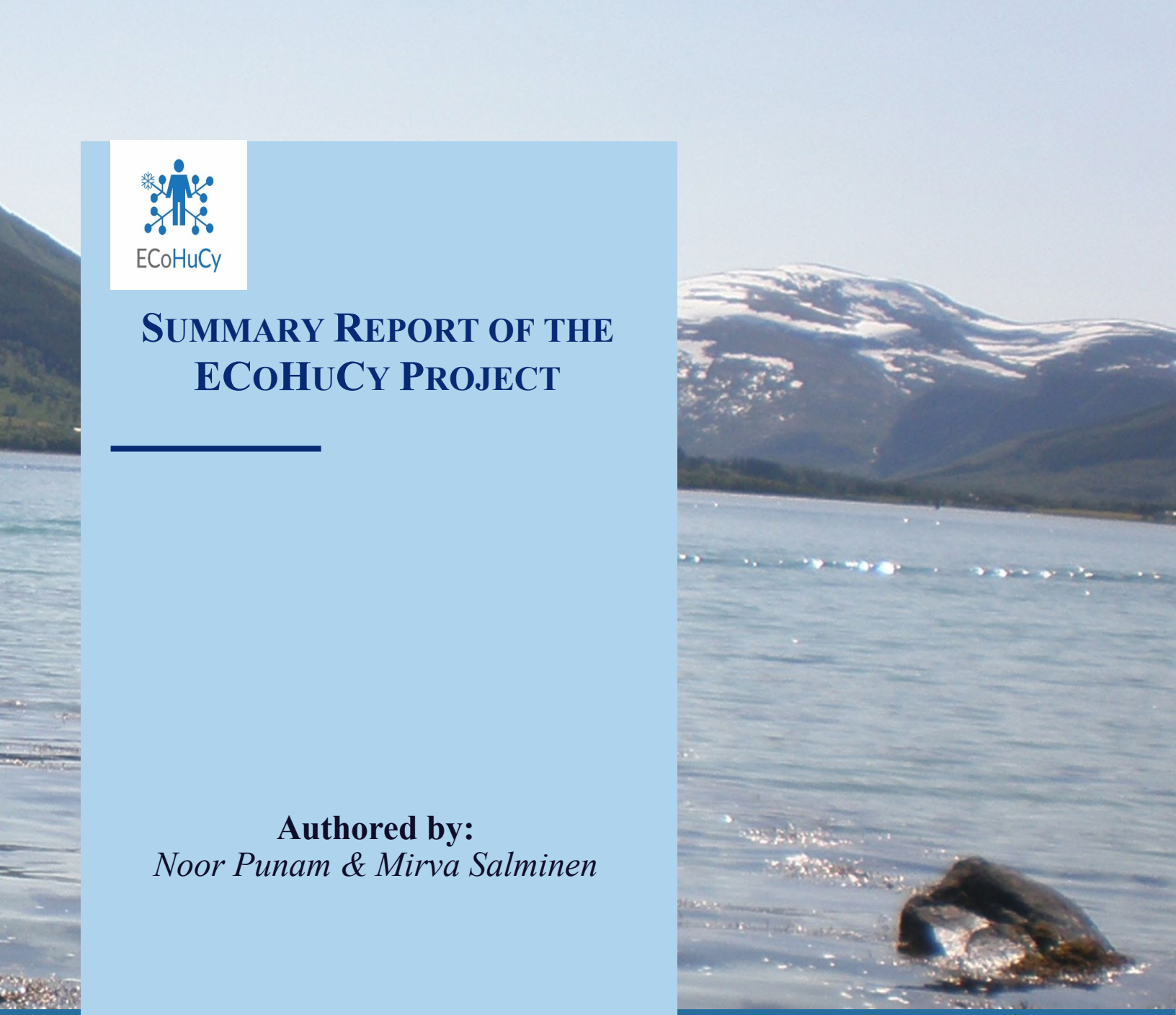

SUMMARY REPORT OF THE ECOHUCY PROJECT

Authored by:
Noor Punam & Mirva Salminen

Background

The digitalisation of society affects human lives in diverse ways. Along with the new possibilities that it brings, there are also threats and problems to be addressed. These include a lack of necessary digital skills and a lack of cybersecurity awareness. Cybersecurity involves the protection of cyberspace, cyber-enabled systems, and the data they contain from unauthorised access. In addition, it provides protection against physical attacks and social engineering, that is, the psychological manipulation of people into disclosing confidential information or taking actions. States, international organisations, corporations and other organisations have generally incorporated cybersecurity into their security policies. However, a comprehensive understanding of how cybersecurity relates to individuals and communities is still lacking. The security of many aspects of human life are affected, both positively and negatively, by digitalisation. Such aspects include health, economy, community, food, personal life, politics and the environment. However, cybersecurity strategies primarily focus on ensuring the smooth functioning of society and the economy, whereas the effects on individuals depend on the success or failure of these measures. The three-year research project 'Enablement Besides Constraints: Human Security and a Cyber Multi-Disciplinary Framework in the European High North (ECoHuCy)' explored digitalisation and cybersecurity through the lens of human security, in the particular context of the European High North (EHN). This region has been exposed to digital transformations which have aimed to promote efficient and effective services for its population, and to provide a more efficient operating format for businesses. These transformations have occurred across services like education, banking, healthcare, social services and retail. The region encompasses remote areas and population centres in the northernmost parts of Finland, Sweden and Norway, which share a number of common characteristics. These characteristics include a delicate relationship between the natural environment and human activity, a sparse and ageing population, limited infrastructure, harsh climate, vast land area and a vulnerability to environmental threats. The concept of human security has been applied to widen and deepen the mainstream understanding of cybersecurity, so that it may respond better to the challenges specific to the region. The project demonstrated that the concept of human security can provide a comprehensive analytical structure for assessing the impact of digital trends and developments on the well-being of individuals and communities. It assessed digitalisation and cybersecurity by considering both opportunities (positive security) and threats (negative security) that affect individuals and communities living in the EHN. It involved four work packages that focused on the following themes:

