1 Introduction

Gerald Zojer

Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland

In the 21st century, the concept of cybersecurity has risen on the agendas of state administrations, (trans/inter)national organisations and corporations. This is due to rapidly advancing digitalisation, which is the process of the digital transformation of our societies. Business, public administration and societal functions are increasingly handled through digital technologies and information and communication technologies (ICTs), which are interconnected in cyberspace. At the same time, the process of digitalisation has advanced to an extent that a functioning society has become dependent on undisrupted cyberspace and ICTs. However, digital technologies are vulnerable, and technical failures, connectivity problems, human abuse or error can cause interruption of services. In order to address such challenges, information security and cybersecurity frameworks have been developed. When the infrastructure of an entire society is threatened, the question of security shifts from the individual or organisational level to the state level. Consequently, most countries have developed cybersecurity strategies to safeguard their cyber infrastructure. The concept of cybersecurity has remarkable visibility in contemporary security literature. Much of it addresses negative security: threats to be mitigated by applying specific measures, such as to protect critical infrastructure from cybercrime,

cyberwarfare, hacktivism or espionage. At the individual level, cybersecurity deals with data protection or privacy. However, the everyday life experiences of individuals or communities interacting with digitalisation also leads to new insecurities and challenges, such as the creation of social exclusion, disappearance of physical services or impacts on local culture. Mainstream approaches to cybersecurity fail to address these security challenges at the individual or community level. Moreover, they tend to treat society at the national level somewhat homogeneously, ignoring the differences and peculiarities between regions within states.

The impacts of digitalisation can also be observed in the northernmost parts of Finland (Lapland), Norway (Troms and Finnmark) and Sweden (Norbotten) – or the European High North (EHN). In the European Commission's 2019 Digital Economic and Society Index, Finland, Norway and Sweden ranked in the top five performing countries. However, the way digitalisation impacts societal development differs depending on the region. The socio-economic and environmental peculiarities of the EHN makes the region distinct from the more southern parts of these countries. The EHN is a peripheral region with a low population density, less developed infrastructure and harsh climate with long and dark winters, and in the rural areas especially, it is shaped by traditional economic activities, such as reindeer herding or fishing. Moreover, the EHN is also the homeland of the Sámi, an Indigenous people consisting of several small language groups. These particularities create a set of features that make the impact of digitalisation in the region distinct.

This book represents a synthesis of the work conducted within the three-year research project ***E****nablement besides* ***Co****nstraints:* ***Hu****man Security and*

*a **Cy**ber Multi-Disciplinary Framework in the European High North* (ECoHuCy). The aim was to design a multidisciplinary, comparative research framework to address human security questions related to the dis-/integrating effects of digitalisation and the increasing importance of cybersecurity. It constructs a research agenda suited for the purposes of policy makers, regulators and academia alike, as well as giving the citizens and communities of the EHN a voice in matters related to cybersecurity. It questions the mainstream conceptualisation of cybersecurity and instead reconstructs it with the human as the referent object of security. By utilising the human security concept, the project establishes a human-centred cybersecurity framework. This theoretical work has been accompanied and supported by several empirical case studies.

In order to develop this novel framework, the project work was divided into four substantial work packages. This book summarises these work packages, with each chapter representing the results of one project work package. It is worth noting that due to the interdisciplinary approach to the overarching theme, many deliverables of the project fit into more than one work package.

Chapter 2, 'Theorizing Security: Human Security Perspective on Cyber Security', summarises the theoretical framework that was developed during the project. It concentrates on the theoretical development of a human security perspective on cybersecurity. It begins with an analysis of the national cybersecurity discourse as established in the countries of the EHN. Then, it discusses the commonalities and shortcomings of these strategies, before elaborating the human security discourse and how it is related to digitalisation in the EHN. The chapter closes with a deconstruction of the

mainstream cybersecurity discourse and presents a human-centred cybersecurity perspective based on the human security concept.

Chapter 3, ‘Citizen and Civil Society Perspectives on Cyberspace in the European High North’, draws attention to the effects cyberspace and ICTs have on citizens in the EHN, with a particular focus on Northern Norway. It brings forth empirical evidence of the benefits and constraints arising from digitalisation for non-profit civil society organisations. It suggests that digitalisation has significant impacts on civil society, but that it neither enhances nor constrains civil society.

Chapter 4, ‘ICT Access and Use Among Elderly People in the European High North’, presents empirical findings on how digitalisation and access to ICTs affects elderly people in the EHN. It shows the dichotomy of how digitalisation can increase access to services for some but create new accessibility challenges for other community members, for example, due to a lack of digital skills, physical impairments or absence of services in local languages. The chapter furthermore discusses how younger family members have become an important resource for elderly members when using digital services.

Chapter 5, ‘Climate Change, Environmental Threats and Cybersecurity in the European High North’, establishes the interconnection between global environmental governance and cybersecurity as well as between the environmental liability regime and the cybersecurity regime. It elaborates how the climatic conditions in the EHN create extra criticality to infrastructure. The chapter examines the interactions, pros and cons of

different categories of regulatory instrument mixes and how they are connected to collateral governance issues and human security.