# Free and open source software as a contribution to digital security in the Arctic

Zojer, Gerald

*Published in:*
Arctic yearbook

Published: 01.01.2019

*Document Version*
Publisher's PDF, also known as Version of record

*Citation for pulished version (APA):*
Zojer, G. (2019). Free and open source software as a contribution to digital security in the Arctic. *Arctic yearbook*, *2019*, 173-188. https://arcticyearbook.com/

# Free and open source software as a contribution to digital security in the Arctic

Gerald Zojer

*Digital technologies have become an integral part of everyday life for most inhabitants of the Arctic, diffusing so deep into society that even traditional activities are becoming digitised. All Arctic states have endorsed cybersecurity strategies, highlighting the significance that is attributed to digitalisation in today's societies. Yet, these strategies reproduce a state-centric traditional security approach. Since digitalisation affects all spheres of human security, cybersecurity needs to be redefined in a more comprehensive way to be inclusive to challenges on the individual and community level. This paper discusses a digital security approach. Acknowledging the importance of software in contemporary information societies, this paper looks at how private and public software property regimes are related to digital security in an Arctic specific context. Following approaches from science and technology studies, with special attention to innovation research, this paper discusses the interrelations of proprietary software, open source software (OSS), and free and open source software (FOSS) approaches with digitalisation, considering the peculiarities of Arctic societies. The paper argues that FOSS provides advantages for the often small user base and niche markets of region specific applications, and thus utilising a FOSS approach promotes digital security in the Arctic.*

## Introduction

The motivation for this paper emerged in summer 2018 during a reindeer calf marking event in Sápmi, the Sámi homeland. During this event, reindeer were gathered in a fence system. First the calves were tagged by giving them a numbered collar. Then calves and adult female reindeer were left together in another fenced area so that the mother animal and the calf could find one another again. Reindeer herders could identify their calves by reading the adults' earmark. The reporting led sometimes to overlapping claims and extended the time the usually free roaming reindeer had to be fenced in. One of the reindeer herders explained how helpful it would be if the process of claiming the calves could be done through an app on a mobile phone or a tablet. Double claims would immediately be recognised and the process could be sped up to release reindeer sooner, thus decreasing the time they are held in captivity. However, since not every herding district uses the same method for the calf marking, such an innovation would be very specific and hiring a programmer would be expensive. Also, the programmer would need to be familiar with the process

Gerald Zojer is a Researcher and PhD-Candidate at the Northern Institute for Environmental and Minority Law, Arctic Centre, University of Lapland.

and particularities of the event, because otherwise there is a risk that the digital service might not be suitable and would be rejected (personal communication, July 1, 2018). This discussion revealed some of the challenges of digitalisation in the Arctic and motivated the need to think about possible ways of how digital innovations can contribute to societal well-being; and in this particular case, even to animal welfare.

Today, digital technologies are widespread and are used for many purposes in Arctic everyday life (e.g. GPS trackers, GPS navigation, drones, smartphones, etc.). Mobile devices can especially be used in multiple ways. Smartphones, for instance, usually contain several technologies or components, such as a camera, a gyroscope, a GPS chip, or a modem. They are thus powerful devices and can be used for numerous different tasks depending on the software. In early 2019, the Google Play store contained over 2.6 million entries (AppBrain, 2019), illustrating the vast number of applications available. Few of these have been developed to suit the needs of Arctic inhabitants. For instance, in northern Finland the app *Porokello* warns drivers of reindeer on roads, aiming at reducing traffic accidents ("Porokello," n.d.); in Norway, the free software app *Reinmerker* makes the database of reindeer ear marks (offline) accessible on mobile devices ("Reinmerker," 2012); and in Yakutia, civil society uses smartphones to report industrial pollution to authorities (personal communication, February 18, 2016).