WP1: Theorising human security in the context of cybersecurity
WP2: Citizen and civil-society perspectives on cyberspace in the EHN
WP3: Social exclusion and internet access in the EHN
WP4: Climate change, environmental threats and cybersecurity in the EHN

Research focus

Work Package 1 concentrated on the development of a theoretical framework for looking at cybersecurity from the perspective of human security. In this work package, digitalisation and cybersecurity were studied together, and the conclusion was reached that national security cannot be the sole objective of cybersecurity policy. Particular consideration was given to the regional challenges generated by digitalisation in people's everyday lives, which national cybersecurity frameworks tend to overlook. As such, the work package recommended that there should be increased cooperation between the three countries regarding digitalisation and cybersecurity. Additionally, Work Package 1 highlighted the necessity to supplement the existing state-centric and technology-centric understandings of cybersecurity with a human-centric perspective. A human security approach allows the transformation of cybersecurity measures so that individuals and communities can be included within their scope.

People and communities should not be treated merely as sources of information in the development of measures related to digitalisation, but should be involved in the decision-making process. The application of a human security perspective to cybersecurity can provide this additional input by identifying the population's needs, interests and fears, as well as the challenges it faces as a result of digitalisation in everyday life. This approach can be utilised as a policy-making instrument to promote human well-being.

Work Package 2 focused on cyberspace as both an opportunity and a threat in community, regional and cross-border contexts, with a particular focus on the local communities and civil society organisations in Northern Norway. Civil society in this context, is deemed to have a dual relation with the state. It acts as an organised counterweight to the state and one can also assume the positive effects of civil association for upholding democracy. It can be seen as an important component in establishing the society/state relationship, which defines the socio-political system of any modern nation. Civil society in the region is affected by a number of cybersecurity policies. Digitalisation has brought about noteworthy changes in Norwegian civil society, but it has not contributed to any intrinsic transformation of that society. It cannot be argued that digitalisation has either contributed to an erosion of democracy or to an enhancement of it in Norway. It does not seem to have significantly shifted the balance between various aspects of civil society or transformed the relationship between society and the state. For local communities, the development of digital venues in the EHN has opened up opportunities for the creation of some new businesses and sources of income. At the same time, some traditional businesses or local shops have gone out of business. Digitalisation has transformed the way communication takes place in Northern Norway amongst local communities, civil society organisations and local authorities. It can be said that it has had a positive impact on communication methods, which has helped to overcome the constraints of large geographical distances.

Work Package 3 examined social exclusion resulting from digitalisation. It focused especially on children, the elderly and minorities. Whilst digitalisation has, on the whole, been beneficial for the EHN, for example enabling people to live, work and study from a distance, difficulties relating to the use of digital services do exist for certain groups. There is an assumption amongst skilled users that everyone wants, can access and has the competency to use digital services. In reality, there is a digital divide resulting from a variation in skills and access. For many elderly people, it is easy to access platforms like Facebook, but more complex to navigate platforms like online banking and municipal online services. Accordingly, elderly people and others who lack digital skills are excluded from some of the benefits of digital technologies, such as not needing to travel long distances to access services. Children tend to struggle less in acquiring digital skills, and so distance learning is not necessarily a challenge for them, but this form of education can affect their social development due to the lack of real-world interaction with their peers. Disabled people can experience exclusion from digital services centres if these centres do not provide disability access. Moreover, many online services are not designed for easy use by people with vision or hearing impairment. Work Package 3 also identified a paucity of digital services in local minority languages. This state of affairs may result in the exclusion of linguistic minorities.

Work Package 4 tackled questions relating to the links and parallels between climate change and cybersecurity in the EHN. The region is susceptible to the impact of climate change, for which reason infrastructure in the region becomes exceptionally critical, energy infrastructure is particularly vulnerable to cyber threats. The conditions of the region give rise to disproportionate governance challenges in terms of integrating environmental policies in line with cybersecurity as the national and international legal frameworks do not address such considerations. Cybersecurity issues have parallels

in aspects of environmental governance and law, such as the concept of sustainable development, the precautionary principle and the 'polluter pays' principle. Identifying the author of environmental damage, especially that caused by climate change, can be very complicated, as it is difficult to trace the damage back to a particular source of pollution. Similar difficulty arises in the case of cyber-damage, as it is often challenging to identify the source of a cyber-attack.

Key findings

- Mainstream cybersecurity frameworks focus on securing information, infrastructure and/or functions vital to society. They do not explicitly acknowledge the (in)securities created by digitalisation for people in their everyday lives.
- National digitalisation and cybersecurity policies do not recognise regional variations in both the opportunities and threats presented by digitalisation. Digitalisation has not altered the balance between different aspects of civil society and affected the relationship between society and the state.
- Diverse regional and communal strategies have considered the voices of different local stakeholders. These strategies have striven to minimise the negative impacts, and thereby to enhance the positive aspects, of digitalisation.
- There is a need for region-specific policies that meet the requirements of the EHN, applicable to critical infrastructure and cybersecurity. Such policies could connect environmental governance and resilience with cybersecurity and apply the principles of human security.
- For local and indigenous peoples, culture and cultural identity are re-shaped by digital transformation. However, this was not found to be a threat to the maintenance of their identities, rather to allow novel manifestations of those identities to develop.