, in Finland it has been acknowledged that "majority of cybercrime is never reported to the Police and reported cybercrimes often remain unsolved or become only partially solved" (Ministry of the Interior, 2017, 32, my own translation; also, Sannikka and Nykänen, 2021). Thus, cybercrime remains beneficial.

According to Lawrence Lessig (1999), governing human behaviour directly in cyberspace is difficult, but it can be conducted indirectly, that is, through regulating the architecture built by coding and, thus, through regulating the code. The architecture can be changed by changing the code and hence problems can be both programmed in and away from it. Commercialisation of cyberspace was a significant change and made it regulable, for "[i]f the code of cyberspace is owned [...], it can be controlled". (ibid., 7, 13; also, Greenstein, 2015; Mueller, 2017, 15.) By regulability Lessig (1999, 19) refers to "the capacity of a government to regulate behavior within its proper reach", which aligns with modern governmentality. Commercialisation coded security and security concerns into the architecture, and to replace openness that had characterised it before, because safe and secure commerce was equalled with predictability and trustworthiness of online transactions (ibid., 39–42). The government could help commerce through regulation, that is, by facilitating it and advancing its interests with regard to cyberspace, but also the market could regulate human behaviour on behalf of the government or, at least, provide information about it. "Regulability then depends in part on identification", which calls for government based on individualisation (ibid., 48–60; see e.g. Foucault 2009b, 60–61, 66, 128–129, 184–185; Helén, 2016, 71–83). The desire of the Finnish state to foster more trustworthy identification in cyberspace was already mentioned in section 1.4.3.

Attribution is an often-discussed form of individualisation in cyberspace. It is a retrospective activity to establish 'who did it' with regard to cyber attacks[86] and/or cyber incidents[87]. It is not a straightforward process, for which reason, for instance, Rid and Buchanan (2015, 7) discuss attribution at three levels: technical/tactical, operational and strategic. At the technical/tactical level, attribution is about "understanding the incident primarily in its technical aspects, the *how*" of the attack. At the operational level, it is about "understanding the attack's high-level architecture and the attacker's profile[,] the *what*". Finally, strategically it is about "understanding who is responsible for the attack, assessing the attack's rationale, significance, [and] appropriate response[,] the *who* and *why*." In addition, "communicating the outcome of a [...] forensic investigation is part and parcel of the attribution process", a goal on its own. (Ibid., 10, italics original.) It has been argued that the weighing in the attribution process is gradually moving from establishing who did it to "finding the adequate policy response, including whether to publicly attribute" (Egloff, 2020, 1). However, attribution at the different levels sets varying requirements for inter alia the certainty of who did it and what can be done about it, for which reason attribution carried out, for example, by political decision makers, law enforcement, investigative media, and cybersecurity companies is not performed in the same way.

[86] Cyber attack is indirectly defined in the Vocabulary of Cyber Security (2018, 30) as an activity aiming to damage information network, information system, equipment, or data or to use them without an authorisation.

[87] Cyber incident is defined in the Vocabulary of Cyber Security (2018, 25) as a realised cyber threat that hinders the operation of an organisation or a system.

Lessig's aforementioned notion about the programmability of cyberspace, which in principle is true but limited by, for example, the so-called legacy systems and gaps in interoperability, is somewhat simplistic. The technical core task of cybersecurity industry and in-house ICT capabilities in all organisations has been and is to code problems away, but the continuous increase in the importance of cybersecurity reveals how difficult task it is. Thus, even if commerce may be "constructing an architecture that perfects control" (Lessig 1999, 6), Lessig could still state around 20 years ago that "governments have not been good at encouraging an architecture of identification" (ibid, 51). The notion may hold true today as well, for the resort to disciplining techniques in the production of societal cybersecurity may bespeak of lacking visibility to cyberspace and lacking information series. This visibility and an abundance of information is held by the multinational ICT corporations instead. Their stand on governmental requests, again, varies greatly from corporation to corporation and from government to government as discussion in section 3.2.5 brings up. In addition, these corporations also struggle with the problems of imperfect control, that is, security.

3.1.6 Privatisation of security

Commercialisation of cyberspace coincides with privatisation of security, for which reason the last part of this section discusses the latter trajectory. In Finland, private security services have increased significantly since the 1980's[88] due to changes in population structure, technological development, security authorities' diminishing resources, transformation of crime, and international legislation (Ministry of Justice, n/d). Some security tasks, powers and responsibilities have been moved from state authorities to businesses and the voluntary sector. This move has followed a global trend of questioning the efficiency and accountability of centralised security government (Krahmann, 2010, 72). The market has instead been perceived "as the ideal mechanism for satisfying citizens' needs, including security", which would in return lead to reduced citizens' obligations vis-á-vis the state (ibid., 73).

Yet, the privatisation of Finnish security embeds an interesting duality: Whereas the appearance of private security guards to public spaces generated a vivid public discussion that pops up every now and then, the fact that the prime security providers in cyberspace are cybersecurity companies and volunteers or third sector

[88] In the early 1980's, Vartioimisliikelaki [Security Company Act] (237/1983) renewed then in force legislation from the 1940's concerning security business. Legislative change in this millennium have further advanced the development of private security business e.g. Laki yksityisistä turvallisuuspalveluista [Act on Private Security Services] (282/2002), Järjestyslaki [Public Order Act] (612/2003) and Laki yksityisistä turvallisuuspalveluista [Act on Private Security Services] (1085/2015). My own translations. The coming into force of these laws have generated vivid public discussion on the authorisation and powers of private guards and security guards, but similar discussion has never taken place with regard to cybersecurity companies.

organisations has never raised considerable public concern. Explanations for this can be speculated: Maybe commercialisation of cyberspace took place before ICT invaded societal structures to the extent that vulnerabilities in technology and its use could constitute a grave societal concern? Maybe security threats were not on top of the mind of people making decisions about digitalisation but the efficiency gains that ICT produce? Therefore, maybe cybersecurity companies have managed to develop solutions, services and expertise that the state does not have 'in-house' thus making it perceived as 'natural' that cybersecurity is above all an acquired service and everyone's personal responsibility?

In Finland, security authorities are responsible only for their own equipment, networks, data and services, as well as investigating cybercrime, (counter) intelligence operations, and countering cyber operations. The Ministry of Finance and DVV coordinate and develop digital security within the public administration and provide, for example, training and information to all stakeholders in society as discussed in section 1.4.3. The National Emergency Supply Association coordinates and develops preparedness and resilience with businesses as presented in section 3.1.2. It has also published a number of cybersecurity guides that can be utilised by individuals and communities alike. The National Cyber Security Centre provides plenty information to the wider public, but its main task is to provide situational picture and to advice and support private and public sector organisations in case of a significant cyber security event. The information provided includes, inter alia, cybersecurity guides and advice to different reference groups (including a guide and videos to private persons) as well as topical news and cybersecurity alerts (including vulnerability alerts). It also entails a monthly cyber weather bulletin on the developments in the segments of information breaches and leaks, scams and phishing, malware and vulnerabilities, automation, operability of networks, digital espionage, evolvement of information security industry, and everyday cybersecurity[89]. Cyber/digital security is still largely a private endeavour in which the state plays a restricted role.

"[P]rivate security has become a pervasive part of everyday life" across the globe engaging in "the seemingly mundane protection of life and assets" (Abrahamsen and Williams, 2011, 1). Therefore, private guards and security guards, cybersecurity companies, as well as healthcare companies, care service providers, and so forth go almost unnoticed in the everyday life[90]. Yet they are an indicator of the contemporary

[89] For the format of the cyber weather bulletin see https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa [March 27, 2022].

[90] Such actors often become visible only when something goes wrong, for example, when the care of elderly people is neglected by a care service provider as in the case of Esperi Care (e.g. Niemistö, Elina and STT (2019) "Valvira keskeytti Esperi Caren hoivakodin toiminnan Kristiinankaupungissa – yhden asiakkaan epäillään kuolleen hoitovirheen takia" [Valvira froze the operation of Esperi Care nursing home in Kristiinankaupunki – it is suspected that a customer died because of malpractice], YLE News,

social order embedded in and inseparable from modern governmentality (ibid., 3, 23). According to Abrahamsen and Williams (2011, 3, 5, 9), changes inside the state are linked to the emergence of global security assemblages, that is, "new security structures and practices that are simultaneously public and private, global and local" and reconfiguring state power. These assemblages encompass transformations in both developed and developing regions, their interconnections, and the vast and immensely varied private security sector that has developed as a result (ibid., 12–14, 56). Moreover, "the privatization of security frequently occurs at the instigation of the state, as part of policies of outsourcing, cost recovery and efficiency" instead of standing in opposition to state authority (ibid., 28). Public-private partnerships in the field of security are indeed relatively common (ibid., 30).

Thus, maybe the booming market of commercial cybersecurity is not so much a result of state neglect as of modern governmentality directing the market through the principle of minimum interference? The recent coupling of human and basic rights with the government of the societal impacts of overarching digitalisation would then be about the establishment of the minimum standard of equality and participation in digitality like, for example, Duffield (2007) and Odysseos (2010) have argued. Yet private security initiatives also emerge when the state is perceived to have a reduced capacity to provide protection. The state tends to tolerate and only infrequently opposes such initiatives even in these situations. (Abrahamsen and Williams, 2011, 69, 81.) In any case, privatisation of security is best understood as "a reconfiguration of both public and private power rather than a simple privatization of previously public functions" and it affects the social, political and economic alike (ibid., 56–57, 59, 80–81) – in and with regard to cyberspace as well. The relative importance of businesses and individuals in the production of security increases.

In the next section, I will address three forms of power that are effective in the production of cyber/digital security: security, law and discipline. Additional

January 25, 2019, https://yle.fi/uutiset/3-10615005; Roslund, Riku and Mäntymaa, Jaakko (2019) "Ylen laaja selvitys paljastaa Esperi Caren hoivakotien karuja käytäntöjä: sängystä pudonneet jätetty lattialle, hoivakoti välillä ilman hoitajaa" [A wide investigation carried out by YLE reveals the harsh practices of Esperi Care nursing homes: customers fallen from their beds left lying on the floor, nursing home occasionally without a nurse], YLE News, January 28, 2019, https://yle.fi/uutiset/3-10617945) or when sensitive information about patients' appointments with psychologists is leaked to internet as in the case of Vastaamo (e.g. Halminen, Laura (2020) "Vastaamon tietomurto on sähköisen maailman suuronnettomuustilanne, mutta missä ovat jumalanpalvelukset ja kriisipäivystys?" [Vastaamo data breach is a disaster in the electronic world, but where are the church services and crisis emergency services?], Helsingin Sanomat, October 24, 2020, https://www.hs.fi/kotimaa/art-2000006698776.html; YLE (2020) "Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa" [YLE followed the Vastaamo data breach: This is how the blackmailer appeared on a forum in the Tor network, the Police is requesting consideration in the publication of details], YLE News, October 25, 2020 [last updated on November 2, 2020], https://yle.fi/uutiset/3-11612399. My own translations.

emphasis is given to surveillance and transparency as often discussed techniques of security that were also touched upon in the articles of this thesis.

3.2 Secured digitality, law and discipline in the Arctic

3.2.1 Statistical production of cyber/digital vulnerabilities, risks and normalities

"For [the established] order actually to guarantee [...] security one has to appeal [...] to a whole series of techniques for the surveillance of individuals, the diagnosis of what they are, the classification of their mental structure, of their specific pathology, and so on" (Foucault, 2009b, 8) – just like advocated in articles I and II. Furthermore, security as a dispositive "inserts the phenomenon in question [...] within a series of probable events" (ibid., 6) and makes "the old armatures of law and discipline function in addition to the specific mechanisms of security" (Foucault, 2009b, 10). Instead of replacing law and discipline, security makes them serve its purposes in a transitioned form. Law, discipline, and security hence do not represent a chronological development towards increasing rationality, but "are always co-present as complex structures, where, in each case, one of the elements exercises dominance over the others" (Wallenstein, 2013, 18).

The government through digitality becomes possible only when people have been connected – to internet, one another, databases, institutions, and so forth. Connectivity generates a culture of global connectivity which embeds digital information collection and its assortment (van Dijck, 2013, 11–14). Gathering information about human behaviour on digital platforms, in corporate ICT architecture and networks, on internet in general, and through devices (information such as location, proximity to sensors and other devices, vital signs, and the personal ways of using devices), again, is a precondition to the kind of statistical knowledge on which cyber/digital security operates (see Foucault 2009b, 8, 66). Thus, the regional, national, and pan-Arctic efforts to improve connectivity are also efforts to extend effective information gathering and control. Sufficient data and statistical instruments then ensure that thinking about cyber/digital security is possible "in terms of the calculus of probabilities" (Foucault, 2009b, 58–59). People's behaviour in cyberspace becomes thus integrated in the mechanisms of security. A person who may have lived 'under the radar' in the rural Arctic, becomes visible when he or she is connected and begins to leave traces by using digital devices and services. This digital existence becomes forced when alternative ways of running errands have been cut down and citizen obligations still require, for example, paying taxes. Opting out of digitality is no longer an option (Kilpeläinen 2016, 65; with regard to the social pressure to be present in social media, Hokkanen et al., 2021, 80).

Digitality thus constructs a form of population registry, whether national or commercial. From this registry, behavioural trends can be extracted via statistical means, which are developing quickly: becoming automated and faster, more sophisticated, and able to deal with ever bigger data masses (so called big data and big data analytics). (See Foucault, 1998, 25, 40–41; Foucault, 1991, 148–149.) With the help of different forms of artificial intelligence, these trends can be turned into behavioural predictions. The aim is to deal better with uncertainty or market and sell commodities more efficiently; extract trends from data that can be amplified or intervened depending on whether they are perceived as positive or as negative. Through an analysis of the distribution of cases – in cyber/digital security the cases of inter alia cyber attacks, information breaches, intrusion attempts or successful intrusions, information leaks, phishing attempts, scamming attempts or successful scams, and human mistakes – the risk for each can be identified. As "risks are not the same for all individuals", groups, communities, companies, organisations, branches of government, business sectors, administrative units, states, and so forth, this differentiation of risks reveals areas of higher or lower risk. Thus, what is dangerous can be identified for all of the aforementioned subjectivities. (Foucault, 2009b, 60–61.) For instance, a national crime victim study in Finland identified the youth as particularly vulnerable to cybercrime (Danielsson and Näsi, 2019, 26–27). The supporting and intervening (non)reactions can then be calculated as comparable cost calculations and targeted to tame the dangerous (Foucault, 2009b, 6, 66).

Moreover, the aim is to establish averages that are "considered as optimal for a given social functioning" and ranges that define "socially and economically acceptable limits" within which an activity must be kept. (Foucault, 2009b, 5–6.) Extracted from data "one will [thus] have the normal, overall curve, and different curves considered to be normal" and "try to reduce the most unfavorable, deviant normalities in relation to the normal, general curve, to bring them in line with this normal, general curve" (ibid., 62). This operation is normalisation. The dispositive of security hence is a device of normalisation, that is, of disposition, arrangement and movement, and not an instrument of normativity, that is, of representation and domination (Panagia, 2019, 722; see also Foucault, 1998, 89).

The processes of societal normalisation have transformed when ICT have intruded further into societal structures and when cyberspace has transformed from the free space of technology enthusiasts to which governments were unwelcome (Barlow, 1996; Lanier, 2010, 14) to a space characterised by governments' attempts to align internet with their jurisdictional boundaries (Mueller, 2017, 3, 71–84). As pointed out in section 3.1.5, cyberspace became governable through its commercialisation, which created room for the indirect regulation of people's behaviour (Lessig, 1999). Internet as "[a] system that is engineered to make communications and information accessible and interoperable across the board enables commercial exchanges of digital goods and information services among any two connected parties [...] [and as such] implies pure free trade [...] unprotected by customs checkpoints or tariffs" (Mueller, 2017, 10). However, technologies that "monitor, limit, intermediate, condition, or block [i]nternet traffic" are widely embedded in the infrastructure and the rising global awareness about the opportunities that internet provides for intelligence gathering has fed into desires to further modify the global flows of information (ibid., 13, 16).

Milton Mueller (2017, 73–84) provides three broad categories of techniques used in such modification attempts, namely, national securitisation, territorialisation of information flows, and efforts to structure control of critical internet resources along national lines. The first category refers to the framing of cybersecurity as a problem of national security, the second to filtering or blocking of access to external sources, data localisation, geo-blocking[91], and attempts to receive international recognition of restrictions on cross-border information flows (ibid., 74, 77). The third category then entails "efforts to find ways to partition the global domain name and IP addressing system along national lines" in order to increase national control (ibid., 82). Yet, such attempts tend to globalise procedures instead of localising them (ibid., 85). Furthermore, "[a]lingment is both irresistible for states to attempt and impossible for states fully to achieve", because of an inherent clash between territorial alignment and economic efficiencies and capabilities of ICT (ibid., 104). The categories of techniques that Mueller discusses can be described as security practices primarily aimed at weakening the undesired kind of circulation.

As mentioned, effective government depends on statistical information on the normal curves along which the population divides. These curves enable pinpointing deviations to which corrective techniques can then be applied – if deemed worthwhile. One of the reasons for cyber/digital security problems is the lack of statistical information and knowledge about people's behaviour in and with regard to cyberspace. "The finitude of the state's power to act is an immediate consequence of the limitation of its power to know" (Gordon, 1991, 16). Even if the state is not interested in the constant surveillance of individuals in all what they do but in the government of population through normalisation (Foucault 2009b, 66), the spottiness of behavioural data poses a problem. Lack of knowledge about what is 'natural' in the processes of population in and with regard to cyberspace makes it difficult to manage these processes (ibid., 70). The presumption of neutrality of technology present in mainstream cybersecurity understanding (cf. Salminen and Hossain, 2018, 111), leads to the ignorance of variations within population and hence tends to hide what is 'natural'. People do not simply obey or refuse to obey, for instance, given cybersecurity guidance, but act unpredictably somewhere in between the perfect citizen or employee and the completely ignorant one. Their behaviour also varies in different situations and transforms over time. (See Foucault, 2009b, 70–72.)

[91] "Geo-blocking restricts access to Internet content based upon the user's geographical location" (Mueller, 2017, 80).

An additional challenge in the Arctic is the scarcity of regional data about people's online behaviour. It may also be in the interests of local people not to have regionally categorised data for such data could stigmatise or help upholding, for example, cultural or ethnic stereotypes. Alternatively, it could make people relatively easily identifiable in sparsely populated areas. (Olsén-Ljetoff and Hokkanen, 2020; Salminen, 2021.)

In the language of national cybersecurity, the problem then is that of 'situational awareness'. "Cyber security management and disturbance management require that the Government and different actors have a reliable, real-time cyber security situation picture" (Security Committee, 2013, 4) "based on efficient and wide-ranging information-collection, an analysis and gathering system [to produce information on vulnerabilities, disturbances and their effects, and] national and international cooperation in preparedness" (ibid., 5; also 7, 23). In national security framing, the state and its security organisations are primarily interested in other states and organisations and the behaviour of particular individuals, whereas, for instance, everyone's vital signs are in the interest of healthcare professionals working in the service of welfare state and with different techniques of security.