New innovations usually do not emerge "from flashes of disembodied inspiration" (MacKenzie & Wajcman, 1985a: 10) but from gradual changes of existing technologies. Software can be seen as such a gradual innovation that may change the use and purpose of a device significantly. Software itself is often built upon previous code and rarely written from scratch. Yet, every technology affects society, its socio-economic structure, its culture, and the environment. Thus, the diffusion of new innovations has repercussions on societal well-being. In governmental digital agendas, digitalisation is often portrayed in a positivist light, but it may also be perceived as challenging societal integrity (e.g. in Salminen & Hossain, 2018; Sheehan & Gulbrandsen, forthcoming; Young, 2019; Zojer, 2019). However, whether or not digitalisation is perceived as beneficial or challenging is out of the scope of this paper. This paper acknowledges that inhabitants of the Arctic use and develop digital technologies and software, and furthermore, that learning computer or programming skills became part of education programs in parts of the Arctic, also within Indigenous communities (e.g. Hirshberg & Petrov, 2014: 387; Sogsakk, n.d.). This paper focuses on how different property regimes of software are related to human well-being, in search for a software regime that most contributes to digital security in an Arctic specific context. It assumes that digitalisation is an ongoing process with increasing societal significance, while considering that Arctic communities may have specific technological needs related to their particular (economic) activities and the often relatively small community size. The paper discuses digitalisation from a human-centred security approach, and elaborates on how different property regimes of software relate to Arctic digital security.

## Digital security in the Arctic

The process of digitalisation progresses rapidly, including in the Arctic region. Information and communications technologies (ICTs), and especially the internet, are of increasing importance for societal functioning, affecting social, economic, and political life. In 2017, in Denmark, Finland, Iceland, Norway, and Sweden, more than 90% of all households had access to computers and internet from home. While in Canada (86% computer access and 84% internet access in 2013), in

the US (72% computer access and 74% internet access in 2013) (OECD, 2019b, 2019a), and in Russia (with an internet penetration rate of 71% in 2016 (Internet Live Stats, n.d.) these numbers were a bit lower, they still show that digital services and ICTs are widespread. Finland, Sweden, and Denmark are furthermore amongst the highest scoring EU countries in the Digital Economy and Society Index (DESI) (European Commission, 2019). Access to computers or internet is crucial for the functionality of most contemporary digital devices. For instance, in 2017, in the Nordic countries, citizens on average used 3 connected IoT (internet of things) devices, such as cars or smart home devices, a number that is expected to double by 2021 (Dahlberg et al., 2017). Also, for electronic governance, telemedicine, or banking, a properly operating cyberspace[1] is critical.

**Cybersecurity**

The significance of cyberspace for modern societies is also reflected in states' policy responses by endorsing cybersecurity strategies. The Committee on National Security Systems defines cybersecurity as "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (CNSS, 2015: 40). In literature related to International Relations, cybersecurity usually focuses on threats to economic and military assets on the national level. It references threats originating from cybercrime, cyberwarfare, hacktivism, or espionage, and is concerned with securing critical infrastructure and thus the defence of cyberspace from cyber-attacks (e.g. Brooks et al, 2018; Kostopoulos, 2013; Singer & Friedman, 2014). Also, the cybersecurity policies of the Arctic states follow such a mainstream approach (Ministry of Justice, 2017; Ministry of the Interior, 2015; Public Safety Canada, 2018; Secretariat of the Security Committee, 2013; The Danish Government, 2018; The Ministry of Foreign Affairs of the Russian Federation, 2016; The Ministry of Government Administration, Reform and Church Affairs, 2013; The White House, 2018). Human individuals are rather treated as "threats", "weakest links", "victims", or are reduced to users that pose a potential risk to cybersecurity (Dunn Cavelty, 2014; Salminen & Hossain, 2018). Mainstream approaches to cybersecurity can thus be placed within a rather traditional and state-centric security framework, where governmental bodies are the securitising actors.

Such a state centric cybersecurity approach, however, runs danger of falling short of addressing security issues on the sub-state level. The complex and multifaceted realities of digitalisation require a widened and deepened cybersecurity understanding, which should treat individuals and communities as securitising actors, and concentrate on facilitating human development (see also Salminen & Hossain, 2018). A human-centred cybersecurity approach enables individuals and communities to address the fears and to vocalise the concerns they perceive. This also empowers them to include issues that originate from a state's actions that might be detrimental to individual security (Hoogensen Gjørv, 2012), as states' measures to combat cyber-attacks may in fact even hamper information security on the individual level (Dunn Cavelty, 2014). Utilising a human security approach for the cyber domain does not neglect the security challenges that states already address, but rather supplements them with the challenges people experience from digitalisation in everyday life (Zojer, 2019). Such a human-centred cybersecurity approach can thus be seen as very similar to the broadening of the security discourse in the academic field of International Relations since the emergence of critical security studies and the human security concept.

