# 6 Conclusions

Gerald Zojer

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

Digitalisation is rapidly changing our societies, and the relatively peripheral areas of northernmost Finland, Norway and Sweden – the European High North (EHN) – have likewise been affected. This region is the homeland of the Sámi, an Indigenous people with several languages. For the EHN – which is sparsely populated, has a less developed infrastructure (health services, information and communication technologies [ICTs], etc.) than in the more southern parts of these countries and which is characterised by a harsh climate – digitalisation offers numerous benefits. As a result of the digitalisation policies of the EHN countries, digitalisation is already relatively advanced. The motif for advancing digital technologies and ICTs is to increase efficiency of existing services and activities and to promote (new) business opportunities. However, digitalisation also creates new challenges to people's everyday lives. While some of the enabling and constraining effects of digitalisation are similar to those in other regions, the peculiarities of the EHN also lead to a distinct set of opportunities and challenges.

For instance, digitalisation of public services can reduce time and resources spent on travel by making services available in remote places. However, this is often accompanied by cutbacks to physical services. Digitalisation can allow people to live, study and work in peripheral areas such as the EHN. However, not everyone wants, can access or is able to use ICTs as required in order benefit from digital (public) services. Thus, digitalisation may create new insecurities or exclusion for some people. ICTs and cyberspace also affect citizens and civil society organisations. The adoption of these technologies has led to instrumental changes in how non-governmental and non-profit organisations operate. Yet, the emergence of cyberspace has both enhancing and constraining effects, and the use of cyberspace has not profoundly altered the terms of the relative power of one type of civil society over another. In other words, digitalisation neither democratises nor undemocratises societies. Digital technologies not only play an ever-increasing role in public administration and personal life, but other core infrastructures also depend heavily on ICTs, such as water or energy supply. The EHN climatic conditions as well as human-induced climate change pose risks to these infrastructures and cybersecurity. Uninterrupted operation of these infrastructures is necessary for human wellbeing.

Digitalisation in the EHN states has been pushed by national and regional policies, and the rapid adoption of digital technologies and ICTs has made societies more dependent on the uninterrupted supply of these services. However, ICTs are vulnerable, and their operation is challenged by connectivity problems, technical malfunctions, human abuse and error as well as hostile interests. Consequently, information security and cybersecurity frameworks have been established in order to address these challenges. When the ICT infrastructure of an entire state is challenged, the question of security is shifted to the national level. The countries of the EHN have endorsed cybersecurity strategies to address such threats. Their aim is to protect critical infrastructure from adverse events. Indeed, the reliability of these infrastructures has become important for the functioning of contemporary societies. However, in the end these technologies should serve a prospering development of humankind. Thus, the aim of cybersecurity must first be to safeguard human wellbeing in a digitalising world. Mainstream cybersecurity approaches, however, fail to address the negative impacts of digitalisation, as these approaches are somewhat techno-determinist, assuming that digital technologies benefit society and that safeguarding their functioning automatically serves societal wellbeing. However, such an understanding fails to acknowledge that digitalisation contains both enabling and constraining effects. Mainstream cybersecurity understanding falls short of addressing challenges and threats that people experience in their everyday lives and that originate from the dispersion of digital technologies. Therefore, cybersecurity needs to be conceptualised in a more comprehensive manner that includes the societal impacts of cyberspace, ICTs and digitalisation and that also considers its effects at the individual and sub-state community levels.

The results of the ***E**nablement besides **Co**nstraints: **Hu**man Security and a **Cy**ber Multi-Disciplinary Framework in the European High North* (ECoHuCy) research project, which are summarised in this synthesis report, show that integrating a human security approach can be inclusive to traditional cybersecurity concerns and the everyday life experiences of people in their region-specific context. This human-centred cybersecurity approach shifts the human into the focus of security concerns and considers both the enabling and constraining effects of digitalisation. This comprehensive cybersecurity framework can be applied as a tool in order to create meaningful and targeted policies that address both the positive and negative impacts of digitalisation while at the same time having the flexibility to consider regional peculiarities.