Currently, much of behavioural research focuses on studying and explaining human behaviour in the digital environment, including its security aspects (e.g. Aiken, 2016; Anwar at al., 2017; Brase et al., 2017; Li et al., 2019; Alshaikh, 2020; Chowdhury et al., 2020; Kennison and Chan-Tin, 2020; Gilliam and Foster, 2020), to fill the aforementioned gap in knowledge. However, simulations are never quite the same as contingencies encountered and the networks in which people's behaviour can be observed are to a great extent owned and monitored by private corporations, which makes the compilation of information complicated and often illegal. In the name of national security, NCSC-FI has a certain (secret) level of visibility to the networks located within the territorial borders of Finland through cooperative arrangements, but this does not lead to comprehensive statistical information collection (Lehto et al., 2017; Lehto et al., 2018). Such information collection may instead have been carried out by ICT companies. Therefore, the national situation picture in cyberspace is only gradually evolving.

3.2.2 Law and discipline in the production of cyber/digital security

Because of the imperfect digital situational picture, the Finnish state has had to resort to law and discipline in the production of cyber/digital security. Here normalisation should not be confused with law or normation, even if it entangles with them. According to Foucault (2009b, 56), "the relationship of the law to the norm" indicates that there is "a normativity intrinsic to any legal imperative", but this relationship is different from "procedures, processes, and techniques of normalization". The role and function of a law is to codify a norm instead of establishing acceptable variance (ibid.). Normation, again, relates to discipline. Discipline analyses and breaks down entities, that is, individualises so that the components become visible and can be modified. Furthermore, it "classifies the components thus identified", "establishes optimal sequences and co-ordinations", "fixes the processes of progressive training [...] and permanent control", and, finally, "establishes the division between those considered unsuitable or incapable and the others". (Ibid., 56–57; with regard to cyberspace, see e.g. Barnard-Wills and Wells, 2012, 229.)

Normation thus establishes an optimal model in terms of a certain result and tries "to get people, movements, and actions to conform to this model"; what is perceived as normal can conform to this model while what cannot is considered abnormal (Foucault, 2009b, 57). Law and discipline, however, have been modified to function as mechanisms of security, also with regard to cybersecurity. While the improvement of individuals digital literacy, which becomes highlighted in all digitalisation and cyber/digital security framings, is the main technology of normalisation in modern governmentality, it is supported by other technologies, for example, by the development of legislation on cybercrime and consumer protection, as well as surveillance diffused into the society.

Two examples are in place to elaborate the difference between law and discipline in the production of cyber/digital security. Päläs and Salminen (2019) examines how effective consumer protection law, which can provide guidance on the perceived adequate level of digital literacy as a civic skill, operates around the concept of an average consumer. Law presumes an abstract average consumer and establishes it as a norm against which estimations of what one knew or what one should have known in these specific circumstances are conducted. What one knew or what one should have known provide the basic level of digital literacy that can be expected of one and all in similar circumstances and, thus, liability assessment can be carried out on a case-by-case basis referring to this basic skill level. According to Schebesta and Purnhagen (2019, 18), "practices and requirements relating to [consumer] information can be framed in two ways: (i) as 'objective' information requirements [for instance, its accuracy, completeness, and sufficiency]; and (ii) as 'subjective' requirements that relate to the understanding and processing of information by the consumer". The concept of an average consumer then takes effect in the evaluation of the (un)fairness of the commercial practice and the influence on the consumer's transactional decision (ibid., 21).

In addition to utilising the average consumer concept as an evaluative principle in a specific case, it can be used in a general way as a characterisation of a practice (Schebesta and Purnhagen, 2019, 25–26). Consumer protection law thus establishes a norm of skilled digital consumer that is capable of making free and informed decisions. This norm, and the responsibilisation of individuals carried out on its basis, is supported, for example, by different behavioural expectations (information consideration obligations, retention obligations) established in particular (legal) rules and legal practice (Päläs and Salminen, 2019). When this norm is inserted in the wider digital literacy as a civic skill discussion, a faint image of what is citizens' good enough digital literary begins to emerge.

Disciplinary normation, again, can take place through information collection and surveillance carried out in Finland by the Police, the Finnish Security and Intelligence Service (SUPO), and the Defence Forces and supported by other law enforcement agencies. The legal frameworks for the operations and supervision of both civilian and military intelligence were renewed in long legislative processes which end results were passed into law in 2019[92]. The legislative processes began in 2013, when the Ministerial Committee on Foreign and Security Policy and the President of the Republic had a joint meeting to discuss the then-new Finland's Cyber Security Strategy (Security Committee, 2013) and noted that the country lacked intelligence legislation. Enacting such legislation was seen as necessary for the implementation of the strategy. The Government began preparing both laws in 2015 and gave government bills to the Parliament in 2018. (The Parliament of Finland, 2019.)

A new Parliamentary Committee, the Intelligence Oversight Committee, and a new position of Intelligence Ombudsman, to operate in connection to the Office of the Data Protection Ombudsman, were established to oversee intelligence collection and began their work in 2019 (The Parliament of Finland, 2019). The Intelligence Oversight Committee "oversees the proper implementation and appropriateness of intelligence operations, monitors and evaluates [their] focus areas [...], monitors and promotes the effective exercise of fundamental and human rights [...], prepares reports by the Intelligence [...] Ombudsman and processes [its] supervisory findings" (The Parliament of Finland, n/d). The Intelligence Ombudsman similarly supervises the legality of intelligence activities, supervises the realisation of basic and human rights, promotes "the realisation of legal protection and the related best practices in intelligence activities", as well as monitors and assesses the functionality of legislation within the Ombudsman's purview and makes development proposals (The Intelligence Ombudsman, n/d).

Very little information about the operations of intelligence collectors and their supervisors is publicly available, even if, for example, SUPO and the Intelligence Ombudsman publish annual reports and the reports and statements of the Parliamentary Committee are selectively available on the committee's website. The Parliamentary Ombudsman also publishes in its annual reports information about both intelligence and secret data acquisition, for example, lawful interception and surveillance carried out by the Police and the Customs. Intelligence and surveillance are not the same thing, but overlap occasionally. These legislative processes hence

[92] In particular, Laki tietoliikennetiedustelusta siviilitiedustelussa [Civilian Intelligence Act] (582/2019), Laki sotilastiedustelusta [Military Intelligence Act] (590/2019) and Laki tiedustelutoiminnan valvonnasta [Act on Intelligence Supervision] (121/2019).

awoke a vivid discussion, for example, on the powers of intelligence agencies and whether Finland was moving from targeted surveillance towards mass surveillance. In addition, the role of courts, on the one hand, in authorising surveillance and, on the other hand, in ensuring that citizens' basic rights are respected became debated. (E.g. Nortio, 2019; Mikkonen, 2017; Saraste, 2017.)

Foucault discussed surveillance as a technique of discipline widely, but I will point out only some of his notions relevant for the production of digisavvy citizens in Finnish Lapland. Surveillance is also one the most examined security techniques in cyberspace, but my interest lies in its everydayness. The aim of disciplinary techniques is to produce effective workforce for the economy. This improvement of the utility and efficiency of the population takes place by working on the individual, his or her body and mind. It concentrates on constant "controlling and correcting the operations of the body" in order to make it docile through subjectivation, use, transformation, and improvement. (Foucault, 1991, 136–138.) Disciplinary techniques hence turn the body into 'capacities', which it tries to increase, while simultaneously subjecting the body to control (ibid., 138).

The disciplinary techniques modified in the dispositive of cyber/digital security and striving to produce digisavvy citizens do not so much coerce but try to persuade individuals to behave in the desired kind of manner, for example, to follow the given guidance in order to protect themselves and others in cyberspace. Security discourses are pivotal in achieving this. Their powerfulness derives from their ability to "inform how people believe they need to seek safety and avoid harm, as well as the choices that they make based on those beliefs" (Stern, 2006, 188). Coercion does take place, for example, when other than digital forms of service provision are no longer available and information management at work is carried out solely via digital means. At the same time, the wearable technologies that enable constant self-observation help self-disciplining often resorted to in order to meet, for instance, the doctor's orders or appearance pressures. Network visibility, which is generally increased in the name of cybersecurity, again, helps employers to oversee their employees even when they are working from distance. ICT have hence made discipline and surveillance more subtle but intrusive, sophisticated, and even self-induced. Yet, they remain to be "adopted in response to particular needs" (Foucault, 1991, 138).

According to Foucault (1991, 141–169), discipline works on the distribution of individuals in space and on the composition of forces, controls people's activities, and organises geneses, which refers to the organisation and hence capitalisation of (the use of) time. Such disciplinary techniques are clearly present in intra-organisational cybersecurity arrangements. For example, prohibition of external access and internal compartmentalisation serve as ways to control the dissemination of information within an organisation as well as to prevent its leakage outside (Foucault, 1991, 142–145). Cybersecurity management is organised and the requisite responsibilities are allocated on the basis of job titles and descriptions and compiled into organisation charts (ibid., 145–147, 166). Time stamps and series are important for having visibility over and controlling changes in the network, as well as establishing liabilities and collecting possible forensic evidence for further analysis. Time synchronisation, again, is a precondition for the functioning of a network. (Ibid., 149–152, 164–165.) Employer organised training takes place regularly so that all employees use their equipment and software efficiently, fil their (security) roles, and know how to act safely in and with regard to cyberspace. The employer also times and supervises both training attendance and activities of employees. (Ibid., 152–164.) It is the people as employees who are responsibilised for the organisation meeting its cybersecurity goals; it is the people who make the organisation cybersecure (see Siltaoja at al., 2015, 445).

3.2.3 Surveillance in a digitalised society

The exercise of discipline presupposes observation, that is, "the techniques that make it possible to see induce effects of power" and the means to make those on whom coercion is applied clearly visible (Foucault, 1991, 171). Modern governmentality hence ties surveillance and transparency tightly together in the dispositive of cyber/digital security. In its perfect mode "all power would be exercised solely through exact observation" (ibid.). This architecture of power "would operate to transform individuals"; in its most efficient form only by making them wary of such observation which executors nevertheless remain invisible to the observed (ibid., 172, 187, 201). However, according to Barnard-Wills and Wells (2012, 231), who discuss surveillance in the context of crime prevention, "the often invoked panoptic diagram" is not of the greatest importance in making sense of contemporary surveillance. Instead, the everyday quality of surveillance becomes visible in "a set of diverse practices and situations in which human agency combines with technology" and "leads to a multiplicity of practices and techniques of [...] control" (ibid., 227, 232).

Jef Huysmans (2016, 75) also points out that surveillance is rather extitutionally than panoptically organised. "Significant practices of surveillance do [...] not work in [...] bounded institutional spaces and their hierarchical organisation of visibility; or, at least, they cannot be fully understood as institutionally bound" (ibid., 76). ICT and social media distributed surveillance across the population so that surveillance became decentralised and diffuse thus allowing multidirectional connections and information flows and also disconnecting it from discipline to an extent. Extitution, then, "refers to relations and practices of governance in various areas of life [...] that are dispersing beyond the physical and spatial confines of the institutions that exercise them", for example, remote work and privatisation of security. (Ibid., 76–78; also, Barnard-Wills and Wells, 2012, 234–235.) The exercise of power does not primarily take place within the physical boundaries of traditional institutions but is fractured and dispersed, which also transforms these institutions. Institutions remain important, but "the physically bounded space is becoming less important for their operation". (Huysmans, 2016, 78; with regard to healthcare and social security, see Salminen, 2019; 2021).

"In situations of extitutional surveillance, the power of monitoring, registering, constructing, and circulating data and rendering subjects as data is highly distributed and mobile" (Huysmans, 2016, 78). Furthermore, it is embedded in everyday practices and becomes established by circulations instead of institutional confinement. "The extraction of personal data for governing conduct" is carried out in an omnipresent manner and is difficult to avoid. (Ibid., 78–79.) A good example of such data collection in the European High North has been given by Shishaev et al. (2020), who ponder upon the technical, legal, and ethical questions with regard to the collection of collective identity research data from online social networking services. While "online social networking analysis represents a promising way to monitor and analyse the identity of a local community" (ibid., 268), "[t]he data circulating in online social networks naturally accumulate and could be used without its owner's knowledge and for undesired purposes" (ibid., 269).

As security aims to overturn likely future trajectories perceived as negative, surveillance is one of the techniques that seemingly offer potential for proactive intervention before harm. In this context, surveillance is often general rather than specific; relates to, for example, crimes both already happened and not yet happened; and "introduce[es] surveillance into areas where nothing crime-related has yet happened, and indeed may never happen". "The innocent [...] are encouraged to accept a certain level of diminution in privacy in exchange for protection that may not be necessary, and which may turn on them should they begin to exhibit characteristics that have been defined as problematic". (Barnard-Wills and Wells, 2012, 229, 231–232.) All individuals and groups become perceived as potentially dangerous and, as a result, previously private or unproblematic behaviours may become problematized to indicate 'risk' or 'being at risk' (ibid., 229).

The surveillance of innocent also serves the purpose of "monitor[ing] the extent to which they are taking responsible actions to minimize their exposure to risk, and to benefit from the protection the technologies offer when they fail to protect themselves" (Barnard-Wills and Wells, 2012, 332). Human vulnerability embedded in 'being at risk' links surveillance closely to human security. Even if claiming to be emancipatory at its core, human security contributes to making vulnerability "an intrinsic, essential quality of identity rather than a moment in individuals' lives" and hence a "source of victimization for particular groups of those encouraged to conceptualize [surveillance] as a protective and benign force" (ibid.).

In their study on vulnerability in datafied society, Hokkanen et al. (2021, 72) widen this conceptualisation of vulnerability by referring to it, first, as term associated with populations or groups that stand out from the majority or can be distinguished by a factor that restricts their ability to act such as age or socio-economic standing.

Second, vulnerability is an ontological concept, that is, “a state that all human beings share”. Third, vulnerability can be understood as an epistemological concept so that the empirical research task is to fill a gap in knowledge concerning vulnerabilities that increase inequality and/or detriment. Finally, it is “a feeling and an expectation on the background”. (Ibid., 72–73.) Their conclusion is that “data collection and digital environments generate vulnerability that manifests in the generation, visibility and categorisation of subjects, their participation and relations to data and other subjects, as well as in the ontological nature of digital existence” (ibid., 84).

3.2.4 The wickedness of transparency

“The diffusion of power through complex networks caused by the multiplication of actors involved in surveillance raises the questions of accountability and transparency” (Barnard-Wills and Wells, 2012, 231; regarding the diffusion of power due to digitalisation more widely see Nye, 2011, 113–151) – as mention in the context of Finnish intelligence legislation already (section 3.2.2). With regard to the lack of transparency, the marketing of surveillance technologies often claims that the focus is on the deviant population and hence the ‘normal’, law-abiding individuals have nothing to fear for (Barnard-Wills and Wells, 2012, 234). A very similar attitude pops up in the wider discussion on digital surveillance as well as on content sharing on online platforms, for example, in the form of the claim that “I have nothing to hide” or that one should live by the law and be willing to waive a part of privacy so that crime can be fought effectively (e.g. Salminen, 2019, 334; 2021, 171; Hokkanen et al., 2021, 74). The norm of the transparency of one’s digital life has thus been adopted to an extent.

While surveillance in cyberspace is partially concealed, the quest for transparency figures prominently in internet governance and among ICT industry (Flyverbom, 2015, 175) – all the way to the extent that it becomes “a form of openness fundamentalism, where by ‘openness’ is seen as a fail-safe solution to virtually any problem” (Morozov, 2013, 90). This kind of internet-centrism “redefines a term like ‘open’ in accordance with the supposed values of ‘the Internet’, only to feed it back into the public conversation” with a shifted meaning so that, for instance, “it is never quite clear whether being open is a means[93] or an end[94]” (ibid., 77–78, 89, 95; see also Flyverbom, 2015, 175).

“[O]nly by suppressing the inherently unstable, subjective, and controversial nature of what we are making transparent we can reduce it to information that can be manipulated, optimized, and tinkered with” (Morozov, 2013, 89). Such reductionism inter alia obscures the purpose for which the information was generated

[93] Transparency as an instrumental value, that is, as a means to some more important end (Morozov, 2013, 80).

[94] Transparency as an intrinsic value, that is, as an end in itself (Morozov, 2013, 80).

and how it is always (re)organised and (re)interpreted (ibid., 72, 87–88). Therefore, one should "stop conflating physical networks with the ideologies that run through them" (ibid., 68) and equating information with transparency and with a direct path to good governance (Flyverbom, 2015, 168–169). Instead, transparency is a form of ordering and hence a technique of government in itself (ibid., 169, 172).

Transparency is a context-bound set of everyday practices which can be directed downwards or upwards, outwards or inwards, and be symmetrical or asymmetrical, but which always revolve around the production and management of visibilities. It "attempts to work on the world by managing possibilities for seeing, knowing and governing". (Flyverbom, 2015, 173.) The translation of transparency ideal into organisational and procedural principles of internet is one way in which it orders 'things'. For example, governments unhappy with the control of chunks of internet infrastructure by private, technical organisations with little oversight can ground their complaints on the principle of transparency – and vice versa. (Ibid., 175–176.)

Transparency ideals are translated also by ICT corporations. For example, according to Mikkel Flyberbom (2015, 176), "[b]oth Google and Facebook[95] claim to be transparent organizations, describe their work as focused on making information available and accessible, and strive to contribute to transparency and openness in societies and politics". Transparency is then turned into "procedural and organisational arrangements, such as architecture, information-sharing and opportunities for employee participation", but also into "decisions about design features and other material arrangements" (ibid., 176–177). The former, organisational ordering associates transparency with a specific style of management, which also entangles it with other concerns like intellectual property rights and cybersecurity as "transparency rarely means full disclosure or openness" but the management of visibilities (ibid., 177). Therefore, even if transparency may manifest inside a corporation, it does not spill over to the relations between the corporation and external stakeholders, such as clients and competitors.

The latter, material ordering of transparency, again, relates, for example, to the question of privacy. ICT corporations "seek to address privacy [...] at the level of [product] design and services" so that "privacy is cast as a matter of transparency and 'user control'" (Flyverbom, 2015, 177). Google and Facebook, for instance, provide users with ways to alter their information and see data that these corporations collect and (re)use, but also require that clients use their real identities when signing up. "This demand for authenticity is described as a way to increase security and trust online, but clearly also ties in with need to have reliable data to mine and aggregate for purposes of profiling users and targeting advertisements". (Ibid., 177–178.) Data management and privacy are hence approached as questions of technical features, user controls,

[95] Facebook changed its corporate name to Meta in October 2021. However, I chose to use its earlier name because that is what appears in Flyverbom's article and by which most people know the company.

and individual responsibility, instead of regulation and politics, all feeding into the government of conduct through techniques that "do not undermine the business models and interests of [these] companies" (ibid., 178; also, Wiatrowski, 2021).

Finally, transparency ideals are translated in attempts to order the political and the societal. Google and Facebook, again, engage in calls for free flow of information and widened participation in politics around internet governance. 'Openness' pops up as a desired value, which conflation with information was highlighted in a previous paragraph. Google's transparency reports, for instance, "disclose how and when governments around the world make requests for user data and other [...] information, when and where the internet has been blocked and when outages have happened or particular services have been made inaccessible by governments" translating transparency into advocacy projects fitting the corporation's aspirations. (Flyverbom, 2015, 178–179.) Such attempts to order politics and societies toward 'openness' "occur against the backdrop of a growing discomfort with the surveillance and tracking made possible by digital technologies, and can be seen as attempts to shift the attention [...] [to] a socio-political vision focused on the benefits of transparency" (ibid., 179). Therefore, "it may be useful to momentarily bracket normative questions about the value or positive effects of transparency and shift attention to empirical and conceptual investigation of [its] limits and potentials", for instance, by examining how the ideal becomes normalised into a durable and concrete order that directs conduct (ibid., 180).