**Digitalisation and human security**

Therefore, it seems suitable to build such a broadened approach of cybersecurity on the human security concept, which aims at promoting human well-being. When looking at the Arctic, the focal shift seems legit, as there are no inter-state conflicts over Arctic territories. The Arctic is considered to be a region of peace and stability, and conflicts can rather be observed between different societal or economic actors within states than between states (e.g. Heininen, 2013; Hossain et al, 2017; Nicol & Heininen, 2014; Tamnes & Offerdal, 2014). While there is no universally satisfying definition for human security, many have built theirs on the seven key areas pointed out in the 1994 HDR, which are economic security, food security, health security, environmental security, personal security, community security, and political security (UNDP, 1994). Instead of focusing on a state's survival, the human security framework focuses on people's "freedom from want" and "freedom from fear." Human security "sits on interstices of human rights, human development, and security discourses" (Martin & Owen, 2014: 1). Within a human security discourse, not only physical integrity but also culture, identity, or human progress should be safeguarded. The positive as well as negative forms of security can be compared to positive and negative forms of human rights, where the "wants" are not less important than people's "fears" (Hoogensen Gjørv, 2012; Roe, 2008). The Commission on Human Security describes the goal of human security as "to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment," and thus to protect "freedoms that are the essence of life" (2003: 4).

Through digitalisation, including the wide diffusion of personal computers (PCs) and the internet, ICTs have become one of the most significant areas of technological progress and have significant interdependence with societal development (c.f. Häußling, 2014: 97). Thus, ICTs can play an important role in safeguarding human security "since they are among the major sources of strengths in improving the quality of living across the world" (Sen, 2014: 24). The UN Human Rights Council identifies the intentional disruption or the prevention of dissemination or access of information from the internet as a violation of human rights (Human Rights Council, 2016). However, digital technologies may also bring new challenges to individual and community security, and have different implications in regional or situational contexts. Zojer (2019) points out that all seven key areas of human security are affected by digitalisation, in both positive and negative ways. On the case study of the European Arctic, Zojer highlights the region-specific implications on human security. For instance, telemedicine may bring basic services to remote places contributing to health, while at the same time reducing the need to travel to far away doctors or hospitals, thereby also reducing the ecological footprint for transportation. A field study in the European Arctic conducted by Sheehan and Gulbrandsen (forthcoming) found that not everyone desires increased digitalisation of health services nor see it as beneficial. It may also be perceived as a result of underfunding of welfare services, as well as generating a lack of physical contact with health professionals. Increasing utilisation of digital technologies also comes with the promise of increasing business opportunities by enabling local enterprises to access global markets, whereas online shopping also challenges established retailers and may lead to a loss of job opportunities (Zojer, 2019). There is indeed a fear that digitalisation and related automation may globally cost up to two billion jobs by 2030, although various economic sectors are affected to different degrees (World Economic Forum, 2016). According to the 2015 HDR, economists historically reject the argument that productivity gains reduce employment in the long run. Yet, the digital revolution may particularly challenge less skilled labour tasks, contributing to increased inequality (UNDP,

2015), and shifting jobs to other regions. For example, in the United States, most jobs created by e-commerce are concentrated around only a handful of metropolitan areas (Gebeloff & Russell, 2017).

### Digital security

As discussed above, security literature and policies in regard to digitalisation are focusing on technology, such as infrastructure, as a referent object and mainly follow a state-centric approach. Not being much of a concern in public discourse at the time, digitalisation was not mentioned and also ICTs remained a side note in the 1994 HDR definition of human security. Given the significance of ICTs and digital technologies in people's everyday life today, it seems, however, appropriate to scrutinise cybersecurity through a human-centred lens. A broadened approach to cybersecurity should shift the focus from technology towards the implications of digitalisation for human well-being and be responsive to region-specific contexts. Salminen suggests introducing the term *digital security* to highlight the interconnection between digitalisation and human security, and to draw a distinction from the prevailing cybersecurity discourse. Such a comprehensive approach "recognises individuals and communities as actors who actively impact (in)security and (un)trustworthiness of the digital environment and, thus, the everyday life of themselves and others" (Salminen, 2018: 188). Although digital security has frequently been used synonymously for information security or cybersecurity, with a similar focus on the protection of technology, it is less biased as a policy tool and receives little attention in International Relations. For example, searching the UN website for "digital security" showed zero results at the time of writing. Yet, as digitalisation refers to digital transformation, it seems appropriate to highlight this dimension when scrutinising the prevailing cybersecurity discourse.

## Free and open source software

The fundamental components of cyberspace and ICTs are computers, whether as end user devices (PCs, smartphones, IoT devices, etc.) or for running the underlying cyber-infrastructure (servers, routers, etc.). Computers consist of the hardware, the physical artifact, and programs, containing libraries, data, and software. Computer programs are a set of instructions telling the hardware what to do. Software is written in a programming language in human readable code (*source code*) that has to be compiled into *object code* for the hardware to be able to understand it. Object code usually only consists of zeros of ones (binary code) and is difficult to read or to reverse engineer by humans; or in case of longer programs, almost impossible.

At the beginning of the computer era, computers were only available at some state-owned facilities or research facilities. Software was considered part of academic knowledge; It underwent a peer review process and was made public. Only in the 1980s, when PCs became more popular, software got unbundled from hardware and was turned into a commodity (Ceruzzi, 1999; Dobusch & Huber, 2007; Holtgrewe & Werle, 2001). In order to protect their research and development efforts, software companies first decided to only sell the object code before implementing legal means to secure their *proprietary software* through Intellectual Property Rights (IPRs) (de Laat, 2005; Holtgrewe & Werle, 2001). IPRs are also tools for creating an artificial shortage of (digital) goods. This is necessary to increase profits, since shortage is a precondition of capitalist commodification while software can be reproduced at will with almost zero costs (Nuss, 2010). Richard Stallman was one of the first to publicly voice his concerns against this development which he considered a privatisation of public knowledge. In 1985 he founded the Free Software Foundation to promote

the idea of free software, whereas the term *free* refers to freedom not price, "so think of it as 'free speech,' not 'free beer'" (Stallman, 2019). For this purpose, he developed the GNU[2] General Public License (GPL)[3], which is a *copyleft* license that utilises copyright conditions to secure public access to the source code. Thus also for free software IPRs play a role, even though in an unorthodox way: authors of free software do claim copyright, but allow others free use, repairing, modifying, or updating the source code (de Laat, 2005; Dobusch & Huber, 2007; Haff, 2018; Raymond, 2002).

**Public vs. private software regimes**

In the business world, however, free software received little attention. Critics suggested that the free software principle was too much focused on philosophical and political concerns. In order to bypass this bias and to push for wider acceptance of software with publicly accessible code, in the 1990s the Open Source Initiative was established and suggested to rather use the term *open source software* (OSS) (Open Source Initiative, 2018). This approach remains contested by *free and open source software* (FOSS) proponents up to the present. Supporters of the free software movement perceive this distinction as downplaying the importance of the inherent philosophy behind free software (Dobusch & Huber, 2007):

> The terms "free software" and "open source" stand for almost the same range of programs. However, they say deeply different things about those programs, based on different values. The free software movement campaigns for freedom for the users of computing; it is a movement for freedom and justice. By contrast, the open source idea values mainly practical advantage and does not campaign for principles. This is why we do not agree with open source, and do not use that term (Stallman, 2019).

FOSS and OSS projects both publish the source code, and both allow copying and distributing the code; free software, however, also requires that the code is allowed to be modified which is not necessarily the case with all OSS licenses, which can be weaker. FOSS thus always qualifies as OSS, but OSS does not necessarily meet FOSS criteria. While the open source movement is convinced about the greater efficiency of the open source model, it explicitly welcomes commercialisation of software (Nuss, 2010). The free software movement argues, however, that free software is not only a practical approach on how to develop software projects, but that ethical values are fundamental to it. FOSS is thus seen as a social movement that aims at promoting social solidarity through sharing and cooperation in a society where culture and life activities become increasingly digitised (Stallman, 2019). Yet, OSS and FOSS have much in common. In fact OSS and FOSS developers often work together in software projects and identify proprietary software as a common adversary. De Laat distinguishes between the public (FOSS/OSS) and private (proprietary) software regimes by "whether knowledge is pursued in order to increase the public stock of knowledge, or to generate rents from its private exploitation" (2005: 1511).