A pivotal question regarding surveillance and transparency then is who is expected and/or obliged to become transparent? In the business model of many ICT corporations, it is the user or the client who is expected to live a transparent life turning into earnings of these corporations. Similarly, in intelligence collection and surveillance those 'who have nothing to hide' should not fear for or be concerned about the omnipresent gaze. However, and as article IV also testifies, such transparency expectations and requirements do not manifest only positively in people's everyday life. Instead, far-reaching data collection and its modification into marketing products irritates, but also generates feelings of insecurity (Salminen, 2021, 170–172).

As a form of resistance to overarching data collection MyData initiative aims "to empower individuals to use their personal data to their own ends, and to securely share them under their own terms" (Declaration of MyData Principles, n/d). According to the initiative's principles, "access and redress, portability, and the right to be forgotten, [should] become 'one-click rights'". Data protection regulation and corporate ethics codes continue to protect people from abuse and misuse, but "common practices [should change] towards a situation where individuals are both protected and empowered to use the data that organisations hold about them". Finally, "a truly free flow of data – freely decided by individuals, free from global choke points – and [...] balance, fairness, diversity and competition in the digital economy" should be created. (Declaration of MyData Principles, n/d, points 1.1.–1.3.) "The core idea is that [people] should have an easy way to see where data about [them] goes, specify who can use it, and alter these decisions over time."[96] This is to be achieved, for example, through organisations and people joining the initiative and following its principles in their own activities[97].

According to Deleuze (2006, 345–346, italics original), the current dispositive of security "is taking shape in attitudes of open and constant *control* that are very different from the recent closed disciplines. [...] The question is not which is worse. Because we also call on productions of subjectivity capable of resisting this new domination". Control attempts to keep the behaviour of individuals and groups within the limits of the acceptable through the techniques of managed transparency, surveillance, intelligence and commercial data collection, normation and disciplining of individual conduct, as well as normalisation. Before turning more towards resistance against some of the aspects of contemporary digitalisation, I will examine the kind of subjectivities expected of individuals in the emerging cyber-physical societies.

3.3 Responsible digital subjectivity

3.3.1 Responsible and resilient individuals

In discussing the responsibilisation of individuals for cybersecurity, article III takes a rather distinctive view to cyber/digital security. Security is not considered a desirable end state in itself, but a condition of trust, which, again, is necessary for digital commerce and other human interaction on digital platforms. Relativity and proportionality contained in modern governmentality come forth, for example, in demands for enough security as a prerequisite for trust and good enough digital literacy as a prerequisite for diminished individual liability. Cybersecurity is institutionalised into a societal structure that enables and sustains economic circulation. (Päläs and Salminen, 2019, 319–320.) Subjects of digital value creation and its safeguarding include digital platforms, but also "everyone from individuals to organisations, states, and all the way to supra-, trans- and multinational actors" (ibid., 320).

While human security may argue that digitalisation empowers individuals, the digital literacy as a civil skill discussion "entails a requirement of a particular level of digital literacy for individuals" as platform users hence responsibilising them

[96] See the web portal of MyData initiative https://mydata.org/ [March 26, 2022].

[97] At the time of writing, MyData had over 100 organisation members and close to 400 individual members throughout the globe. The list of organisation members is available at https://mydata.org/organisation-members/ [March 27, 2022].

for cyber/digital security. (Päläs and Salminen, 2019, 321). Responsibilisation takes place concerning (in)action in both digital and physical spheres (ibid., 332). Individuals are expected to have reflexive moral capacities that "concretize [...] self-regulation promoted by legal norms, moral exhortation, information sanctions and tacit conventions" (Siltaoja et al., 2015, 445, 448). The goal of responsibilisation is hence set from the outside, often by the state, and it sets the individual "responsible according to a certain idea(s), rule(s) and rationality(ies) while keeping [the goal] in mind" (ibid.).

The technical part of cybersecurity individuals may, and often do, outsource to cybersecurity companies – just like the state, businesses and other organisations. Responsibilisation hence contributes to a further societal transformation, that is, commodification and privatisation of security as discussed in sections 3.1.5 and 3.1.6. Acquisition of cybersecurity as a product, for example, in the form of anti-virus software or virtual private network (VPN), operates somewhat similarly to insurance, which is a well-recognised form of commodified security. Both seek to manage freedom in people's everyday life, widen the scope of possibilities but still retain it within certain limits, and shape the way in which uncertainties are perceived and (self-)managed (Lehtonen and Liukko, 2010, 373–374). Insurance incorporates personal responsibility, because responsible individuals make plans for the future, consider themselves and their close ones, and acquire sufficient financial backing (ibid., 377–378) – just like they acquire technical cybersecurity products in case their own coding skills or knowledge to look for open security solutions are inadequate (see Zojer, 2019b).

Article III focuses on responsibilisation of consumers, which is one of the subject positions that individuals can take with regard to cyber/digital security. However, it is often the one reserved for individuals in modern governmentality (e.g. Chandler and Reid, 2016, 28). Responsibilisation entangles with the contemporary discursive and material practices of resilience as already pointed out in sections 1.1 and 1.4.3. In brief, resilience is, for example, "a set of discursive practices of governing through societal security" (Chandler and Reid, 2016, 30) or, from a systemic point of view, "the capacity to absorb, withstand and 'bounce back' quickly and efficiently from a perturbation" (Zebrowski, 2016, 4). It is perceived as a system's natural capacity as well as an improvable capacity within an array of complex adaptive systems such as critical infrastructure, society, individual, or group (ibid.; see also Salminen, 2018b).

According to Chris Zebrowski (2016, 3), the concept of resilience premises security on the exercise of natural functions. It "aim[s] to foster, facilitate and optimize the inherent resilience of systems deemed vital to life" or society, stresses community participation and systemic self-organisation in a bottom-up fashion, and exploits human creativity and freedom hence correlating with modern governmentality. It is "a way of understanding what life is and what life should be". (Ibid., 3, 78.) In accordance with this, "[t]he resilient subject is one that has been taught, and accepted, the lessons concerning the danger of autonomy and the need to be 'capacity-built' in order to make the 'right choices' in development of sustainable responses to threats and dangers posed by its environment" (Chandler and Reid, 2016, 1). Such a resilient subject is characterised by his or her acceptance of adaptive position with regard to changes in the environment, that is, disciplining of the inner self instead of striving to act on and transform this environment (ibid., 1–5, 57; also, Macmillan, 2011, 5, 19). The role of the state, as pointed out also by article I, is to facilitate and enable adaptive and capable individual choices (Chandler and Reid, 2016, 4–5; Rautiainen, 2018, 21). However, as article IV clarifies, while conforming to adaptation, people in Finnish Lapland also seek different kinds of subject positions amidst digitalising everyday life.

Subjects of modern governmentality can no longer be sufficiently protected by the state but live in permanent insecurity caused by contingencies, which requires them to "become autonomous actors with a moral responsibility to better manage their own individual risks" (Zebrowski, 2016, 12–13; see also Chandler and Reid, 2016, 27, 30). They, including individuals and communities, are expected to adapt quickly, regenerate and transform when having faced an emergency, and to learn from it in order to prevent its reoccurrence (ibid., 13–14, 78; see also Salminen, 2018b). Security becomes societalised, that is, the state works "through the choices and behavioural agency of society itself" (Chandler and Reid, 2016, 27).

In Finland, the insertion of digitalisation and cyber/digital security into the framework of comprehensive security (see section 1.3.2) does this move rather distinctively. But whereas Chandler and Reid (2016, 30; similarly, Coaffee and Fussey, 2015, 87) argue that "resilience practices are transforming security discourses from concerns with external threats to fears over the domestic or internal coping", the discursive and material history of the Finnish comprehensive security model exceeds that of resilience in the country. One of the core principles of this model has been, and is, collaboration between internal and external security authorities, across national borders, and across administrative branches and public-private divisions to counter the synthesis of external and internal threats (Heusala, 2011, 97). Moreover, according to Anna-Liisa Heusala (2011, 100), distinguishing comprehensive security and human security from one another is to an extent artificial, which can be seen particularly in the context of everyday security concerns. From this perspective, it is not surprising that both the prevailing digitalisation and cybersecurity understandings and the respective human security related conceptualisations support the same governmentality.

Societalisation of security, according to Chandler and Reid (2016, 29), leads to security being reduced to generic, everyday problems of individual behaviour. The argument in this thesis, however, is that everyday digital security does not concern generic, but specific security problems embedded in place and time. Contextualisation enables not only making the specificities of everyday (in)security visible, but also thinking differently and addressing security differently, that is, by resisting the practices of resilience (see e.g. McCluskey, 2019; Vaughan-Williams and Stevens, 2016; interestingly also Chandler and Reid, 2016, 53). While the appeal and power of modern governmentality depend on its own capacity to adapt and expand, its strategic function is to naturalise institutions, practices and forms of subjectivity supporting its rationality (Chandler and Reid, 2016, 56, 61). Therefore, for example, resilience is capable of absorbing other discourses and developing them further (ibid., 64). "[R]esilience policy becomes increasingly driven by security concerns [while] security policy adopts the language of resilience" (Coaffee and Fussey, 2015, 87). In the process, not only the techniques of security change but those of resilience as well. The profoundness of this change varies and hence resilience can also just rebrand existing practices or operate in the service of enduring processes. (Ibid., 88–89, 91.)

According to Coaffee and Fussey (2015, 92), "the language of security has become recast as that of resilience without changing its fundamental focus and purpose" and hence playing out national security in the local realm as resilience or community-building. At the same time, resilience has been embedded in everyday practices and networked responses, for example, through responsibilisation (ibid., 94). As a result, diverse and even contradictory concepts and practices of resilience have emerged, which, according to Dunn Cavelty et al. (2015, 4) call for the examination of the plurality of resiliences and the requisite practices and subjectivations. The common nominator for resiliences is the examination of "the relations between unpredictable subjects and their complex environments" hence assuming that "the (in)security of a subject is not only dependent on the character and severity of the threat [...] abut also on the subject itself" towards whom the threat is posed (ibid.). The discussion comes, again, close to human security, but the difference seems to be that "resilience marks a significant shift from the predictable to the contingent" (ibid., 5). Like in cyber/digital security, the calculative techniques of security may or may not function leaving room for surprises – and the necessary techniques of the self to survive them (e.g. Coaffee and Fussey, 2015, 101).

In Finland, policies and strategies related to comprehensive security have adopted resilience discourse over the past years. For example, the latest Security Strategy for Society (2017) mentions 'resilience' 47 times, its 2010 version 21 times, while its predecessor from 2006 does not recognise 'resilience' (Security Committee, 2017a; Ministry of Defence, 2010; Security and Defence Committee, 2006). National cybersecurity strategies from 2013 and 2019, quite interestingly, do not utilise resilience discourse[98], even if (cyber) 'resilience' is a widely used concept in (technical) cybersecurity and critical infrastructure protection literatures (e.g.

[98] Finland's Cyber Security Strategy 2013 mentions 'resilience' only five times, while its 2019 update does not refer to the term.

Demchak, 2012; Bologna et al., 2014; Lewis, 2015; DiMase et al., 2015; Setola et al., 2016; Gisladottir et al., 2017; Petrenko, 2019; Eisenberg et al., 2019; Zou et al., 2021). Responsibilisation of subjects is instead carried out directly in the name of comprehensive security and with the civic skill discourse. It is likely, though, that cyber/digital security practices coevolve with the practices of comprehensive security further so that resilience may emerge as a 'thing' in them as well. In developing regions within developed states, to which category Finnish Lapland is often casted, resilience entangles with the digitalisation of everyday life quite concretely. For example, digitalisation tends to concentrate physical services and customer service to centres far away, which demands creativity and persistence from local inhabitants so that everyday situations are managed as explained in article IV (see Salminen, 2021, 170).

In the Arctic, resilience is a household name – possibly, because of the metaphors utilised to construct it as a frontier, an unexplored wilderness, or being in a constant flux due to climate change. The Arctic Council defines resilience as "the capacity of communities and systems to recover and restore themselves from various kinds of crises and disturbances". Because "the speed of ongoing change makes adaptation [in the Arctic] extremely challenging[,] [g]overnments, indigenous peoples, local communities, researchers, and businesses must work together to build resilience to the social-ecological changes that are underway". (Arctic Council, 2020.) Arctic Resilience Report (2016, viii), facilitated by the Arctic Council, concluded "a five-year effort to better understand the nature of Arctic change, including critical tipping points, as well as the factors that support resilience, and the kinds of choices that strengthen adaptive capacity". This effort had been "set in motion at the start of the Swedish Chairmanship of the Arctic Council (2011–2013)" (ibid.) and it served as a stepping stone for the adoption of the Arctic Resilience Action Framework (ARAF) by the Arctic Council Ministers in the Fairbanks Declaration in 2017 (Arctic Council, n/d).

"The ARAF [which was operational between 2017 and 2019] [was to provide] the Arctic Council with a common frame of reference for building resilience in the Arctic region" (Arctic Council, n/d), that is, "a common set of Guiding Principles and Priorities for Action, as well as a platform to continue discussing priorities as they evolve" (Arctic Council, 2017, 1, 4). One of the actions of ARAF was to convene an Arctic Resilience Forum in Rovaniemi in 2018[99] "as part of the programme of Finland's Chairmanship in the Arctic Council [2017–2019]. The Forum [was to] provide an opportunity to share best practices and identify additional challenges to building resilience. In addition[,] the aim of the Forum [was] to create conditions to strengthen resilience and adaptability of different stakeholders in the Arctic

[99] The First Arctic Resilience Forum was organised in Rovaniemi on September 9–10, 2018. See Gaia Consulting (2018).

region." (Arctic Council, n/d.) The Forum convened for the second time virtually in 2020[100] under the Islandic Chairmanship of the Arctic Council (2019–2021) (Arctic Council, 2020). The discursive and material practices are hence not only institutionalising "resilience" as a survival strategy, but also as an illuminating truth about the living conditions in the Arctic as a constant struggle.

According to the Arctic Resilience Report, there are "four key factors that contribute to resilience: 1) the capacity for self-organization – that is, to make decisions and implement responses to change; 2) diversity of responses to change; 3) the ability to learn from and integrate diverse types of knowledge; and 4) capacity to navigate surprise and uncertainty" (Arctic Council, 2016, xiii). "[A] decline in the capacity for self-organization [is] strongly associated with a loss of resilience. Capacities linked to learning, the maintenance of social memory, and learning from crisis[, again, are] very important for enhancing resilience" (ibid.). The report discusses neither digitalisation, nor cyber/digital security, but refers to 'telecommunications' three times (Arctic Council, 2016, 44, 211, 214); to 'digital networks' (ibid., 170), 'digital assistant' (ibid., 190) and 'cyberspace' once (ibid., 122); to 'internet' eight times (ibid., 117, 122 [twice], 141 [four times], 142) as well as to 'new technologies' or 'new communications technologies' (ibid., xii, 63, 65, 82, 97, 119, 169 [twice]).

Similarly, the Arctic Resilience Action Framework mentions 'telecommunications' only twice (Arctic Council, 2017, 11, 16) as does the report on the First Arctic Resilience Forum (Gaia Consulting, 2018, 58, 70). 'Digital' appears in the former once (Arctic Council, 2017, 22) and in the latter four times (Gaia Consulting, 2018, 29, 39 [twice], 44). The latter also mentions 'internet' (ibid., 39) and 'new technologies' (ibid., 26) once. Therefore, it seems that the Arctic Council perceives neither digitalisation nor cyber/digital security a factor that significantly contributes to resilience in the Arctic. They both remain side clauses added here and there – in contradiction to what the reports of the Arctic governance bodies briefed in section 1.2 noted.

The aforementioned should maybe not be seen as surprising for, according to Renaud et al. (2018, 199), "most governments do not actively support citizens in terms of mitigating [...] cyber risk [in] the way they act to regulate other, older and more well-known risks". The Arctic Council is an inter-governmental organisation with indigenous presentation. For example, governments tend to have well-established structures for managing "a variety of health, safety and physical crime risks[,] [...] [but] the computer owner [...] is largely held responsible for managing his/her own cyber security" (ibid.). "[T]here is very little support [...] in terms of actively helping people to manage their cyber defences, nor is an official safety net

[100] The Second Arctic Resilience Forum was organised as a series of webinars between October 7, 2020 and December 16, 2020. See Arctic Council (2020).

put in place to support those who do fall victim to cyber attacks. As things stand, the most pervasive official strategy is the provision of advice." (Ibid.) A pivotal question then is what happens to the production of security when power is in this way moved from politicians and administrators to technocrats and nerds with the ability to formulate the cyber-physical environment and when individuals are simultaneously responsibilised for their own security (Salminen, 2018b, 206).

3.3.2 Techniques of the self

The techniques with which individuals can, and are obliged to, help themselves entail the so-called techniques of the self, which Foucault studied widely as well. Self-techniques are historically important compilations of practices aimed at developing and modifying oneself so that a certain mode of being can be attained (Foucault, 2014, 269–270). In modern governmentality, they have been interpreted as implications of both self-centrism and self-care (often through self-denialism). The aims of such techniques have been multiple, including salvation, knowing oneself, good manners, socially acceptable forms of exercising individual freedom, and overcoming of oneself. (Ibid., 273–274, 304.)

Thus, self-techniques do not only involve one's relationship to oneself, but also to others as self-care contributes to finding a suitable place in society, community, and human relations in general and as it requires the listening of advice. Those who take care of themselves in a suitable manner are also able to behave appropriately and care for others, as well as to look after the society – also in and with regard to cyberspace. On the contrary, forcing others to accept one's gratifications and preferences indicates abuse and the person resorting to such behaviour is a slave to his or her desires unable to constrain them. (Ibid., 275–277, 290, 301–302.) Self-techniques are hence a category of techniques that human beings utilise to understand who they are (ibid., 300).

According to Foucault (2014, 300), four groups of such techniques can be distinguished: (1) techniques of production, (2) notational techniques, (3) techniques of power, and (4) self-techniques. The first include the ways to produce, modify and manipulate objects; the second the ways of using notations, meanings and symbols as well as giving meanings. The techniques of power specify human behaviour, subject people to government with particular ends, and objectify subjects. Finally, self-techniques enable individuals, by themselves or together with others, to modify their bodies, minds, behaviours and modes of being in order to reach a certain stage. These groups of techniques seldom operate separate from one another and all of them include a certain way of guiding and transforming individuals – not only their capacities, but also their attitudes. (Ibid.; also, Macmillan, 2011, 7.) In addition, self-care is a universal principle and a lifestyle required from everyone throughout his or her life (Foucault, 2014, 311–312). It thus comprises three components: "a general attitude with respect to oneself, to others and to the world; a form of attention turned towards oneself; [and] a series of practices or techniques of the self" which all are "features of the ethical sense of conduct" (Davidson, 2011, 30).

Confession, dialogue, listening, and searching for the inner truth of the soul (conscience) have been important self-techniques (e.g. Foucault, 2014, 298–330). The latter entails an inventory of what one has done, what one should have done, and comparing the two in order to remind oneself of the correct behaviour, that is, one should practice introspection. Instead of denying oneself, one should learn the truth of him- or herself and turn that into a principle guiding one in facing different events in life. (Ibid., 316–317.) The technique is related to confession, which is a ritual relied on for the production of truth and entailing "someone's acknowledgement of his own actions and thoughts" (Foucault, 1998, 58–59). In confession, "the speaking subject is also the subject of the statement" and the ritual requires the presence of a partner to whom the confession is made and who can provide guidance (ibid., 19, 61–62) irrespective of whether face-to-face or in a technology mediated manner like on digital platforms. Confession is so wide-spread practice that it is no longer perceived as an effect of constraining power. Instead, an inner urge compels individuals to confess. (Foucault, 1998, 60–63.) Such practices not only help finding oneself, but also controlling one's representations and conforming to rules (ibid., 319). With regard to cyber/digital security, one is expected to acknowledge and confess, for instance, gaps in his or her digital literacy, as well as actions he or she has taken and mistakes done, on the basis of which further examination of a cyber incident takes place (see Päläs and Salminen, 2019; Salminen and Päläs, 2021).