**Motivation and economic considerations**

FOSS/OSS development does not mean, however, that only private persons contribute code in their free time. For instance, from 2005 to 2017, 15,637 developers from a minimum of 1,513 companies contributed to the code of the Linux[4] kernel. In 2017, among the top contributing companies were Intel, Red Hat, IBM, Samsung, or Google (Corbet & Kroah-Hartman, 2017). Yet, also independent or volunteering programmers contribute and especially many smaller and specific software solutions are user innovations or (co-)developed by independent actors. Among the

motivations of volunteers are factors such as intellectual stimulus, improving programming skills, empowerment, the felt need for a particular software solution, the desire to support the case of FOSS/OSS, or the joy of working in a team (David & Shapiro, 2008; Ke & Zhang, 2011; Li, Tan, & Teo, 2012; Raymond, 2002). FOSS/OSS communities are thus heterogeneous, consisting of individuals or firms, or a mix of both, and their projects may have diverse hierarchical and leadership structures.

Although usually being cheaper solutions than proprietary, FOSS/OSS projects can nonetheless generate profits. Revenues can be made from writing code, providing service, maintenance and support, bug fixing, education and training, or by creating documentation (Dobusch & Huber, 2007; Haff, 2018; Nuss & Heinrich, 2002). For instance, Red Hat, a developer of Linux operating systems, reported a net income of US $434 Million in 2018 (Red Hat, n.d.). In 2018 IBM announced its intent to buy Red Hat for US $34 Billion to diversify its portfolio (Baker & Roumeliotis, 2018). While former Microsoft CEO Steve Ballmer called Linux – due to its licensing regime – a cancer (Greene, 2001) and accused its users to be communists (Lea, 2000), today also Microsoft increasingly integrates Linux into its proprietary Windows operating system. Moreover, in 2018 Microsoft acquired Github, the world's largest open source code sharing platform for US $7.5 Billion, in order to support the empowerment of software developers (Nadella, 2018). Thus, despite the early aversion of the business sector toward free software, today FOSS/OSS solutions are deeply embedded in the commercial IT market and are often mixed with proprietary software solutions.

## Discussion

Arctic people(s) have been highly innovative throughout history. The rich diversity of Arctic technologies, including traditional knowledge(s); techniques and tools used for hunting or the herding of livestock; or their craftsmanship are living proof. Due to interaction with the South, there are also many technologies developed outside the region that diffused into Arctic communities, including most digital technologies. Technologies are, however, not confined to physical artifacts, but also refer to the human activities related to it in a twofold manner: in the practice of creating a technology, as well as in the usage, that is, what people know as well as what they do with it. For instance, a "computer without programs and programmers is simply a useless collection of bits of metal, plastic and silicon" (MacKenzie & Wajcman, 1985a, p. 3). Consequently, software also needs to be considered a technology, albeit not being a physical object. While manufacturing goods in traditional industries require heavy and expensive machinery due to the computerisation of individuals, the means of production in a digital society are no longer exclusive property of large corporations (Nuss & Heinrich, 2002). Instead, individuals can participate in the production of new innovations. This is particularly relevant in an Arctic context as it allows local residents to become (co-)producers of digital technologies despite living in remote places with a limited financing base.

### Innovation stakeholders

One critique on the current cybersecurity policies is that they tend to be techno-determinist; they tend to assume that technological advancements will automatically benefit society (Salminen & Hossain, 2018; Zojer, 2019). Yet, since the 1980s science and technology studies scrutinise this faith in technology by arguing that technologies are not neutral objects but embed culture and politics and are thus socially constructed. Moreover, technologies also affect the direction of

societal development (e.g. Bijker, Hughes & Pinch, 2012; Latour, 2004; MacKenzie & Wajcman, 1985b; Winner, 1980). Most technologies, especially those developed in recent decades, are not isolated devices, but are part of large technological systems (LTS). Such systems include physical artifacts that require each other to function; organisations, such as investors or manufacturers; scientific components, since engineers and designers utilise scientific knowledge for their problem solving; regulatory laws; or system artifacts, such as natural resources that are used to build the hardware (Hughes, 2012). These heterogeneous and interacting network components constitute a "seamless web," in which technological and societal development are tightly interlinked (Hughes, 1986). The LTS approach, however, also illustrates the importance of different actors in the innovation process, such as states' policies or funding regimes.

**Small markets and niche products**

Software firms in a traditional manufacturer structure might be suitable actors to design software for new applications, as firms have specialised knowledge about what they produce. However, this specialisation does not necessarily overlap with user's interests, especially if they look for specific applications. Moreover, firms tend to develop products aimed for a large user base in order to maximise their profits, while providing solutions for specific niches are often unprofitable. Buying custom-tailored solutions usually is too expensive for end users (von Hippel, 2005). These findings coincide with the experiences and concerns of the reindeer herder discussed above. The small markets and specific niches in the Arctic will, however, often require unique solutions for a small user base. Such particularities are not only confined to technical aspects, but the Arctic is also rich of different language groups, of which many are small. For instance, the Skolt Sámi museum in Neiden developed its own font "Helveticaskolt" for its main exhibition (Skolt Sámi Museum, 2017) in order to express the Skolt Sámi language in written form. Skolt is only used by 300 people and is considered "severely endangered" by the UNESCO (Moseley, 2010). Regarding software, FOSS has proven useful for being adaptive and addressing small language groups (Benjamin, 2012).

**Economic considerations**

When a new technology is being designed and reaches a bottleneck, such as not meeting the users' needs or being too expensive, its dispersion may remain unsuccessful. Hughes called such bottlenecks "reverse salients." To overcome reverse salients, designers or engineers need to involve the users to identify and understand a bottleneck (Hughes, 2012). User innovations, such as FOSS, can reduce this obstacle, as the users are usually the experts on how a new technology need to be designed (Bijker, 2010; von Hippel, 2005). A reflexive innovation policy benefits from democratising and opening innovation networks, and from including heterogeneous actors with their numerous expertise and knowledges (Rammert, 1997; see also Windeler, 2018). Takeishi and Lee (2005) have furthermore shown, on the example of the mobile music business, that also strict IPR regimes can become reverse salients and hinder innovations.

Most software firms operate in a capitalist mode of production. Maximising profits is of essence when designing a new technology. However, economic laws and economic calculations are specific to different forms of society and to how a society is organised (MacKenzie & Wajcman, 1985a: 17). User innovations are better suited to reflect the social organisation of the community where a new technology is used. Moreover, FOSS/OSS challenges the idea that the individual appropriability of the revenues of an innovation is essential for an economically prosperous society, because such "commodification may even be regarded as a threat to the wealth of a nation

because it jeopardises long-term innovation by limiting access to knowledge and technology" (Holtgrewe & Werle, 2001: 61). There is also empirical evidence that user-based innovation likely increases social welfare (von Hippel, 2005).

**Sustainability and empowerment**

Beside cost factors, flexibility and adaptability of FOSS/OSS projects are one of their strengths. FOSS/OSS projects are the most used solutions on infrastructure devices (servers) and on mobile devices (Schrape, 2016). For clients with big number of devices, such as public administrations or large corporations, the use of FOSS/OSS can be advantageous from a pecuniary standpoint as well as to avoid lock-in effects, which create dependencies on a single manufacturer. The possibility to avoid lock-ins makes FOSS/OSS popular in developing and emerging economies (Dobusch & Huber, 2007; Sowe, Parayil & Sunami, 2012). User-centred innovations that are freely revealed can substitute or supplant manufacturer product development, making communities more independent (von Hippel, 2005).

Free software is furthermore concerned about sharing and cooperation. Making code publicly available allows other users or developers to build on the previous work of each other. Such "free riding" is explicitly welcome in FOSS communities. Sometimes only small changes of code are necessary to adapt the software to other use cases. Copyleft licenses provide guarantee that subsequent contributions of software remain a public affair, as also derivates of the original software need to follow the same license conditions. Note, that this is not the case with some OSS licenses, which may allow derivates of the original work to be placed under a more restrictive license (de Laat, 2005; Schrape, 2016). Moreover, when a FOSS/OSS project is discontinued, the code remains accessible so that others can continue to work on the project. Both, repairability and continuity contribute to the sustainability of FOSS/OSS (Sowe, 2012). In search for a suitable design of digital database and information systems for Sámi traditional knowledge, also Petterson highlights that "open source code and local ownership allow for reuse and development of other's applications" (2011: 187).