While many of such techniques are utilised in the production of digisavvy citizens, the techniques themselves have also been moved to cyberspace and began to operate especially in social media. For instance, Mareile Kaufmann (2015) has examined the utilisation of social media for self-care during and after the terrorist attacks in 2011 in Oslo and on Utøya in Norway. She understands resilience as "an act of self-care that draws upon people's self-governing capabilities" and is carried out by individuals responsibilised for their own security (ibid., 974). Web 2.0 technologies contemporarily influence "the way in which the subject, the care, and the self-care come about" in both "the first-response kind of functions [...] of resilient self-organization [...] and the emotional functions that emerged in the longer aftermath" (ibid., 975, 977). Social media was hence, first, used "as a tool to gain an overview of the unfolding situation", to establish some sort of normality amidst the situation, and to "identify who is in danger" (ibid., 978–979). Second, it was utilised "to affect and to be affected [when] emotions were described, distributed, consumed, experienced and conserved in a networked manner". It "enabled and reinforced a form of dealing with the attacks on an emotional level, as well as instances of care and self-care". (Ibid., 981.) Yet, the use of social media for collective mourning also raised concerns for privacy and misinformation (ibid., 981–983). In a similar manner, even if in less dramatic circumstances, people participating in the workshops for article

IV emphasised the potential for self-caring practices that social media and ICT in general bear (Salminen, 2021, 168).

Techniques of modern governmentality such as resilience and self-techniques in the production of cyber/digital security depend on their counter-techniques towards which I will turn in the next section. Governmentality is "a form of power which makes individuals subjects. Two meanings of the [...] 'subject' are here at play: subject to someone else by control and dependence [and subject] tied to his own identity by a conscience or self-knowledge. Both meanings suggest a form of power which subjugates and makes subject to." (Foucault, 1982, 781.) Instead of satisfying with such subjectivity, individuals seeking freedom could carry out "a critical reflection on oneself [...] to find alternative to the objectifying mode of subjectivity" that enables domination "by hindering the [evolvement] of free and autonomous subjects" (Macmillan, 2011, 4–5). Politics can then "be considered from the perspective of reflective practice of freedom" in which "the free man will determine his conduct and the manner to achieve the goals he has set for himself" without resorting to the binary of the permitted and the forbidden (ibid., 5, 7). Instead of mere rule-following and relating oneself to norms, "[i]t is the relation to truth of the free subject that allows him to become master of his conduct" and able to take care of himself – and of others as a consequence (ibid., 8).

Ethics associated with the care of the self refers more to universal principles understood through experience and reflection on the self and others than pure self-centrism. "[T]he subject is not fundamentally capable of truth [but] needs to accomplish a certain number of actions on himself to become capable of knowing". (Macmillan, 2011, 8–9, 19.) Self-techniques comprise such actions. They thus not only facilitate the internalisation of particular techniques of government embedded in the dispositive of security in and with regard to cyberspace, but also provide potential for behaving differently through self-reflection, ethical conduct, and resistance.

3.3.3 The (im)possibility of resistance?

Articles II and IV operate in parallel in the governmentality setting. Article II investigates from a human security perspective what kind of personal/health security concerns related to digitalising healthcare and social security people residing in Finnish Lapland may have. It embeds this perspective in the explication of an inconsistency in the ongoing regional administration reform that created room for local resistances in south-western Lapland. Article IV then serves as its counterpart. It illuminates the actual ways in which people living in Finnish Lapland ponder upon digitalisation and cybersecurity as part of their everyday lives. The experienced impossibility of influencing the direction towards which societal digitalisation is developing is one of its conclusions. The article makes visible, for example, the dependency on ICT and functioning communication networks that people point out as a vulnerability inherent in their lives. However, they also envision resistance to overarching digitalisation in order to improve their own and others' wellbeing.

"[T]here [is] an immediate and founding correlation between conduct and counter-conduct" (Foucault, 2009b, 196). They constitute one another. More precisely, counter-conduct is internal to the phenomenon sought to be managed, a kind of border-element, which the conduct of conduct seeks to merge within its range of accepted forms of behaviour (see ibid., 214–215). In other words, "[w]here there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power" (Foucault, 1998, 95). It manifests itself in a multiplicity of roles in power relations such as adversary, target, support, or handle. Hence "there is no single locus of great Refusal", but a plurality of resistances varying in their form, endurance, extent, possibilities, effects, and so forth. These resistances are distributed in an irregular manner, mobile, and transitory and they produce cleavages in society that fracture unities and cause regroupings. Such points of resistance enable revolutions in a similar way that the conduct of conduct seeks to merge counter-conduct in accepted forms of behaviour. (Ibid., 95–96; Foucault, 2009b, 215.)

Like power relations, resistances are omnipresent and entail a degree of freedom (Foucault, 2014, 281–282). "Power is exercised only over free subjects, and only insofar as they are free. By this we mean individual or collective subjects who are faced with a field of possibilities in which several ways of behaving, several reactions and diverse comportments, may be realized" (Foucault, 1982, 790). Therefore, power relations ought to be studied from the perspective of the forms of resistance set against the multiple forms of power. Power struggles hence visualised are "transversal", that is, not restricted to one location; aim at "the power effects as such"; immediate because they take place close to individuals' everyday life and because they concern contemporary problems to be solved in the present; "question the status of the individual", that is, his or her (non-)difference; tackle the privileges of knowledge but also of secrecy and mystification; and, finally, revolve around the question of who we are. They are not struggles against any institution, for example, the state, but against a form of power conceptualised in this thesis as modern governmentality in and with regard to cyberspace. (Ibid., 780–781.)

Resistance can take the form of external blockages, such as population's passive or active resistance taking place outside the given field, in this thesis, outside the practices of digitalisation and cyber/digital security like in article II, as well as the form of internal resistance, that is, the forms of attack and counter-attack within the field like in article IV (Foucault, 2009b, 194). Foucault was particularly interested in the latter as it seeks to transform the conduct of behaviour. Its "objective is a different form of conduct, that is to say: wanting to be conducted differently, by other leaders [...], towards other objectives [...], and through other procedures and methods". (Ibid., 194–195.) Such revolts do not take place in a vacuum, but are linked to other problems and conflicts as, for example, to the reform of regional administration as in article II (ibid., 196).

These counter-conducts "have as their objective and adversary a power that assumes the task of conducting men in their life and daily existence (Foucault, 2009b, 200). They can be found, for instance, from individual behaviours, more or less organised groups such as Anonymous[101] or Suohpanterror[102], and entirely new attitudes represented, for instance, by WikiLeaks[103] (ibid., 204). Thus, they include both the "specifically private forms of the problem of conduction: How to conduct oneself, one's children, and one's family?" and the problem of conduction in the public domain (ibid., 230; also, Davidson, 2011, 27). Moreover, "[c]onduct and counter-conduct share a series of elements that can be utilized and reutilized, reimplanted, reinserted, taken up in the direction of reinforcing a certain mode of conduct or of creating and recreating a type of counter-conduct" (Davidson, 2011, 27; also, Foucault, 2009b, 215).

Resistance and counter-conduct should not be understood merely as passive reactions or as disobedience, but in order to resist one must activate something as productive and inventive as power itself (Davidson, 2011, 27). As "power never exhaustively determines a subject's possibilities" "ethics is in effect a kind of freedom of conduct", which can be exercised in counter-conduct as self-care (ibid., 30). Counter-conduct "*transforms* one's relation to oneself and to others; it is an active intervention of individuals and constellations of individuals in the domain of the ethical and political practices and forces that shape us" (ibid., 32, italics original).

Instead of merely subordinating conduct to law (see 3.1.4, 3.1.5 and 3.2.2), the real effects of the battle for rights should be investigated in attitudes and behaviour. "[T]he attempt to create a new mode of life is much more pertinent than the question of individual rights" that stabilises certain forms of conduct. (Davidson, 2011, 31, 33.) It entails the risk of becoming evaluated as dangerous with the requisite consequences amongst peers, in social groups and communities, as well as in the

[101] According to one of the many definitions, Anonymous is a shared pseudonym and a hacker network "resist[ing] the private accumulation of wealth and the expropriation of knowledge". It "targets the websites and the communication infrastructure of institutions that limit access to information technology, seclude sensitive information from public scrutiny, or prosecute those who struggle for unrestrained access to these technologies". (Deseriis, 2013, 34.)

[102] Suohpanterror is a Sámi artist collective commenting on injustices in Sapmi and/or against the Sámi. Its main form of expression is posters on digital platforms. See e.g. the collective's Facebook site https://fi-fi.facebook.com/suohpanterror [February 27, 2022].

[103] "WikiLeaks is a multi-national media organization and associated library. [...] [It] specializes in the analysis and publication of large datasets of censored or otherwise restricted official materials involving war, spying and corruption." WikiLeaks (2015) What is WikiLeaks. https://wikileaks.org/What-is-WikiLeaks.html [March 19, 2022]. The materials are provided by people who wish to disclose secrets without a fear of being exposed or incurring a liability (Domscheit-Berg, 2011, 13). WikiLeaks manages the entire laying of information process from the uploading of materials by informants to their refining, verification, contextualisation, and publication (ibid., 257).

society as a whole (ibid., 36–37). As mentioned in the previous section, counter-conduct utilises self-techniques like the internalisation of obedient behaviour does. Their difference, however, arises from their aims: instead of rule-following, counter-conduct seeks to advance ethical self-evaluation and decision making on the basis of such reflections. This is where the basis for empowerment in its more radical form lies.

Ball and Olmedo (2013, 85–86) anchor resistance to modern governmentality to subjectivity as well[104]: subjectivity is "a site of struggle and resistance" carried out in practices of resistance. A person paying attention to "the *how(s) of power* inside and around him or her", as well as of his or her beliefs and practices, can perceive the power relations he or she is imbricated in and "begin to take an active role in [his or her] self-definition" (ibid., 86, italics original). This becoming active takes place, for example, by defining what one does not want to be or to become. As governmentality "works best when we come to want for ourselves what is wanted from us", resisting it "implies problematising the essence and 'raw material' of our own practices" (ibid., 89). All ICT users could hence conduct critical investigations of their digitalising everyday life and decide upon what kind of equipment, network, service, and application users they wish to be – or not to be (see e.g. Zojer, 2019b). The practices of resistance, however, are not invented by the individual, but embed in the local culture, society, and in his or her social groups. Historical, political and economic factors constrain the field of opportunities for resistance alike. (Ball and Olmedo, 2013, 86–87.)

In a similar vein, Jaron Lanier (2010) points out in his rather provocative manifesto that a human being is not a gadget. Aligning with Morozov's (2013) remarks about openness discussed in section 3.2.5, he claims that the 'open culture' of Web 2.0 promotes more the freedom of machines than of people (ibid., 3). As "small changes in details of a digital design" may have a profound effect on the experiences and behaviour of people playing with it (see also Lessig, 1999) and as "developers of digital technologies design a program that requires you to interact with a computer as if it were a person, they ask you to accept [...] that you might also be conceived of as a program" (Lanier, 2010, 4, 20).

Furthermore, like discussants in the workshops organised for article IV, Lanier states that "impersonal communication has demeaned interpersonal interaction". This has led to "a reduced expectation of what a person can be, and of who each person might become". (Lanier, 2010, 4, 6.) The corresponding phrasing in the workshops was that because in social media one can be whoever he or she wishes to be, one may risk losing his or her identity (Salminen, 2021, 172). Because "different media designs stimulate different potentials in human nature" (Lanier, 2010, 5;

[104] Ball and Olmedo (2013) discuss performativity in the field of education, but I have generalised their approach.

also van Dijck, 2013, 7), the calls for ethical responsibility for those who provide or obligate digital service use presented in the workshops also receive backing. Instead of conforming to the dominant design of digital platforms, one could, for instance, consider avoiding anonymous posting, putting effort in finding audiences outside the readers of Wikipedia[105] and the followers on Instagram[106] or YouTube[107], creating websites that do not fit into the templates provided by social media, spending time to create quality videos and well-though blog posts, and innovating in Twitter[108] instead of describing events or just retweeting (Lanier, 2010, 21). Even if the aforementioned still holds the individual firmly entangled with modern governmentality, it at least tries to halt individuals and communities to reflect their conduct in cyberspace, which produce different assemblages of freedom and security.

[105] ”Wikipedia is an online free-content encyclopedia [...] supported by the Wikimedia Foundation and consists of freely editable content”. Wikipedia (2022) Wikipedia: About. https://en.wikipedia.org/wiki/Wikipedia:About [April 17, 2022].

[106] Instagram is a social media platform owned by Meta.

[107] YouTube is an online video sharing platform owned by Alphabet Inc., which is Google’s mother company.

[108] Twitter is a microblogging and social networking platform which defines itself through a task of ”foster[ing] free and global conversations that allow all people to consume, create, distribute, and discover information about the topics and events they care about most”. Twitter (2021) Global Impact Report 2020. https://about.twitter.com/content/dam/about-twitter/en/company/global-impact-2020.pdf [April 17, 2022].

4. Concluding remarks

4.1 Whose security in cyberspace? Whose freedom?

“In the grand scheme of things, what exactly is being improved is not very important; being able to change things, to get humans behave in more responsible and sustainable ways, to maximize efficiency, is all that matters.” (Morozov, 2013, viii.) This “quest to fit us all into a digital straightjacket by promoting efficiency, transparency, certitude, and perfection – and, by extension, eliminating their evil twins of friction, opacity, ambiguity, and imperfection – will prove to be prohibitively expensive in the long run. [...] Imperfection, ambiguity, opacity, disorder, and the opportunity to err, to sin, to do the wrong thing: all of these are constitutive of human freedom, and any concentrated attempt to root them out will root out the freedom as well.” (Ibid., xi–xii.)

This thesis is essentially a narrative about evolving cyber/digital security, its institutionalisation in Finland, and the positioning of individuals in it. The latter in particular stands at the heart of this thesis as much of it describes the security subjectivities allocated to individuals in digitality and government through them, as well as problems in and resistance to the adoption of such subjectivities. My aim has been to depict the production of digital/cyber security as it currently takes place in the Arctic, the European High North, and in Finnish Lapland, where security practices embed in the national arrangements of Finland (and those of the EU). Regional and national diagrams of digitalisation partially overlap, but also differ from one another to the extent that I have found it important to discuss both. In addition, there is a notable lack of a regional cybersecurity diagram, which sustains security practices that maintain the state and ICT corporations as the primary definers of cyber/digital security. Starting from a sub-state and inter-state setting, as well as focusing on the security and wellbeing of individuals and communities, has made visible some of the tensions round which power relations in digitality and its securitisation twine.

Furthermore, I have tried to envision either through human security or governmentality studies, or by combining the two, how ‘things’ could be ordered differently so that individuals’ and communities’ freedom to decide for themselves could be better preserved under the pressure of overarching control which potentiality digitalisation advances. These concluding remarks also continue this discussion. All techniques of government discussed in this thesis have multiple, even contradictory effects that are gradually manifesting themselves as digitalisation of societies advances. Influencing digitalisation and its securitisation is hence pivotal now, when ‘things’ are in flux, before their firmer fixation and institutionalisation (see e.g. Choucri et al., 2018 about the international institutionalisation of cybersecurity). Therefore, it is necessary to ask whose security in and with regard to cyberspace matters; towards what kind of strategic imperative digital Lapland is being steered; and how to govern radical freedom, resistance, and ignorance that defy 'the right kind of' digisavviness?

In order to be able to ask such questions, there is a need to "pay attention to the way that cyber security is understood as a problem of government, the particular vocabularies and discourses that construct this problem and the solutions those problematizations privilege" (Barnard-Wills and Ashenden, 2012, 115). Throughout this thesis, I have tracked and described both discursive and material practices in which cyber/digital security in Finnish Lapland becomes produced. These practices, assembling into different security techniques in the service of modern governmentality, also produce their counterpart, that is, counter-conduct of individuals and communities seeking to be governed differently. Security dispositive is thus in constant transformation currently energised by power struggles related to the government of cyberspace. The fast pace of ICT development, but also human (re)interpretation of the technology and its use feed into these struggles.

As discussed in the four articles that constitute the empirical part of this thesis, manifold framings of cyber/digital security aim to protect different 'things' and position these 'things' differently vis-á-vis one another. Technical cybersecurity seeks to protect both flowing and standing information, whereas national security framings focus on critical infrastructures, vital societal functions and core societal values hence aiming to ensure circulation essential to economy and society. Human-centric framings of cyber/digital security then focus on the everyday lives of individuals and communities in their specific contexts. According to a human security approach, cyber/digital security should incorporate both enablement and protection of people, introduction of their own views in security production, prevention and mitigation of threats that are not necessarily existential in their character but still cross the threshold of being considered security problems, and both long-term developments and short-time changes. Thus far, these kinds of aims have been accommodated better in regional digitalisation programmes than in national cybersecurity policies.

The protection of different 'things' produces different threat and risk imageries that are countered and mitigated by alternative means and measures. However, these framings overlap, enmesh, and all operate within the dispositive of security embedded in modern governmentality. They all contribute to what is emerging as cyber/digital security in Finnish Lapland. In this thesis, my primary aim has not been to answer to the 'what' of cyber/digital security, but to the 'how' and 'with what effects' of cyber/digital security. What is sustained in society is circulation, but as the thesis has shown, the 'how' question becomes answered differently depending on power relations at the points of decision making. Who can influence decision making and which knowledge and truths are valued? Where does the money go to? What kinds of practical arrangements are created? Decisions taken modify the everyday life of everyone; especially, when they are carried out within the comprehensive security model of the Finnish society and responsibilise one and all for cyber/digital security.

On the one hand, practices of digitalisation and its securitisation, such as guidance, extitutional surveillance, transparency management and criminalisation, seek to produce obedient individuals who meet the norm of digisavvy citizens and willingly provide information of themselves to those in (legitimate) need. Such citizens also master the principles cyber/digital security and are able to protect themselves from dangers lurking in cyberspace without being too skilled in concealing their information and hence complicating data collection and government with the techniques (of security) available. Thus, they constitute a digital population from which normal behavioural curves can expectedly be calculated and educational and training interventions targeted accurately to bring deviant trends in line with this normality. However, the enduring lack of information concerning, for example, individuals' behaviour in and with regard to cyberspace complicates this task and directs governmental decision making towards the utilisation of disciplining techniques. Individuals and communities become governable and accede to modern governmentality when they come to value the benefits that digitalisation provides them. On the other hand, the aforementioned practices embedded in self-techniques provide potential for deciding for oneself which at the same time may entail becoming dangerous either as too skilled or as ignorant, resistant to change, and/or incompetent.