**Mainstream cybersecurity considerations**

While not being specifically related to an Arctic context, there are differences between public and private software regimes also from a traditional cybersecurity perspective. FOSS/OSS advocates argue that the more eyes are on the code, the more likely and faster bugs (software errors) can be fixed, while proponents of proprietary software argue for "security through obscurity" (Dobusch & Huber, 2007; Raymond, 2002). Yet, research suggests that the quality and software security between public or private regimes is more or less equal (Clarke, Dorwin, & Nash, n.d.; Haff, 2018: 36–40; Kairala, Koskinen, & Turpeinen, 2015). However, while proprietary software may contain malicious contents, free software published under the GPL imposes political restrictions to avoid that, as the GPL prohibits software to be used to violate human rights, to contain destructive viruses, or code for surveillance purposes (de Laat, 2005). Because the source code of proprietary software is a black box, some end users do not trust them. When China decided to use the open source operating system (Neo)Kylin for public administration and in the military, the step was perceived as being an attempt to block attacks from foreign governments (Heath, 2013). In 2019, the Russian military also announced readiness to shift their computers to open source operating systems (Cimpanu, 2019).

## Conclusions

With increasing digitalisation, information, and no longer work or energy, is the most important factor of production. Touraine (1971) coined this as the characteristic of a post-industrial society. In response to the acknowledgement of the significance of ICTs for the functioning of contemporary societies, the Arctic states (like most others) have endorsed cybersecurity policies. Cybersecurity is related to safeguarding critical cyber-infrastructure and can be compared to a traditional, state-centric security approach. Mainstream cybersecurity policies tend to assume somewhat homogenous societies within national borders and treat individuals as possible risks to cyber-infrastructure. Such an approach runs danger of neglecting the regional particularities and context-specific challenges of digitalisation to communities and individuals. The concept of digital security has been used in this paper to highlight a human-centred security approach to digitalisation, including both "hard" and "soft" security concerns. Consequently, the differentiation between digital security and cybersecurity can be compared to the broadening of human security in relation to a traditional security understanding. Since the securitisation of an issue is a politically powerful act that may direct attention or drastic measures to an issue, it is important to scrutinise the mainstream cybersecurity approach in order to assure that a) policies are sensitive to the regional particularities and needs; b) listen to concerns and challenges of individuals and communities; c) policies are concerned about human well-being, because the purpose of technologies is to improve quality of life after all.

Computers have become integral parts of economic, political, and everyday life and strongly affect the course of action and mindset of people (cf. Rammert, 2016: 246). Yet, computerisation also provides people with a powerful tool to develop new software-based innovations locally and independently from traditional manufacturer models. This paper discussed how the different software regimes of proprietary software, open source software (OSS) and free and open source software (FOSS) are related to digital security in an Arctic context, which includes a) small niche markets and small user bases; b) small people with cultural particularities and small language groups; c) particular local or traditional knowledge for which technologies should be inclusive. Following constructivist approaches from science and technology studies, technologies are not seen as neutral but they embed culture and politics. User based innovations increase inclusiveness of local culture and knowledge (von Hippel, 2005). Both proprietary and free and open source software models can provide economic benefits. A FOSS/OSS approach, furthermore, decreases dependence on outside actors and allow to repair, modify, or adapt software to local needs. FOSS moreover increases sustainability, as copyleft licenses guarantee openness and availability of code, as well as – under the GPL – prohibit violation of human rights. The paper thus concludes that when developing software innovations in the Arctic, utilising a FOSS approach contributes to digital security.

## Notes

1. Cyberspace is used here as the virtual space in which digital technologies are interconnected to each other.

2. GNU is the project name for a free Unix clone Richard Stallman developed in an attempt to keep the popular operating system available to the public. GNU is an acronym and stands for "GNU's Not Unix."
3. Today there are numerous free software licenses existing, however, the GPL remains the most popular one (Schrape, 2016: 26).
4. Linux is one of the most successful free and open source projects. Linux operating systems are software bundles powering numerous devices, such as servers, PCs, or smartphones (e.g. Android or Sailfish OS are based on the Linux kernel).

## References

AppBrain. (2019, June 13). Number of Android applications on the Google Play store. Retrieved June 14, 2019, from AppBrain website: https://www.appbrain.com/stats/number-of-android-apps

Baker, L. B., & Roumeliotis, G. (2018, October 29). IBM to acquire software company Red Hat for $34 billion. Retrieved June 11, 2019, from Reuters website: https://www.reuters.com/article/us-red-hat-m-a-ibm-idUSKCN1N20N3

Benjamin, M. (2012). Language data as a foundation for developing countries; The ANLoc 100 African Locales Initiative. In S. K. Sowe, G. Parayil, & A. Sunami (Eds.), *Free and open source software and technology for sustainable development* (pp. 164–181). Tokyo, New York, Paris: United Nations University Press.