The former group of people, the experts, needs to be kept in Finland and 'on the right side', that is, working for Finnish companies, administration and other organisations in order to keep the nation safe. There is a similar desire to localise such skills in Lapland, but the governance documents discussed in section 1.2 testify how varyingly these desires have been met all over the Arctic. The latter group of people, the laymen, needs to be awakened through raising awareness, cultivating skills, and explicating the negative, potentially disastrous consequences of failing to participate in digitality and self-protection; their 'civic skills' have to be improved and their attitudes changed – if not otherwise, then by raising the costs of doing things differently very high or eradicating alternatives to running errands digitally. This group comprises the majority of Finnish population, but because of the mental images hold of the Arctic, it becomes addressed as a developmental issue in Lapland.

This duality of cyber/digital security actors' expected obedience and self-reliance, as well as the embeddedness of economic rationality in government, is evident, for example, in the final report of the Ministry of Transport and Communications' working group, which was "to examine how to improve information security[109] and

[109] In the report, information security and cybersecurity are used synonymously (Ministry of Transport and Communications, 2021, 19).

data protection in sectors that are critical to the functioning of society", published in 2021 (Ministry of Transport and Communications, 2021, 5). Here the report serves as a final example of the evolving discursive and material practices in which cyber/digital becomes produced and which continuously seek to formulate responses to the societal security problem that also evolves continuously.

Amongst other things, the working group discussed the allocation of responsibility between the private and the public from an economics perspective. According to it, "[i]n the development of information security and data protection, the responsibilities of private actors face the responsibilities and needs of the entire society" and the actions of private and public actors are currently not aligned (Ministry of Transport and Communications, 2021, 21, my own translation). "From the perspective of the society, all actors ought to protect their products and services by sufficient measures", which for individuals means ensuring information security on their equipment (ibid., my own translation). However, and even if the remark about the non-alignment of private and public actors' interests and actions regarding cyber/digital security is the same in this thesis, meeting such a requirement is not enough but individual responsibility is actually much wider and to an extent undefined as also discussed throughout this thesis.

Some actors may not acquire a sufficient level of information security and data protection due to, for example, the fact that when a problem occurs, no actor has to bear all of the consequences but the society will cover a part (Ministry of Transport and Communications, 2021, 21). For an individual (in)acting in insecure cyberspace the consequences which the society will cover are an essential ingredient of, for example, trust and confidence to act in cyberspace. They serve as a form of social insurance that frees people to take some risk. As it became evident in the workshops organised for article IV, some people stay away from or only minimally use digital applications and services because they are aware of cyber threats and do not trust the environment, other actors operating in it, and/or their own digital skills. Uncertainty about one's digital literacy as such may serve as an obstacle to engagement in digital(ised) activities. (Salminen, 2021, 171–172.) Zero societal acceptance for mistakes and full liability for one's actions could quickly end the ongoing digital development. Societal negotiations about acceptable risk and proportionate liability in and with regard to cyberspace are therefore taking place in multiple fora in the form of, for instance, risk calculations, court proceedings, legislative bills, and strategic and operational planning.

According to the Ministry's working group, the so-called privacy paradox also feeds into the problem of cyber/digital security. The paradox emerges when actors give the impression that they are interested in information security and data protection, but behave in a manner that ignores both. (Ministry of Transport and Communications, 2021, 22.) This paradox has been and remains a recurring issue that has received its most notable expressions in the hearings, court cases and (subsequent) sanctioning of ICT giants for breaches of privacy. Such cases with high news value are, nevertheless, only the tip of an iceberg and the problem is actually much more mundane (see e.g. Lehto et al., 2018). As acquiring and maintaining a sufficient level of information security and data protection generally requires higher investment, actors are likely to decide for a lower level of security. Other factors like the (estimated) costs of an information breach and reputation management influence decision making as well. From the perspective of the society, an actor's decision for insufficient information security and data protection decreases the wellbeing of and trust amongst the citizenry and increases both opportunity costs and resource needs. As a suggested solution, the regulator should construct a system in which actors have an interest to acquire and maintain sufficient information security and data protection. (Ministry of Transport and Communications, 2021, 22–23.)

However, law is only gradually catching up with regulating, for example, both individual and collective behaviour in cyberspace and corporate actions in collecting, (re)organising, and selling information (see e.g. Wiatrowski, 2021). Many of the recommendations of the working group entail either reviewing and possibly updating legislation in force or enacting new laws. For example, a unified legal framework for cooperation between authorities in the event of an information breach should be created. In the same process, cooperation models with the private sector should evaluated. (Ministry of Transport and Communications, 2021, 8.) Clear and proportionate, risk-based information security requirements for critical industries should be set in law. Authorities ought to have sufficient powers to issue binding information security orders to these industries. (Ibid., 10.) Critical industries should be obliged to define critical ICT processes and functions, as well as to regularly audit them (ibid., 10–11). Alongside strengthening regulation, guidance and supervision, financial resources in both public and business sectors should be directed to improve information security and data protection (ibid., 18). The state is thus seeking a firmer grip of control on cyberspace though regulation; especially, in the critical sectors that sustain circulation in economy and society.

From the perspective of individual security, the suggestion to develop a centralised service through which private persons and representatives of organisations could receive information and report information security threats and breaches to NCSC-FI, regulatory authority, and/or the Police, as well as to the Data Protection Ombudsman, is an important one (Ministry of Transport and Communications, 2021, 16). Nonetheless, it still seems that the security concerns of individuals amidst their digitalising everyday life are not primary in comparison to the continuity of economic and governmental functions and services, as they occupy relatively little space in the discussion. The security of corporations, states and societies is ranking first, which indirectly may or may not contribute to the security of individuals and communities.

This is the main critique of this thesis expressed in both the articles and this synthesis: While individuals are increasingly responsibilised for cyber/digital security in society, they, first, receive relatively little support from society in recognising and carrying out their respective security roles and, second, have relatively little influence in what is defined as a security problem. Therefore, the rationality of a cyber-physical order which is critically vulnerable to technology's and individuals' imperfection and the latter's freedom to act deserves to become problematised from a number of perspectives such as human security and/or resistance and self-care. What bothers me in contemporary cyber/digital security is the presumption that the human being has to adapt to the needs of technology that is inherently vulnerable or to be programmed out of the loop. ICT should serve people, not the other way around.

In shifting the gaze from information, information infrastructure and functions vital to society to individuals and communities in their everyday lives, a human security approach to cyber/digital security seeks to empower people to decide for themselves. However, empowerment is linked to responsibilisation as it implies individual rights and responsibility. Digital human and basic rights then serve as the minimum standard for wellbeing, but should be considered merely an intermediate stage in achieving the unachievable human fulfilment. By basing its framework on 'freedom from fear, want, and indignity', human security attempts to define security and the sought values following from security such as human development, wellbeing, equality, and individuals' and communities' flourishment from the outside; not necessarily from within communities and in line with their framings.

Simultaneously, human security continues to characterise (human) life in the Arctic as 'vulnerable' and 'precarious' and therefore in need of protection, as well as distinctively a struggle given the prevailing spatializations of these areas and advancing climate change. It thus subjectifies individuals and communities to seek wellbeing through security, development, and resilience; to choose from the available alternatives for their own, externally defined benefit; to claim for basic and human rights as a baseline for fulfilled life; and to acknowledge their own insufficiency and need for perfection. However, they are also expected to recognise their own capacity to lead their lives towards the goals set. While increasing autonomy, empowerment hence "often intertwine[s] with the ideas and promised of [modern] governmentality in making individuals more self-responsible and committed to the 'common values and ethos'" (Siltaoja et al., 2015, 448–449).

Furthermore, the wellbeing of those unable to participate in advancing digitality is "negotiated through market order and existing hierarchies" and provides a few "alternative ways [of] doing things if one wishes to adopt a new identity that resembles an active subject" set by digitalisation and cyber/digital security (Siltaoja et al., 2015, 450). As mentioned by the participants in the workshops organised for article IV, there is little opportunity to influence the ongoing digital development but to adapt to it. That is, one is to accept those services and applications to his or her use that are necessary and/or beneficial and learn the required know-how – or accept being permanently dependent on the help and guidance of close-ones and/or individuals allocated support roles in digitality. In other words, one is to adopt the subjectivities fostered by the digitalisation of society and its securitisation. Yet, influencing digitalisation should be somehow possible; at least, by contacting and pressuring decision-makers. (See Salminen, 2021, 174.)

Human security successfully lifts individuals and communities to the centre of analysis, but advocates mainly for (equal) access to information and cyberspace, improvement of people's digital literacy, and the realisation of digital rights and rights dependent on the functioning of digitalised infrastructures. It calls for considering local conditions in advancing economic, infrastructural, social, cultural, environmental, and other forms of development. By so doing, it seeks to align cyber/digital security defined as individuals' and communities' security with both technical and strategic understandings of security in and with regard to cyberspace. Moreover, it seeks to establish the bare minimum to be reached in all of the aforementioned aspects of cyber/digital security: good enough connection; good enough skills; strong enough legal stance for individuals and communities in relation to the state, corporations, and other stakeholders in global capitalism built on the network of networks; and distinct enough identity based on the local characteristics and conditions. However, it does not challenge the rationality of modern governmentality, for example, in overarching digitalisation or in securitising digitality.

Human security thus does not 'free' people from modern governmentality but accommodates them firmly in the dispositive of security. Nor is the aim in the critiques of modern governmentality to 'free' people, as all social (inter)action presupposes some forms of self-government and the government of others. Instead, the examination of modern governmentality, including its current forms, consequences, resistances, and struggles, creates room for questioning, thinking differently, and acting differently. (Kaisto and Pyykkönen, 2015, 13–14.) The aim is to change government practices so that they become more suitable to people (Siltaoja et al., 2015, 454). Problematising the prevailing truths is necessary for individuals and communities to decide ethically upon their conduct.

"Through the writing of (in)security, identity, which in the lived experiences of everyday life might be more fluid, becomes necessarily more entrenched, fixed" (Stern, 2006, 192–193), which may suggest that there is value in avoiding the language of security in describing individuals' and communities' everyday experiences in and with regard to cyberspace (cf. McCluskey, 2019, 10). The multiplicity of subjectivities may thus become better 'protected'. However, struggles for security can also be carried out by the production of subjectivities that "represent the subjects in resistance" (ibid., 195). "[P]aying close attention to how people live the necessity for identity and security in their daily lives, and also how they resist some of the totalizing moves that inhere in their struggles" provide a way for examining security from another perspective (Stern, 2006, 202), which I have tried to do in this thesis as well.

Counter-conduct may call for radical freedom, for example, hacktivism, ignoring social media, abstaining from connectiveness, or refusing to conform to the use of applications and services and/or developing alternative ways of using them to serve one's values and interests. Counter-conduct is internal to modern governmentality but it indicates freedom within the prevailing governmental rationality and attempts to change it. Thus, freedom is to some extent present in all relations of power, including security dispositive. In Saul Tobias's (2005, 66) phrasing, freedom is "the utilization of the power which circulates in all relations […] and which is productive as much as it is constraining".

For Foucault, individual freedom requires ethical conduct indicating care for oneself, but also for others – also in cyber-physical societies. Ethics can hence be understood as an invitation to practice freedom; to expand the field of possibilities also within the dispositive of security (Tobias, 2005, 68). Pivotal to such conduct is autonomy, transgression and decision making from one's own starting points, which nonetheless become constructed in social interaction with others. Being able to care for oneself and others in such a manner could lead to security through other practices and possibly with another labelling.

Heavy responsibilisation, that it, setting the alternatives for one to choose from and calling for correct decisions, as well as for carrying out the consequences for those decisions, may not lead to improved security, but to mere rules following as Renaud et al. (2018) have argued. Maybe the path could be, instead, to support ethical life that also accommodates human erring, sinning, and inactivity? Not as subjects responsibilised for their own wellbeing and security, but as individuals and communities who conduct themselves ethically and strive for government that aligns with this ethicality. Not as self-reliant, entrepreneurial, observant, and resilient subjects willing to develop their capacities when a need arises and calling for their human and basic rights when social insurance and the respective support networks no longer exist. Scrapping of such support networks and turning them into networks of commercial service providers is facilitated by digitalisation in the name of widened individual freedom, but it mainly advances servitude to global, faceless, and seemingly unchallengeable 'market forces'.

According to Foucault (1982, 781), there are "three types of struggles: either against forms of domination (ethnic, social, and religious); against forms of exploitation which separate individuals from what they produce; or against that which ties the individual to himself and submits him to others in this way (struggles against subjection, against forms of subjectivity and submission)". Even if struggles against domination and exploitation have not disappeared, the struggle against the submission of subjectivity is becoming more important. (Ibid., 782.) As a consequence, there is a need “to imagine and to build up what we could be to get rid of this kind of political ‘double bind,’ which is the simultaneous individualisation and totalisation of modern power structures”. New forms of subjectivity ought to be promoted “through the refusal of [the] kind of individuality which has been imposed on us.” (Ibid., 785.)

In comparison, Jennifer Einspahr (2010), who investigates freedom from structural domination, calls for focusing on the relations in which subjects and, in particular, the positions they can occupy become produced. “[I]f freedom is essentially about what kinds of subjects we are, then freedom can all too easily be equated with ‘free will’, a feeling of being free, or an ‘internal’ state, while crucial questions about what kind of world we would like to share together go unasked” (ibid., 4). “[W]hen framed around the subject question, freedom is often conflated with agency”, even if “exercising agency is not indicative of one’s freedom” (ibid., 4, 6). Instead, freedom ought to be understood “as a structural concept that centres not on individuals but on their relative positions (as members of groups) vis-à-vis other individuals (as members of groups) and institutions” (ibid., 4). One could add ‘and in relation to other ‘things’ as well’. Einspahr (2010, 4) further claims that when freedom is conflated with agency, agency is confused “with resistance and resistance with freedom” (also Tobias, 2005, 69).

Moreover, both Einspahr (2010, 9) and Tobias (2005, 69) argue, by leaning on philosophical literature that has been referred to in human security as well, that thinking about individual freedom merely in terms of individual agency tends to be seen as incompatible with claims for societal equality and ignores an analysis of the conditions under which self-creation can take place. First, “’individuals’ and their ‘choices’ are [...] embedded in much larger contexts, [...] which raise doubts about our freedom regardless of how much or how little our chosen actions are impeded” (ibid., 9). Second, “[i]f we have little hope for attaining a goal, or if our living conditions make such a goal literally unimaginable, this ‘choice’ will never appear on our list of possibilities at all” (ibid., 9–10). Finally, “positions of vulnerability, dependence, or subjection [...] affect an individual’s ability to make a meaningful choice”, for example, “if one choice would likely result in safety or protection, and the other in danger or harm [...] the freeness of such choice is called into question” (ibid., 10). Foucault agrees on the importance of the positions that individuals occupy in networks of power relations, but encourages conduct that may become interpreted as dangerous and argues that where there is choice, there is freedom.

In sum, the partial societal failure in security production in and with regard to cyberspace due to the ignorance of some of the voices may provide “an opening for thinking security differently” (Stern, 2006, 189). In such an endeavour, the subjectivities of individuals need to be considered in their plurality instead of reducing them to mere consumers – more precisely, to the abstract category of an average consumer – taking care of their safety and security in cyberspace on the basis of their own self-interest and/or societal obligations. In Finnish Lapland, other subjectivities commonly accepted for individuals include, for example, resilient inhabitants serving as the first line of emergency response; exotic indigenous people with their unique cultures, livelihoods and knowledge; local hosts and guides for global tourism; and vulnerable rural residents and communities whose unfulfilled lives need to be improved via (digital) development. All of the aforementioned subjectivities incorporate a particular presence in cyberspace as well, but so do a number of other, less stereotypical subjectivities. Such presences are currently becoming accepted as one of the referent objects of cyber/digital security – not only in a human security approach but also on the Finnish agenda for digital security.

The general feature in the Arctic subjectivities, however, is that they produce individuals and communities both as dependent on external input and circulation and as expectedly self-assured human beings. The partial societal failure in security production in and with regard to cyberspace thus also manifests in the intensifying demands for personal, community, organisational, and national resilience in cyberspace. This duality resides in modern governmentality, but could become balanced differently through ethical reflection and modified self-techniques in the form of self-care. Such a transformation in the techniques of security still anchors change to individuals and communities, but not through submission but resistances. It also enables the construction of subjectivities that are based on speaking truth to power regardless of the risk of becoming considered dangerous. The question of whose security and freedom hence does not concern so much the different referent objects but the ethical self-definition of subjects.

4.2 The future of digitality?

While writing this thesis, the national cyber/digital security practices and arrangements in Finland have caught up with some of the initial critiques of the ECoHuCy project. For example, the individual is no longer left totally alone to ponder upon his or her security questions related to digitalisation, but guidance and advice is available in various formats and by different providers as discussed in this thesis. Unfortunately, much of this material is available online and hence does not reach people who do not know where to look it up, cannot do so, or are not interested. Nonetheless, it is a change: Contemporary practices increasingly address individuals' security concerns by informing them how to help themselves. In addition, in both Finland and the EU digitalisation and cyber/digital security are now addressed together, no longer on two separate agendas that may or may not overlap. This integration improves understanding of the effects of digitalisation and its securitisation on society and economy, but also on the everyday lives of individuals and communities. Furthermore, national institutional arrangements for cyber/digital security, many of which have been described in this thesis, have evolved and become strengthened since 2016.

Nonetheless, power relations between individuals, communities, corporations, states, and other organisations in and with regard to cyberspace remain asymmetrical. This can best be seen by seeking answer to the question of who is to be transparent in cyberspace. States, corporations, and hacker communities have the means to manage their transparency and deal with surveillance, whereas individuals still struggle to gain ownership of their data and self-determination. The state of affairs makes them vulnerable and often irritated. Simultaneously, they are expected to be responsible, that is, to behave in the correct, safe manner in and with regard to cyberspace. Yet, they have little influence, inter alia, on network architecture, algorithms and applications; political and/or economic decision-making on digitalisation and its securitisation; or where ICT corporations pay their taxes. Either because they lack the right kind of language or the position from which to speak. For a long period of time, the responsibility of ICT corporations included only financial accountability to their shareholders, but ethical, environmental, and political responsibilities are catching up. At last.

ICT and connectivity are still expected to improve efficiency and effectiveness of operation, as well as people's wellbeing. This is the motivation for their introduction, application and development in different contexts. However, they also decrease people's wellbeing which is the motivation for increasing regulation. The state seems to have been governing not enough, because people's experiences of, for example, data breaches, social engineering, scams, and service outages, but also difficulties in using ICT and/or digital services as well as unsolved cybercrime, have been eroding trust towards digitality. It has been noted that responsibilisation of individuals and communities without predictability concerning what is required of them in terms of knowledge and skills does not lead to cyber/digital security. Neither does constant surveillance, education and training, because people remain psychophysical entities who occasionally get tired, upset, absent-minded and/or choose to behave differently. Humanness should therefore be accepted and coded into cyber-physicality, not as an error but as a feature – at best, as a security feature. The human being sill outranks the programme in innovating and 'getting the gut feeling that something is not right'.

As a conclusion, securitisation of digitalisation seems to be partially failing. Circulation of information, or other 'things' which circulation now depends on digitalised infrastructure, cannot be protected, nor are people, organisations and states fully resilient towards unwanted circulation or occasional interruptions of circulation. Should they even be? They did not necessarily choose to be resilient and digisavvy citizens responsible for (national) cyber/digital security production. What cyber/digital security entails is relatively clear when it is anchored to information, critical infrastructure, or vital societal functions, but becomes blurrier and more fluid when its referent object is the everyday life of individuals and communities in all its multiplicity. Still, it is this everyday context that gives security its content and meaning.

A human security approach to cyber/digital security brings in a number of perspectives that are sidelined by the mainstream framings and, thus, provides a more complete picture of security problems. The quest for future cyber/digital security government then remains to accommodate what is dangerous in a manner that supports human freedom and accepts multiplicity. This requires continued development of security and other practices that try to reach the numerous, shifting diagrams of cyber-physical society. It requires enough contextualised information so that governing through working on the population's conditions of life becomes possible without as much focus on disciplinary techniques. The argument is a vicious circle for it is conditioned by individuals' and communities' willingness to provide information about themselves.

Cyber/digital security has not been and still is not a major regional issue in the Arctic. However, and on top of digital development, the Arctic governance bodies could discuss the topic under resilience, but have thus far chosen not to do so. The reasons for this silence can only be speculated, but given the importance of contextualisation in cyber/digital security problems, change in policy could lead to better regional solutions serving the interests of local people, communities and businesses. Instead of only applying national policies, the northernmost regions of Europe could investigate and build security form their own starting points – as it has been done, for example, with regard to digital health and social services to an extent. The challenge will remain in financing, but building unforced trust towards government closer to people's everyday life might be easier than towards multinational corporations or even the state that is increasingly digital, virtual and outsourced.

Digitalisation as a societal development in the Arctic – or anywhere else – will not be turned around. It is driven by such strong economic and governmental beliefs and practices built on those beliefs. Where digitalisation thrusts, cyber/digital security now follows. Therefore, it is not a clean, well-established compilation of security techniques, but an internally contradictory and quickly evolving wholeness, which continuously (re)produces itself and finds new manifestations. In this thesis, I have tried to elaborate on how cyber/digital security becomes accommodated in the ways of thinking, knowledge, and institutions that have been developed for the physical world but are now transformed and/or supplemented with the task of creating order in the digital sphere. Security practices themselves thus also enmesh and contribute to the evolvement of cyber-physicality. Simultaneous, they transmit the technical and strategic understandings of security to ever new areas of everyday life.

Bibliography

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

Aaltola, Mika, Fjäder, Christian, Innola, Eeva, Käpylä, Juha, & Mikkola, Harri (2016) Huoltovarmuus muutoksessa. Kansallisen varautumisen haasteet kansainvälisessä toimintaympäristössä. [Transforming Security of Supply. The Challenges of National Preparedness in International Operational Environment.] FIIA Report 49. Helsinki: The Finnish Institute of International Affairs. https://www.fiia.fi/wp-content/uploads/2017/04 /fiiareport49_huoltovarmuus_muutoksessa.pdf [March 26, 2021].

Abrahamsen, Rita, & Williams, Michael C. (2011) *Security Beyond State. Private Security in International Relations.* Cambridge: Cambridge University Press.

Aiken, Mary (2016) *The Cyber Effect*. London: John Murray Publishers.

Ahonen, Pasi et al. (2017) KYBER-TEO – tuloksia 2014–2016. Julkisten tulosten kooste. [KYBER-TEO – results 2014–2016. Compilation of public results.] VTT Technology 298. Espoo: VTT. https://www.vttresearch.com/sites/default/files/pdf/technology/2017/T298.pdf [July 27, 2021].

Alhanen, Kai (2007) *Käytännöt ja ajattelu Michel Foucault'n filosofiassa* [Practices and thinking in Michel Foucault's philosophy]. Helsinki: Gaudeamus.

Alshaikh, Moneer (2020) Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security* 98, 102003. https://doi.org/10.1016/j.cose.2020.102003.

Ani, Uchenna Daniel, He, Hongmei, & Tiwari, Ashutosh (2019) Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology* 21(1), 2–35. https://doi.org/10.1108/JSIT-02-2018-0028.

Anttila, Ulla (2012) *Enhancing human security through crisis management – opportunities and challenges for learning.* (Doctoral dissertation) National Defence University, Department of Leadership and Military Pedagogy, Publication series 1, No. 9/2012. Helsinki: National Defence University. http://urn.fi/URN:ISBN:978-951-25-2357-3.

Anwar, Modh, Hu, We, Ash, Ivan, Yuan, Xiaohong, Li, Ling, & Xu, Li (2017) Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior* 69, 437–443. https://doi.org/10.1016/j.chb.2016.12.040.

Aradau, Claudia (2010) Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 41(5), 491–514. https://doi.org/10.1177/0967010610382687.

Arctic Council (2016) Arctic Resilience Report. Carson, Marcus, & Peterson, Gerry (Eds). Stockholm: Stockholm Environment Institute and Stockholm Resilience Centre. http://www.arctic-council.org/arr [August 27, 2021].

Arctic Council (2017) Arctic Resilience Action Framework. Cooperating for a More Resilient and Prosperous Arctic Region. May 2017. https://oaarchive.arctic-council.org/bitstream/handle/11374/2019/EDOCS-4248-v4-Arctic-Resilience-Action-Framework-after-New-York-SAO-2017.pdf?sequence=7&isAllowed=y [April 27, 2021].

Arctic Council (2020) Virtual Arctic Resilience Forum Launches in October. September 21, 2020. https://arctic-council.org/en/news/virtual-arctic-resilience-forum-launches-in-october/.

Arctic Council (n/d) Arctic Resilience Action Framework (ARAF). https://sdwg.org/what-we-do/projects/arctic-resilience-action-framework-araf/ [April 27, 2021].

Arctic Economic Council (AEC) (2017) Arctic Broadband – Recommendations for and Interconnected Arctic. https://arcticeconomiccouncil.com/wp-content/uploads/2017/03/AEC-Report_Final-LR.pdf [October 12, 2020].

Arctic Economic Council (AEC) (2018) AEC Connectivity Working Group: Mandate. https://arcticeconomiccouncil.com/wp-content/uploads/2018/11/Connectivity-WG-Mandate-FINAL.pdf [October 12, 2020].

Ball, Stephen H., & Olmedo, Antonio (2013) Care of the self, resistance and subjectivity under neoliberal governmentalities. *Critical Studies in Education* 54(1), 85–96. http://dx.doi.org/10.1080/17508487.2013.740678.

Barlow, John Perry (1996) A Declaration of the Independence of Cyberspace. https://www.eff.org/cyberspace-independence [March 28, 2021].

Barnard-Wills, David, & Ashenden, Debi (2012) Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture* 15(2), 110–123. https://doi.org/10.1177/1206331211430016.

Barnard-Wills, David, & Wells, Helen (2012) Surveillance, technology and the everyday. *Criminology & Criminal Justice* 12(3), 227–237. https://doi.org/10.1177/1748895812446644.

Betz, David J., & Stevens, Tim (2013) Analogical reasoning and cyber security. *Security Dialogue* 44(2), 147–164. https://doi.org/10.1177/0967010613478323.

Bhat, P. Ishwara (2019) *Ideas and Methods of Legal Research.* New Delhi: Oxford University Press.

Bologna, Sandro, Lazari, Alessandro, & Mele, Stefano (2015) Improving Critical Infrastructure Protection and Resilience against Terrorism Cyber Threats. In: Čaleta, Denis, & Radosevic, Vesela (Eds.) *Comprehensive Approach as "Sine Qua Non" for Critical Infrastructure Protection.* Amsterdam: IOS Press, 79–90. https://doi.org/10.3233/978-1-61499-478-7-79.

Booth, Ken (2007) *Theory of World Security*. Cambridge: Cambridge University Press.

Booth, Ken, & Wheeler, Nicholas J. (2007) *The Security Dilemma: Fear, Cooperation and Trust in World Politics*. Basingstoke: Palgrave Macmillan.

Bourne, Mike (2014) *Understanding Security*. Basingstoke: Palgrave Macmillan.

Brase, Gary L., Vasserman, Eugene Y., & Hsu, William (2017) Do Different Mental Models Influence Cybersecurity Behavior? Evaluations via Statistical Reasoning Performance. *Frontiers in Psychology* 8, 1929. https://doi.org/10.3389/fpsyg.2017.01929.

Brennen, Scott, & Kreiss, Daniel (2014) Digitization and Digitalization. Culture Digitally (group blog). https://culturedigitally.org/2014/09/digitalization-and-digitization/.

Bubandt, Nils (2005) Vernacular Security: The Politics of Feeling Safe in Global, National and Local Worlds. *Security Dialogue* 36(3), 275–296. https://doi.org/10.1177.0967010605057015.

Buchanan, Ben (2016) *The Cybersecurity Dilemma. Hacking, Trust, and Fear between Nations.* London: C. Hurst & Co.

Bussolini, Jeffrey (2010) What is a Dispositive? *Foucault Studies* 10, 85–107. https://doi.org/10.22439/fs.v0i10.3120.

Buzan, Barry, Wæver, Ole, & de Wilde, Jaap (1998) *Security: A New Framework for Analysis*. Boulder (CO): Lynne Rienner.

Callewaert, Staf (2017) Foucault's Concept of Dispositif. *Praktiske Grunde. Nordisk tidsskrift for kultur- og samfundsvidenskab* 1–2, 29–52. http://praktiskegrunde.dk/2017/praktiskegrunde(2017-1+2f)callewaert.pdf.

Castells, Manuel (2010) *The Rise of the Network Society*. 2nd edition. The Information Age: Economy, Society, and Culture Vol. 1. Chichester: Wiley-Blackwell.

Catlaw, Thomas J., & Sandberg, Billie (2018) The Quantified Self and the Evolution of Neoliberal Self-Government: An Exploratory Qualitative Study. *Administrative Theory & Praxis* 40(1), 3–22. https://doi.org/10.1080/10841806.2017.1420743.

Ceesay, E. N., Myers, K., & Watters, P. A. (2018) Human-centered strategies for cyber-physical systems security. *EAI Endorsed Transactions on Security and Safety* 4(14), 1–10. https://doi.org/10.4108/eai.15-5-2018.154773.

de Certeau, Michel (1988) *The Practice of Everyday Life*. English translation by Steven Rendall. Berkeley (CA): University of California Press.

Chandler, David, & Reid, Julian (2016) *The Neoliberal Subject. Resilience, Adaptation and Vulnerability*. London: Rowman & Littlefield.

Chong, Isis, Xiong, Aiping, & Proctor, Robert W. (2019) Human Factors in the Privacy and Security of the Internet of Things. *Ergonomics in Design* 27(3), 5–10. https://doi.org/10.1177/1064804617750321.

Choucri, Nazli, Madnick, Stuart, & Koepke, Priscilla (2018) Institutions for Cybersecurity: International Responses and Data Sharing Initiatives. In: Shrobe, Howard, Shrier, David L., & Pentland, Alex (Eds.) *New Solutions for Cybersecurity*. Cambridge (MA): MIT Press, 11–79.

Chowdhury, Noman H., Adam, Marc T. P., & Teubner, Tim (2020) Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security* 97, 101963. https://doi.org/10.1016/j.cose.2020.101963.

Churruca Muguruza, Cristina (2017[2007]) Human Security as a policy framework: Critics and Challenges. *Deusto Journal of Human Rights* 4, 15–35. https://doi.org/10.18543/aahdh-4-2007pp15-35.

Clark, Robert M., & Hakim, Simon (2017) Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security. In: Clark, Robert M., & Hakim, Simon (Eds.) *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level.* Cham: Springer, 1–17.

Coaffee, Jon, & Fussey, Pete (2015) Constructing resilience through security and surveillance: The politics, practices and tensions of security-drive resilience. *Security Dialogue* 46(1), 86–105. https://doi.org/10.1177.0967010614557884.

Coburn, Andrew, Leverett, Éireann, & Woo, Gordon (2018) *Solving Cyber Risk: Protecting Your Company and Society*. Hoboken (NJ): John Wiley & Sons.

Czarniawska, Barbara (2004) *Narratives in Social Research*. London: Sage.

Danielsson, Petri, & Näsi, Matti (2019) Suomalaiset väkivallan ja omaisuusrikosten kohteena 2018 – Kansallisen rikosuhritutkimuksen tuloksia. [Violent Crimes and Property Offences in 2018 in Finland – Results of National Crime Victim Study.] Institute of Criminology and Legal Policy, Briefs 35/2019. Helsinki: University of Helsinki. https://helda.helsinki.fi/bitstream/handle/10138/305388/Katsauksia_35_%20Danielsson_N%c3%a4si_2019.pdf?sequence=4&isAllowed=y [April 9, 2021].

Davidson, Arnold I. (2011) In praise of counter-conduct. *History of the Human Sciences* 24(4), 25–14. https://doi.org/10.1177/0952695111411625.

Dean, Mitchell (2008[1999]) *Governmentality. Power and Rule in Modern Society*. London: SAGE Publications Ltd.

Dean, Mitchell, & Villadsen, Kaspar (2016) *State Phobia and Civil Society. The Political Legacy of Michel Foucault.* Stanford (CS): Stanford University Press.

Declaration of MyData Principles (n/d) https://mydata.org/declaration/ [March 26, 2022].

Deibert, Ronald J. (2018) Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs* 32(4), 411–424. https://doi.org/10.1017/S0892679418000618.

Deleuze, Gilles (1999[1986]) *Foucault.* Translated and edited by Seán Hand. London: Continuum.

Deleuze, Gilles (2006) What Is a Dispositif? In: Deleuze, Gilles; Lapoujade, David (Ed.) *Two Regimes of Madness. Texts and Interviews 1975–1995.* Translated to English by Ames Hodges and Mike Taormina. New York (NY): Semiotext(e), 338–348.

Demchak, Chris C. (2012) Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI). *Journal of Comparative Policy Analysis: Research and Practice* 14(3), 254–269. https://doi.org/10.1080/13876988.2012.687619.

Deseriis, Marco (2013) Is Anonymous a New Form of Luddism? A Comparative Analysis of Industrial Machine Breaking, Computer Hacking, and Related Rhetorical Strategies. *Radical History Review* 117, 33–48. https://doi.org/10.1215/01636545-2210437.

Digital and Population Services Agency (DVV) (n/da) Digiturvallinen elämä. [Digitally Secure Life.] Online training site. https://dvv.fi/digiturvallinen-elama [October 21, 2020].

Digital and Population Services Agency (DVV) (n/db) Digituki. [Digital Support.] https://dvv.fi/digituki [December 16, 2020].

Digital and Population Services Agency (DVV) (2020) Digituen alueellinen kehittäminen jatkuu kattavasti Suomessa [The regional development of digital support continues extensively in Finland.] Press release, October 21, 2020. https://dvv.fi/-/digituen-alueellinen-kehittaminen-jatkuu-kattavasti-suomessa [December 16, 2020].

van Dijck, José (2013) *The Culture of Connectivity. A Critical History of Social Media*. New York (NY): Oxford University Press.

Dillon, Michael, & Logo-Guerrero, Luis (2008) Biopolitics of security in the 21st century: an introduction. *Review of International Studies* 34, 265–292. https://doi.org/10.1017/S0260210508008024.

DiMase, Daniel, Collier, Zachary A., Heffner, Kenneth, & Linkov, Igor (2015) Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions* 35, 291–300. https://doi-org.ezproxy.ulapland.fi/10.1007/s10669-015-9540-y.

Domscheit-Berg, Daniel (2011) *WikiLeaks. Sisäpiirin salaisuudet*. [Inside WikiLeaks: My time with Julian Assange at the world's most dangerous website.] Finnish translation by Pirkko Roinila and Veera Kaski. Helsinki: Kustannusosakeyhtiö Tammi.

Duffield, Mark (2007) *Development, Security and Unending War. Governing the World of Peoples.* Cambridge: Polity Press.

Duffield, Mark (2010) The Liberal Way of Development and the Development-Security Impasse: Exploring the Global Life-Chance Divide. *Security Dialogue* 41(1), 53–76. https://doi.org/10.1177/0967010609357042.

Dunn Cavelty, Myriam (2014) Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics* 20(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y.

Dunn Cavelty, Myriam, Kaufmann, Mareile, & Kristensen, Kristian Søby (2015) Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue* 46(1), 3–14. https://doi.org/10.1177/0967010614559637.

Dunn Cavelty, Myriam, & Wenger, Andreas (2020) Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy* 41(1), 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Egloff, Florian J. (2020) Public attribution of cyber intrusions. *Journal of Cybersecurity* 6(1), 1–12. https://doi.org/10.1093/cybsec/tyaa012.

Einspahr, Jennifer (2010) Structural Domination and Structural Freedom: A Feminist Perspective. *Feminist Review* 94(1), 1–19. https://doi.org/10.1057/fr.2009.40.

Eisenberg, Daniel, Seager, Thomas, & Alderson, David L. (2019) Rethinking Resilience Analytics. Perspective. *Risk Analysis* 39(9), 1870–1884. https://doi.org/10.1111/risa.13328.

European Union Agency for Cybersecurity (ENISA) (2020) ENISA Threat Landscape 2020. Threat reports. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Findikaattori.fi (2020) Maanpuolustustahto 1970–2020 [The Will to Defend One's Nation], December 14, 2020. https://findikaattori.fi/fi/77.

Finnemore, Martha, & Hollis, Duncan B. (2016) Constructing Norms for Global Cybersecurity. *The American Journal of International Law* 110(3), 425–479.

Flyberbom, Mikkel (2015) Sunlight in cyberspace? On transparency as a form of ordering. *European Journal of Social Theory* 18(2), 168–184. https://doi.org/10.1177/1368431014555258.

Foucault, Michel (1977) Le jeu de Michel Foucault. Dits Ecrits tome III texte n° 206. Entretien avec D. Colas, A. Grosrichard, G. Le Gaufey, J. Livi, G. Miller, J. Miller, J.-A. Miller, C. Millot, G. Wajeman. *Ornicar?, Bulletin Périodique du champ freudien* 10, 62–93. http://1libertaire.free.fr/MFoucault158.html.

Foucault, Michel (1980[1977]) The Confession of the Flesh. A conversation with Alain Grosrichard, Gerard Wajeman, Jaques-Alain Miller, Guy Le Gaufey, Dominique Colas, Gerard Miller, Catherine Millot, Jocelyne Livi and Judith Miller. In: Gordon, Colin (Ed.) *Power/Knowledge. Selected Interviews and Other Writings 1972–1977*. Translated into English by Colin Gordon, Leo Marshall, John Mepham and Kate Soper. Pantheon Books: New York (NY).

Foucault, Michel (1982) The Subject and Power. *Critical Inquiry* 8(4), 777–795.

Foucault, Michel (1991[1975]) *Discipline and Punish. The Birth of the Prison*. London: Penguin Books.

Foucault, Michel (1994[1966]) *The Order of Things. An Archaeology of the Human Sciences*. New York (NY): Random House.

Foucault, Michel (1998[1976]) *The Will to Knowledge. The History of Sexuality: 1*. Penguin Books: London.

Foucault, Michel (2006[1961]) *History of Madness*. Translated into English by Jonathan Murphy and Jean Khalfa. London: Routledge.

Foucault, Michel (2009a[1969]) *The Archaeology of Knowledge*. Translated into English by A. M. Sheridan Smith. Abingdon: Routledge.

Foucault, Michel (2009b) *Security, Territory, Population. Lectures at the Collège de France 1977–78*. Edited by Michel Senellart, translated into English by Graham Burchell. Basingstoke: Palgrave Macmillan.

Foucault, Michel (2010) *The Birth of Biopolitics. Lectures at the Collège de France 1978–79*. Edited by Michel Senellart, translated into English by Graham Burchell. Basingstoke: Palgrave Macmillan.

Foucault, Michel (2014[1994]) Parhaat. [The Best Of.] Translated into Finnish by Tapani Kilpeläinen, Simo Määttä and Johan L. Pii. Tampere: Eurooppalaisen filosofian seura ry.

Gaia Consulting (2018) Report of the 1st Arctic Resilience Forum 10-11 September 2018 in Rovaniemi, Finland. https://oaarchive.arctic-council.org/bitstream/handle/11374/2379/Arctic-Resilience-Forum-Final-Report-_-2018.pdf?sequence=1&isAllowed=y [April 27, 2018].

Galtung, Johan (1969) Violence, Peace and Peace Research. *Journal of Peace Research* 6(3), 167–191. https://www.jstor.org/stable/422690.

Gilliam, Andrew R., & Foster, G. Tad (2020) Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior* 108, 106319. https://doi.org/10.1016/j.chb.2020.106319.

Gisladottir, Viktoria, Ganin, Alexander A., Keisler, Jeffrey M., Kepner, Jeremy, & Linkov, Igor (2017) Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis* 37(9), 1644–1651. https://doi.org/10.1111/risa.12729.

Gordon, Colin (1991) Governmental Rationality: An Introduction. In: Burchell, Graham, Gordon, Colin, & Miller, Peter (Eds.) *The Foucault Effect. Studies in Governmentality*. Chicago (IL): The University of Chicago Press, 1–51.

Government of Iceland (2019) Together Towards a Sustainable Arctic. Iceland's Arctic Council Chairmanship 2019–21. https://www.government.is/library/01-Ministries/Ministry-for-Foreign-Affairs/PDF-skjol/Arctic%20Council%20-%20Iceland's%20Chairmanship%20 2019-2021.pdf [October 19, 2020].

Government Resolution on Comprehensive Security, 5.12.2012. https://www.defmin.fi/files/3023/Periaatepaatos_kokonaisturvallisuudesta_2012_fi.pdf.

Government Resolution on Security of Supply 1048/2018, 18.12.2018. https://www.finlex.fi/fi/laki/alkup/2018/20181048.

Greenstein, Shane M. (2015) *How the Internet became commercial: innovation, privatization, and the birth of a new network.* Princeton (NJ): Princeton University Press.

Gulbrandsen, Kristin Smette, & Sheehan, Michael (2020) Social Exclusion as Human Insecurity: A Human Cybersecurity Framework Applied to the European High North. In: Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (Eds.) *Digitalisation and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North.* Cham: Palgrave Macmillan, 113–140.

Helén, Ilpo (2016) *Elämän politiikat. Yhteiskuntatutkimus Foucault'n jälkeen. [Politics of life. Social sciences after Foucault.]* Helsinki: Tutkijaliitto.

Henman, Paul (2013) Governmentalities of Gov 2.0. *Information, Communication & Society* 16(9), 1397–1418. https://doi.org/10.1080/1369118X.2012.706314.

Heusala, Anna-Liisa (2011) Kokonaisturvallisuus ja inhimillinen turvallisuus yhteiskuntatieteellisessä tutkimuksessa [Comprehensive security and human security in social scientific research]. *Tiede ja ase* 69, 96–111.

Hildebrandt, Mireille (2013) Balance or Trade-Off? Online Security Technologies and Fundamental Rights. *Philosophy and Technology* 26(4), 357–379. https://doi.org/ 10.1007/s13347-013-0104-0.

Hokkanen, Julius, Soronen, Anne, Talvitie-Lamberg, Karoliina, & Valtonen, Sanna (2021) Haavoittuvuuden kudelmat. Digitaalinen subjekti ja haavoittuvuus datavetoista yhteiskuntaa käsittelevässä tutkimuskirjallisuudessa. [Weaves of vulnerability. Digital subject and vulnerability in research literature on datafied society.] *Media ja viestintä* 44(2), 69–90. https://doi.org/10.23983/mv.109860.

Homolar, Alexandra (2015) Human security benchmarks: Governing human wellbeing at a distance. *Review of International Studies* 41, 843–863. https://doi.org/10.1017/S0260210515000352.

Hoogensen Gjørv, Gunhild (2012) Security by any other name: negative security, positive security, and a multi-actor security approach. *Review of International Studies* 38(4), 835–859. https://doi.org/10.1017/S0260210511000751.

Hudson, Heather E. (2015) *Connecting Alaskans. Telecommunications in Alaska from Telegraph to Broadband.* Fairbanks: University of Alaska Press.

Huysmans, Jef (2016) Democratic curiosity in times of surveillance. *European Journal of International Security* 1(1), 73–93. https://doi.org/10.1017/eis.2015.2.

Hyvärinen, Matti (2006) Kerronnallinen tutkimus. [Narrative research.] Pdf -file, published on the author's internet site in February 2006. http://www.hyvarinen.infor/material/Hyvarinen-Kerronnallinen_tutkimus.pdf [March 28, 2010]. The site is no longer active.

Hyvärinen, Matti (2009) Narrative Analysis. Pdf -file, published on the author's internet site on January 27, 2009. http://www.hyvarinen.info/material/Hyvarinen-Narrative_Analysis.pdf [March 28, 2010]. The site is no longer active.

IBM (2022) X-Force Threat Intelligence Index 2022. https://www.ibm.com/security/data-breach/threat-intelligence/ [March 23, 2022].

The Intelligence Ombudsman (n/d). Oversight of Intelligence. https://tiedusteluvalvonta.fi/en/oversight-of-intelligence [February 23, 2022].

Jackson, Norman, & Carter, Pippa (1998) Labour as Dressage. In: McKinlay, Alan, & Starkey, Ken (Eds.) *Foucault, Management and Organization Theory: From Panoptic on to Technologies of Self.* London: SAGE Publications, 49–64. http://dx.doi.org/10.4135/9781446221686.n4.

Jarvis, Lee (2019) Toward a Vernacular Security Studies: Origins, Interlocutors, Contributions, and Challenges. *International Studies Review* 21(1), 107–126. https://doi.org/10.1093/isr/viy017.

Kangas, Urpo (1982) *Lesken oikeudellinen asema: oikeusdogmaattinen tutkimus lesken sosiaaliturvan laajuudesta.* [The legal status of widow: A judicial dogmatic study on the scope of widow's social security.] (Doctoral dissertation) Lakimiessarja A N:o 158. Helsinki: Suomalainen lakimiesyhdistys.

Kaisto, Jani, & Pyykkönen, Miikka (2015) Johdanto. Hallinnan analytiikan suuntaviivoja. [Introduction. Guidelines of the analytics of government.] In: Kaisto, Jani, & Pyykkönen, Miikka (Eds.) *Hallintavalta. Sosiaalisen, politiikan ja talouden kysymyksiä.* [Governmentality. Questions of the social, the political and the economy.] Helsinki: Gaudeamus, 7–24.

Kansaopistot (n/d) What is a folk high school. https://en.kansanopistot.fi/frontpage/what-is-a-folk-high-school/ [March 26, 2022].

Kaufmann, Mareile (2015) Resilience 2.0: social media use and (self-)care during the 2011 Norway attacks. *Media, Culture & Society* 37(7), 972–987. https://doi.org/10.1177/0163443715584101.

Kennison, Shelia M., & Chan-Tin, Eric (2020) Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology* 11, 546546. https://doi.org/10.3389/fpsyg.2020.546546.

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

King, Gary, & Murray, Christopher J. L. (2001) Rethinking Human Security. *Political Science Quarterly* 116(4), 585–610. https://doi.org/10.2307/798222.

Kiravuo, Timo, & Särelä, Mikko (2013) The Care and Maintenance of Cyberweapons. In: Rantapelkonen, Jari, & Salminen, Mirva (Eds.) *The Fog of Cyber Defence.* Helsinki: National Defence University, 231–243. http://urn.fi/URN:ISBN:978-951-25-2431-0.

Koivunen, Erka (2013) Contaminated Rather than Classified: CIS Design Principles to Support Cyber Incident Response Collaboration. In: Rantapelkonen, Jari, & Salminen, Mirva (Eds.) *The Fog of Cyber Defence.* Helsinki: National Defence University, 145–153. http://urn.fi/URN:ISBN:978-951-25-2431-0.

Koopman, Colin (2013) *Genealogy as Critique: Foucault and the Problems of Modernity.* Bloomington (IN): Indiana University Press.

Krahmann, Elke (2010) *States, Citizens and the Privatisation of Security.* Cambridge: Cambridge University Press.

Kshetri, Nir (2020) The evolution of cyber-insurance industry and market: An institutional analysis. *Telecommunications Policy* 44(8), 1–14. https://doi.org/10.1016/j.telpol.2020.102007.

Laitinen, Joonas, & Keski-Heikkilä, Anni (October 19, 2020) Nokia rakentaa Kuuhun kaikkien aikojen ensimmäisen mobiiliverkon (news article). Helsingin Sanomat. https://www.hs.fi/talous/art-2000006674471.html [October 19, 2020].

Lanier, Jaron (2010) *You Are Not a Gadget.* A Manifesto. New York (NY): Alfred A. Knopf.

Lapland Hospital District (2007) From Technological Initialization to the Development of Services 2001–2007. Rovaniemi: Lapland Hospital District.

Lapland Hospital District, Länsipohja Healthcare District, The Regional Council of Lapland, & Centre of Expertise on Social Welfare in Northern Finland (2011) UULA. New services and operational models in Lapland 2008–2011. Rovaniemi: Lapland Hospital District.

Lapland Hospital District, Länsipohja Healthcare District, The Regional Council of Lapland, & Centre of Expertise on Social Welfare in Northern Finland (2016) Lapin SoTe Digitalisaation Tiekartta 2020. [Roadmap of the digitalisation of social security and health services in Lapland towards 2020.] http://www.sosiaalikollega.fi/teknologia/lapin-sotedigitalisaation-tiekartta-2020.

Lehto, Martti, Limnéll, Jarno, Innola, Eeva, Pöyhönen, Jouni, Rusi, Tarja, & Salminen, Mirva (2017) Finland's cyber security: the present state, vision and the actions needed to achieve the vision. Publications of the Government's analysis, assessment and research activities 30/2017. Prime Minister's Office: Helsinki.

Lehto, Martti, Limnéll, Jarno, Kokkomäki, Tuomas, Pöyhönen, Jouni, & Salminen, Mirva (2018) Strategic management of cybersecurity in Finland. Publications of the Government's analysis, assessment and research activities 28/2018. Prime Minister's Office: Helsinki.

Lehto, Martti, Hummelholm, Aarne, Iida, Katsoyoshi, Jakstas, Tadas, Kari, Martti J., Minami, Hiroyuki, Ohnishi, Fujio, & Saunavaara, Juha (2019) Arctic Connect Project and Cyber Security Control, ARCY. Informaatioteknologian tiedekunnan julkaisuja [Publications of the Faculty of Information Technology.] No. 78/2019. University of Jyväskylä. https://jyx.jyu.fi/bitstream/handle/123456789/63655/978-951-39-7721-4.pdf?sequence=1&isAllowed=y.

Lehtonen, Turo-Kimmo, & Liukko, Jyri (2010) Justifications for commodified security: the promotion of private life insurance in Finland 1945–90. *Acta Sociologica* 53(4), 371–386.

Lemke, Thomas (2015) New Materialisms: Foucault and the 'Government of Things'. *Theory, Culture and Society* 32(4), 3–25. https://doi.org/10.1177/0263276413519340.

Lessig, Lawrence (1999) *Code and Other Laws of Cyberspace*. New York (NY): Basic Books.

Lewis, Ted G. (2015) *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Hoboken (NJ): John Wiley and Sons, Inc.

Li, Ling, He, Wu, Xu, Li, Ash, Ivan, Anwar, Mohd, & Yuan, Xiaohong (2019) Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management* 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Limnéll, Jarno, Majewski, Klaus, & Salminen, Mirva (2014) *Kyberturvallisuus. [Cybersecurity]* Jyväskylä: Docendo.

Lin, Patrick, & Allhoff, Fritz (2019) Arctic 2.0: How Artificial Intelligence Can Help Develop a Frontier. *Ethics & International Affairs* 33(2), 193–205. https://doi.org/10.1017/S0892679419000108.

Lockheed Martin (n/d) The Cyber Kill Chain (web resource). https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Macmillan, Alexandre (2011) Michel Foucault's Techniques of the Self and the Christian Politics of Obedience. *Theory, Culture & Society* 28(4), 3–25. https://doi.org/10.1177/0263276411405348.

Martin, Mary, & Owen, Taylor (2010) The Second Generation of Human Security. Lessons from the UN and EU experience. *International Affairs*, 86(1), 211–224. https://doi.org/10.1111/j.1468-2346.2010.00876.x.

McCluskey, Emma (2019) *From Righteousness to Far Right. An Anthropological Rethinking of Critical Security Studies.* Montreal & Kingston: McGill-Queen's University Press.

Medby, Ingrid A. (2019) Language-games, geography, and making sense of the Arctic. *Geoforum* 107, 124–133. https://doi.org/10.1016/j.geoforum.2019.10.003.

Mikkonen, Minttu (February 27, 2018) Nokia aikoo rakentaa ensimmäisen 4g-verkon Kuuhun – "Meidän pitää oppia kommunikoimaan avaruudessa" (news article). Helsingin Sanomat. https://www.hs.fi/ulkomaat/art-2000005584769.html [October 19, 2020].

Mikkonen, Riikka (August 28, 2017) Tiedustelulaki: kohti massavalvontaa? [Intelligence law: towards mass surveillance?] Blog entry for Electronic Frontier Finland (Effi), https://effi.org/blog-2017-08-28-Riikka-Mikkonen/ [March 3, 2021].

Ministry of Defence (2010) Security Strategy for Society. Government Resolution 16.12.2010. https://www.defmin.fi/files/1883/PDF.SecurityStrategy.pdf [March 25, 2021].

Ministry of Defence (2016) Suomen puolustuksen teknologisen ja teollisen perustan turvaaminen. [Securing the technological and industrial base of national defence in Finland]. Government Resolution. http://urn.fi/URN:ISBN:978-951-25-2771-7 [March 26, 2021].

Ministry of Finance of Finland (2018) Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma. [Development Programme for Digital Security in Public Administration.] Ministry of Finance publications 32/2018. http://urn.fi/URN:ISBN:978-952-251-975-7.

Ministry of Finance of Finland (2019) Päätös [Decision] 21.11.2019. Valtiovarainministeriön päätös avustuksesta kuntien digitalisaation edistämiseen. [Decision of the Ministry of Finance on public assistance for the advancement of municipalities digitalistion.] https://vm.fi/documents/10623/12045794/Valtiovarainministeri%C3%B6n+p%C3%A4%C3%A4t%C3%B6s+avustuksesta+kuntien+digitalisaation+edist%C3%A4miseen.pdf/4bc0f697-f53e-efe5-40f8-9f781f116e77/Valtiovarainministeri%C3%B6n+p%C3%A4%C3%A4t%C3%B6s+avustuksesta+kuntien+digitalisaation+edist%C3%A4miseen.pdf [February 16, 2021].

Ministry of Finance of Finland (2020a) Digitalisaation edistämisen ohjelma 2020–2023. Toimintasuunnitelma 2020. [Programme to advance digitalisation in the society. Action Plan.] https://vm.fi/documents/10623/1464506/Digitalisaation+edist%C3%A4misen+ohjelman+toimintasuunnitelma/5cd124e3-ec59-2fcb-79e0-a501f7ec404c/Digitalisaation+edist%C3%A4misen+ohjelman+toimintasuunnitelma.pdf [February 2, 2021].

Ministry of Finance of Finland (2020b) Digital security in public sector. Publications of the Ministry of Finance 2020:23. http://urn.fi/URN:ISBN:978-952-287-857-1 [October 20, 2020].

Ministry of Finance of Finland (2020c) Kartoitus kuntien digitaalisista palveluista. [A survey on the digital services of Finnish municipalities.] Final report 24.4.2020. https://vm.fi/documents/10623/306832/Kuntien+digikartoituksen+raportti/e2cce3b9-251a-e834-1482-53b9d5b5b962/Kuntien+digikartoituksen+raportti.pdf [February 15, 2021].

Ministry of Finance of Finland (2020d) Valtiovarainministeriö on myöntänyt vuoden 2020 avustukset kuntien digitalisaatiohankkeisiin. [Ministry of Finance granted public assistance to municipalities' 2020 digitalisation projects.] Press release, December 11, 2020. https://vm.fi/-/valtiovarainministerio-on-myontanyt-vuoden-2020-avustukset-kuntien-digitalisaatiohankkeisiin [February 16, 2021].

Ministry of Foreign Affairs of Finland (2017) Exploring Common Solutions. Finland's Chairmanship Program for the Arctic Council 2017–19. https://um.fi/documents/35732/0/Finland%27s%20Chairmanship%20Program%20for%20the%20Arctic%20Council%20%281%29.pdf/b13cda82-7b03-df0a-f86b-1d3e06b8041f?t=1533205711183 [October 19, 2020].

Ministry of Justice (n/d) Vartijoiden ja järjestyksenvalvojien käyttö on lisääntynyt. [The use of private guards and security guards has increased.] https://intermin.fi/poliisiasiat/vartiointi-ja-jarjestyksenvalvonta [March 19, 2021].

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

Ministry of the Interior (2017) Tietoverkkorikollisuuden torjuntaa koskeva selvitys. [Report on combatting cybercrime.] Sisäministerion julkaisu 14/2017. [Publication of the Ministry of the Interior 14/2017.] https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf?sequence=1 [March 23, 2022].

Ministry of Transport and Communications (2021) Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti. [Improving information security and data protection in the critical sectors of society. Working group final report.] Publications of the Ministry of Transport and Communications 2021:1. http://urn.fi/URN:ISBN:978-952-243-614-6 [July 27, 2021].

Morozov, Evgeny (2013) *To Save Everything, Click Here. The Folly of Technological Solutionism.* New York (NY): PublicAffairs.

Mueller, Milton (2017) *Will the Internet Fragment?* Cambridge: Polity Press.

Mäkinen, Juha (2010) Educating Soldiers and Security Sector Actors for Human Security-Oriented Activities. *Tiede ja ase* 68, 63–77.

National Cyber Security Centre (NSCS-FI) (n/d) https://www.kyberturvallisuuskeskus.fi/en/.

National Emergency Supply Agency (NESA) (n/da) Huoltovarmuuden historiaa. [History of security of supply.] https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/huoltovarmuuden-historia [March 26, 2021].

National Emergency Supply Agency (NESA) (n/db) Sektorit ja poolit. [Sectors and pools.] https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit [July 27, 2021].

National Emergency Supply Agency (NESA) (2021a) Kyber2020 -ohjelma. [Cyber 2020 programme.] Final report. https://www.huoltovarmuuskeskus.fi/files/f648900490855488126353b3e6f9bcfafea36467/2.kyber-2020-loppuraportti.pdf [July 23, 2021].

National Emergency Supply Agency (NESA) (2021b) Digitaalinen turvallisuus 2030. [Digital Security 2030.] Description of the programme. https://www.huoltovarmuuskeskus.fi/files/ed3e9dfe08bc05dbe6317a126e2cc80c7778a4b0/2.dt2030-ohjelman-kuvaus.pdf [July 23, 2021].

Nortio, Jukka (2019) Tiedustelulait muuttavat oikeuskäytäntöä. [Intelligence laws change judicial practice.] (news article) Lakimiesuutiset 17.6.2019, https://lakimiesuutiset.fi/tiedustelulait-muuttavat-oikeuskaytantoa/ [March 3, 2021].

Nye, Joseph S. Jr. (2011) *The Future of Power*. New York (NY): Public Affairs.

Nygård, Mikael (2015) Hyvinvointivaltiosta kilpailuvaltioon? [From a welfare state to a competition state?]. In: Autto, Janne, & Nygård, Mikael (Eds.) *Hyvinvointivaltion kulttuurintutkimus. [Cultural studies of welfare state.]* Rovaniemi: Lapin yliopistokustannus, 136–166.

Odysseos, Louiza (2010) Human Rights, Liberal Ontogenesis and Freedom: Producing a Subject for Neoliberalism? *Millennium* 38(3), 747–772. https://doi.org/10.1177/0305829810364876.

OECD (2015) Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document. https://www.oecd.org/digital/digital-security-risk-management.htm [October 10, 2020].

Olsén-Ljetoff, Laura, & Hokkanen, Liisa (2020) The Interconnection Between Digitalisation and Human Security in the Lives of Sámi with Disabilities. In: Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (Eds.) *Digitalisation and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North.* Cham: Palgrave Macmillan, 295–322.

Paananen, Rauli (2021) Kyberturvallisuuden kehittämisohjelma. [Cyber Security Development Programme.] Publications of the Ministry of Transport and Communications 2021:7. http://urn.fi/URN:ISBN:978-952-243-599-6 [July 23, 2021].

Panagia, Davide (2019) On the Political Ontology of the *Dispositif. Critical Inquiry* 45(3), 714–746. https://doi.org/10.1086/702613.

The Parliament of Finland (2019). Tiedustelulait. [Intelligence laws.] Information kit on the legal project, May 9, 2019. https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/ aineistot/kotimainen_oikeus/LATI/Sivut/tiedustelulait.aspx [March 3, 2021].

The Parliament of Finland (n/d). Intelligence Oversight Committee. https://www.eduskunta.fi/EN/valiokunnat/tiedusteluvalvontavaliokunta/Pages/default.aspx [February 23, 2022].

Peltonen, Matti (2008) Mikä on dispositiivi? [What is a dispositive?] *Tieteessä tapahtuu* 26(7), 75–77. https://journal.fi/tt/article/view/701.

Petrenko, Sergei (2019) *Cyber Resilience*. Gistrup: River Publishers.

Prokkola, Eeva-Kaisa (2018) Rajan turvallistaminen ja poikkeustilan arjen geopolitiikka. Tornion kaupunki maahantulon reittinä syksyllä 2015. [Securitisation of the border and geopolitics of the everyday of the state of exception. The town of Tornio as an immigration route in autumn 2015.] *Alue ja ympäristö* 47(1), 3–16.

Pupavac, Vanessa (2010) The Consumerism–Development–Security Nexus. *Security Dialogue* 41(6), 691–713. https://doi.org/10.1177/0967010610388204.

Päläs, Jenna (2022) *Oikeusasema jakamistalouden hyödykesopimuksissa. Tutkimus vallasta, subjektiuksista sekä oikeuden ja sosiaalisen välisestä etääntymisestä.* (Doctoral dissertation) University of Lapland, Acta electronica Universitatis Lapponiensis 340. Rovaniemi: University of Lapland.

Päläs, Jenna, & Salminen, Mirva (2019) Alustan asiakkaan vastuusta ja vastuuttamisesta yksilöturvallisuuden tuottamisessa – sopimusoikeudellinen näkökulma kyberturvallisuuteen jakamistaloudessa. [Responsibility and responsibilisation of the platform user in the production of individual security – A contract law perspective to cybersecurity in sharing economy.] In: Päläs, Jenna, & Määttä, Kalle (Eds.), *Jakamistalousjuridiikan käsikirja [Handbook of Sharing Economy and Law]*. Helsinki: Alma Talent, 319–380.

Raffnsøe, Sverre (2008) Qu'est-ce qu'un dispositif? L'analytique sociale de Michel Foucault. *Symposium*. Canadian Journal of Continental Philosophy / Revue canadienne de philosophie continentale 12(1), 44–66.

Raffnsøe, Sverre, Gudmand-Høyer, Marius, & Thaning, Morten S. (2016) Foucault's dispositive: The perspicacity of dispositive analytics in organizational research. *Organization* 23(2), 272–298. https://doi.org/10.1177/1350508414549885.

Rajavuori, Mikko, & Huhta, Kaisa (2020) Digitalization of security in the energy sector: evolution of EU law and policy. *Journal of World Energy Law and Business* 13, 353–367. https://doi.org/10.1093/jwelb/jwaa030.

Rautiainen, Janne (2018) Yhteiskunta 2030+ Suomen kriisinkestävyys. [Society 2030+ Resilience in Finland.] In: Rantapelkonen, Jari (Ed.) *Tuleva sota III – Tulevaisuuden sodan tulevaisuus [Future war III – The future of future warfare.]* Helsinki: Edita / National Defence University, 19–41. http://urn.fi/URN:ISBN:978-951-25-3017-5.

The Regional Council of Lapland (2013) Lapin digiohjelma 2020. [The digitalisation programme for Lapland 2020.] https://www.lapinliitto.fi/wp-content/uploads/2020/12/Lapin-Digiohjelma-2020.pdf [February 28, 2021].

Renaud, Karen, & Flowerday, Stephen (2017) Contemplating human-centred security & privacy research: Suggesting future directions. *Journal of Information Security and Applications* 34(1), 76–81. https://doi.org/10.1016/j.jisa.2017.05.006.

Renaud, Karen, Flowerday, Stephen, Warketin, Merrill, Cockshott, Paul, & Oregon, Craig (2018) Is the responsibilization of the cyber security risk reasonable and judicious? *Computers & Security* 78, 198–211.

Richmond, Oliver P. (2011) Post-colonial hybridity and the return of human security. In: Chandler, David, & Hynek, Nik (Eds.) *Critical Perspectives on Human Security. Rethinking Emancipation and Power in International Relations*. Abingdon: Routledge, 43–55.

Rid, Thomas, & Buchanan, Ben (2015) Attributing Cyber Attacks. *Journal of Strategic Studies* 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382.

Salminen, Mirva (2010) *Struggle over outsourcing of the security functions of the state: The case of September 16, 2007 shooting in Baghdad*. M. Soc. Sc. thesis. Tampere: University of Tampere.

Salminen, Mirva (2018a) Digital security in the Barents region. In: Hossain, Kamrul, & Cambou, Dorothée (Eds.) *Society, Environment and Human Security in the Arctic Barents Region.* Abingdon: Routledge, 187–204.

Salminen, Mirva (2018b) Kyber-fyysinen sota 2030+ Yhteiskuntien kompleksisuus tuottaa yllätyksiä sodankäyntiin. [Cyber-physical war 2030+ The complexity of societies generates surprises in warfare.] In: Rantapelkonen, Jari (Ed.) *Tuleva sota III – Tulevaisuuden sodan tulevaisuus [Future war III – The future of future warfare.]* Helsinki: Edita / National Defence University, 197–226. http://urn.fi/URN:ISBN:978-951-25-3017-5.

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.

Salminen, Mirva (2021) Arkipäivän digitaalinen turvallisuus Euroopan pohjoisilla alueilla: tapaustutkimus Tunturi-Lapista. [Everyday digital security in the European High North: A case study from Fjeld Lapland.] *Media ja viestintä* 44(1), 158–180. https://doi.org/10.23983/mv.107305.

Salminen, Mirva, & Hossain, Kamrul (2018) Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North. *Polar Record* 54(2), 108–118. https://doi.org/10.1017/S0032247418000268.

Salminen, Mirva, & Kerttunen, Mika (2020) The becoming of cyber military capabilities. In: Tikk, Eneken, & Kerttunen, Mika (Eds.) *Routledge Handbook of International Cybersecurity*. London: Routledge, 94–107.

Salminen, Mirva, & Päläs, Jenna (2021) The COVID-19 induced societal digital leap: incorporating a legal view in the responsibilisation of individuals for cybersecurity. In: Kirchner, S. (Ed.) *Governing the Crisis: Law, Human Rights and COVID-19*. Münster: LIT Verlag, 36–64.

Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (2020a) *Digitalisation and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North.* Cham: Palgrave Macmillan.

Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (2020b) Comprehensive Cybersecurity and Human Rights in the Digitalising European High North. In: Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (Eds.) *Digitalisation and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North.* Cham: Palgrave Macmillan, 21–55.

Salminen, Pertti (2021) Kokonaismaanpuolustuksen alkutaipaleella. [The first decades of comprehensive defence.] In: Liimatta, Hannu (Ed.) *Pääesikunta 100 vuotta.* [Defence Command Finland 100 Years.] Tampere: PunaMusta Media Oyj, 145–158.

Sannikka, Marja, & Nykänen, Petra (January 22, 2021) Resurssipula vaivaa poliisia – rikosoikeuden professori: Erittäin suuri osa rikoksista jää tutkimatta. [The Police suffers from a lack of resources – Professor of Criminal Law: A significant share of crimes remains uninvestigated.] (article) YLE News. https://yle.fi/uutiset/3-11751534 [March 23,2022].

Saraste, Anna (September 22, 2017) Valmisteilla oleva tiedustelulaki lupaa turvaa terrorismilta mutta vie Suomea kohti massavalvontaa. [Intelligence legislation in preparation promises security from terrorism, but takes Finland towards mass surveillance.] (article) The Ulkopolitist (an independent online journal for international relations). https://ulkopolitist.fi/2017/09/22/valmisteilla-oleva-tiedustelulaki-lupaa-turvaa-terrorismilta-mutta-vie-suomea-kohti-massavalvontaa/ [March 3, 2021].

Saunavaara, Juha, Kylli, Ritva, & Salminen, Mirva (2021) Telecommunication Line Infrastructure and the Arctic Environment: Past, Present and Future. *Polar Record* 57(e8), 1–12. https://doi.org/10.1017/S0032247421000036.

Schebesta, Hanna, & Purnhagen, Kai Peter (2019) An Average Consumer Concept of Bits and Pieces: Empirical Evidence of the Court of Justice of the European Union's Concept of the Average Consumer in the UCPD. In: de Almeida, Lucila, Cantero Gamito, Marta, Djurovic, Mateja, & Purnhagen, Kai Peter (Eds.) *The Transformation of Economic Law. Essays in Honour of Hans-W. Micklitz.* Oxford: Hart Publishing, 13–27.

The Security Committee (2013) Finland's Cyber Security Strategy. Government Resolution 24.1.2013. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

The Security Committee (2014) Kansallisen kyberturvallisuusstrategian toimeenpano-ohjelma 11.3.2014. [Implementation programme of the national cybersecurity strategy 11.3.2014.] https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf [March 22, 2022].

The Security Committee (2017a) Security Strategy for Society. Government Resolution 2.11.2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english. pdf.

The Security Committee (2017b) Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020. [Implementation Programme for Finland's Cyber Security Strategy for 2017–2020.] https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf [March 22, 2022.]

The Security Committee (2019) Finland's Cyber Security Strategy 2019. Government Resolution 3.10.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf.

The Security and Defence Committee (2006) The Strategy for Securing the Functions Vital to Society. Government Resolution 23.11.2006. https://www.defmin.fi/files/858/06_12_12_YETTS__in_english.pdf [March 25, 2021].

Setola, Roberto, Luiijf, Eric, & Theocharidou, Marianthi (2016) Critical Infrastructures, Protection and Resilience. In: Setola, Roberto, Rosato, Vittorio, Kyriakides, Elias, & Rome, Erich (Eds.) *Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach.* Studies in Systems, Decision and Control. Vol 90. Cham: Springer, 1–18.

Shackelford, Scott J. (2019) Should Cybersecurity Be a Human Right? Exploring the 'Shared Responsibility' of Cyber Peace. *Stanford Journal of International Law* 55(2), 155–184.

Sharp, Greg (2019) The Arctic of Myth. Article on the Arctic Institute's website, Aug 13, 2019. https://www.thearcticinstitute.org/arctic-myth/.

Sheringham, Michael (2006) *Everyday Life. Theories and Practices from Surrealism to the Present.* Oxford: Oxford University Press.

Shishaev, Maxim, Fedorov, Andrey, & Datyev, Igor (2020) Analysis of Online Social Networking When Studying the Identities of Local Communities. In: Salminen, Mirva, Zojer, Gerald, & Hossain, Kamrul (Eds.) *Digitalisation and Human Security. A Multi-Disciplinary Approach to Cybersecurity in the European High North.* Cham: Palgrave Macmillan, 267–293.

Siltaoja, Marjo, Malin, Virpi, & Pyykkönen, Miikka (2015) 'We are all responsible now': Governmentality and responsibilized subjects in corporate social responsibility. *Management Learning* 46(4), 444–460. https://doi.org/10.1177/1350507614541199.

Stalla-Bourdillon, Sophie (2014) Privacy Versus Security… Are We Done Yet? In: Stalla-Bourdillon, Sophie, Phillips, Joshua, & Ryan, Mark D. (Eds.) *Privacy vs. Security.* Springer Briefs in Cybersecurity. London: Springer, 1–90.

Stephen, Kathrin (January 11, 2012) Holy Grail or Next Cold War? Metaphors for Describing the Arctic. Article on the Arctic Institute's website. https://www.thearcticinstitute.org/holy-grail-next-cold-war/ [August 3, 2021].

Stern, Maria (2006) 'We' the Subject: The Power and Failure of (In)Security. *Security Dialogue* 37(2), 187–205. https://doi.org/10.1177/0967010606066171.

Stern, Maria, & Öjendal, Joakim (2010) Mapping the Security-Development Nexus: Conflict, Complexity, Cacophony, Convergence? *Security Dialogue* 41(1), 5–30. https://doi.org/10.1177/0967010609357041.

Stevens, Daniel, & Vaughan-Williams, Nick (2016) *Everyday Security Threats: Perceptions, Experiences, and Consequences.* Manchester: Manchester University Press.

Taddeo, Mariarosaria (2013) Cyber Security and Individual Rights, Striking the Right Balance. *Philosophy and Technology* 26(4), 353–356. https://doi.org/ 10.1007/s13347-013-0140-9.

Tadjbakhsh, Shahrbanou (2014) Human security twenty years on. Expert Analysis, June 2014. The Norwegian Peacebuilding Resource Centre (NOREF). https://www.files.ethz.ch/isn/181368/540cb240aa84ac7133bce008adcde01f.pdf.

Tadjbakhsh, Shahrbanou, & Chenoy, Anuradha (2009[2007]) *Human Security: Concepts and Implications.* Abingdon: Routledge.

Task Force on Telecommunications Infrastructure in the Arctic (TFTIA) (2015) Meeting 1 Summary by Co-chairs (Norway, Kingdom of Denmark). https://oaarchive.arctic-council.org/handle/11374/1664 [October 12, 2020].

Task Force on Telecommunications Infrastructure in the Arctic (TFTIA) (2017) Telecommunications Infrastructure in the Arctic: A Circumpolar Assessment. https://oaarchive.arctic-council.org/handle/11374/1924 [October 12, 2020].

Tobias, Saul (2005) Foucault on Freedom and Capabilities. *Theory, Culture and Society* 22(4), 65–85. https://doi.org/10.1177/0263276405053721.

Trump, Benjamin D., Hossain, Kamrul, & Linkov, Igor (Eds.) (2020) *Governance for Cyber Security and Resilience in the Arctic.* NATO Science for Peace and Security Series – D: Information and Communication Security, No. 58. Amsterdam: IOS Press.

Tuckness, Alex, & Wolf, Clark (2017) *This is Political Philosophy. An Introduction*. Malden (MA): John Wiley & Sons, Inc.

Turner, Mandy, Cooper, Neil, & Pugh, Michael (2011) Institutionalised and co-opted. Why human security has lost its way. In: Chandler, David, & Hynek, Nik (Eds.) *Critical Perspectives on Human Security. Rethinking Emancipation and Power in International Relations*. Abingdon: Routledge, 83–96.

The United Nations Development Programme (UNDP) Human Development Report 1994. New York (NY)/Oxford: Oxford University Press. http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf [June 21, 2021].

The United States Department of State (2015) One Arctic: Shared Opportunities, Challenges and Responsibilities. U.S. Chairmanship of the Arctic Council 2015–17. https://2009-2017.state.gov/e/oes/ocns/opa/arc/uschair/index.htm [October 19, 2020].

Valtonen, Vesa, & Branders, Minna (2021) Tracing the Finnish Comprehensive Security Model. In: Larsson, Sebastian, & Rhinard, Mark (Eds.) *Nordic Societal Security. Convergence and Divergence.* London: Routledge, 91–108. https://doi.org/10.4324/9781003045533.

Vaughan-Williams, Nick, & Stevens, Daniel (2016) Vernacular theories of everyday (in)security: The disruptive potential of non-elite knowledge. *Security Dialogue* 47(1), 40–58. https://doi.org/10.1177/0967010615604101.

Villadsen, Kaspar (2021) 'The Dispositive': Foucault's Concept for Organizational Analysis? *Organization Studies* 42(3), 473–494. https://doi.org/10.1177/0170840619883664.

Virtu Service Point Manual (n/d) https://lapitoy.sharepoint.com/sites/Virtu-tiedostomateriaali/Jaetut%20asiakirjat/Tuotantoymp%C3%A4rist%C3%B6n%20tiedostomateriaali/virtu/S%C3%A4hk%C3%B6iset%20asiointipaikat/ohjeet26112018_EN.pdf [March 26, 2022].

Wallenstein, Sven-Olov (2013) Introduction: Foucault, Biopolitics, and Governmentality. In: Nilsson, Jakob, & Wallenstein, Sven-Olov (Eds.) *Foucault, Biopolitics, and Governmentality*. Södertörn Philosophical Studies 14. Huddinge: Södertörn University, 7–34.

Walters, William (2012) *Governmentality. Critical Encounters*. Abingdon: Routledge.

Whelan, Glen (2019) Born Political: A Dispositive Analysis of Google and Copyright. *Business & Society* 58(1), 42–73. https://doi.org/10.1177/0007650317717701.

Wiatrowski, Aleksander (2021) *Abuses of Dominant ICT Companies in the Area of Data Protection.* (Doctoral dissertation) University of Lapland, Acta electronica Universitatis Lapponiensis 307. Rovaniemi: University of Lapland. http://urn.fi/URN:ISBN:978-952-337-259-7.

Wolfers, Arnold (1952) "National Security" as an Ambiguous Symbol. *Political Science Quarterly* 67(4): 481–502. https://doi.org/10.2307/2145138.

Workman, Michael, Phelps, Daniel C., & Gathegi, John N. (2013) *Information Security for Managers.* Burlington (MA): Jones & Bartlett Learning.

Wæver, Ole (1995) Securitization and Desecuritization. In: Ronnie D. Lipschutz (Ed.) *On Security*. New York (NY): Columbia University Press, 46–84.

White, Hayden (1975) *Metahistory. The Historical Imagination in Nineteenth-Century Europe.* Baltimore (MD): The Johns Hopkins University Press.

Zebrowski, Chris (2016) *The Value of Resilience. Securing Life in the Twenty-First Century*. Abingdon: Routledge.

Zimmermann, Verena, & Renaud, Karen (2019) Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies* 131, 169–187.

Zojer, Gerald (2019a) The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens. *The Yearbook of Polar Law* X, 297–320. https://doi.org/10.1163/22116427_010010014.

Zojer, Gerald (2019b) Free and open source software as a contribution to digital security in the Arctic. *Arctic Yearbook 2019*. https://arcticyearbook.com/arctic-yearbook/2019/2019-scholarly-papers/312-free-and-open-source-software-as-a-contribution-to-digital-security-in-the-arctic [October 20, 2020].

Zou, Bo, Choobchian, Pooria, & Rozenberg, Julie (2021) Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies. *Journal of Transportation Security*. https://doi.org/10.1007/s12198-021-00230-w.