Bijker, W. E. (2010). Democratization of Technology, Who are the Experts? Retrieved February 1, 2019, from http://www.angelfire.com/la/esst/bijker.html

Bijker, W. E., Hughes, T. P., & Pinch, T. (Eds.). (2012). *The social construction of technological systems: New directions in the sociology and history of technology* (Anniversary ed). Cambridge, Mass: MIT Press.

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity essentials*. Indianapolis, Indiana: John Wiley & Sons Inc.

Ceruzzi, P. (1999). Inventing personal computing. In D. A. MacKenzie & J. Wajcman (Eds.), *The social shaping of technology* (2nd ed, pp. 64–86). Buckingham [Eng.] ; Philadelphia: Open University Press.

Cimpanu, C. (2019, May 30). Russian military moves closer to replacing Windows with Astra Linux. Retrieved June 4, 2019, from ZDNet website: https://www.zdnet.com/article/russian-military-moves-closer-to-replacing-windows-with-astra-linux/

Clarke, R., Dorwin, D., & Nash, R. (n.d.). *Is Open Source Software More Secure?* [Homeland Security / Cyber Security]. Retrieved June 1, 2019, from University of Washington website: https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/oss(10).pdf

CNSS. (2015). *Committee on National Security Systems (CNSS) Glossary* (No. CNSSI No. 4009). Committee on National Security Systems.

Commission on Human Security. (2003). *Human Security Now*. New York: United Nations.

Corbet, J., & Kroah-Hartman, G. (2017). *Linux Kernel Development Report 2017*. Retrieved June 10, 2019, from The Linux Foundation website:

https://www.linuxfoundation.org/publications/2017/10/2017-state-of-linux-kernel-development/

Dahlberg, H., Öberg, J., Sanda, M., Nilsson, M., Glaumann, M., Gjestrup, A., … Wikberg, J. (2017). *Connected Things. New digital ecosystems—Unlocking the growth potential of IoT*. Retrieved April 14, 2019, from Telia website: http://mb.cision.com/Public/40/2203407/bb4409aaefaeb6c2.pdf

David, P. A., & Shapiro, J. S. (2008). Community-based production of open-source software: What do we know about the developers who participate? *Information Economics and Policy*, *20*(4), 364–398. https://doi.org/10.1016/j.infoecopol.2008.10.001

de Laat, P. B. (2005). Copyright or copyleft? *Research Policy*, *34*(10), 1511–1532. https://doi.org/10.1016/j.respol.2005.07.003

Dobusch, L., & Huber, J. (2007). Freie Software für freie Bürger/innen: Kommunale Chancen und Aufgaben bei der Verwendung von Freier und Open Source Software. In L. Dobusch & C. Forstleitner (Eds.), *Freie Netze—Freies Wissen: Ein Beitrag zum Kulturhauptstadtjahr Linz 2009* (pp. 106–141). Wien: Echo Media Verl.

Dunn Cavelty, M. (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

European Commission. (2019, September 4). The Digital Economy and Society Index (DESI) [Text]. Retrieved September 7, 2019, from Digital Single Market—European Commission website: https://ec.europa.eu/digital-single-market/en/desi

Gebeloff, R., & Russell, K. (2017, July 6). How the Growth of E-Commerce Is Shifting Retail Jobs. *The New York Times*. Retrieved November 24, 2017, from https://www.nytimes.com/interactive/2017/07/06/business/ecommerce-retail-jobs.html

Greene, T. C. (2001, June 2). Ballmer: "Linux is a cancer." Retrieved June 11, 2019, from The Register website: https://www.theregister.co.uk/2001/06/02/ballmer_linux_is_a_cancer/

Haff, G. (2018). *How open source ate software: Understand the open source movement and so much more*. New York, NY: Springer Science+Business Media.

Häußling, R. (2014). *Techniksoziologie* (1. Auflage). Baden-Baden: Nomos.

Heath, N. (2013, March 22). Chinese government builds national OS around Ubuntu. Retrieved April 10, 2019, from ZDNet website: https://www.zdnet.com/article/chinese-government-builds-national-os-around-ubuntu/

Heininen, L. (2013). Security in the Arctic. In N. Loukacheva (Ed.), *Polar Law Textbook II* (pp. 37–52). Copenhagen: Norden.

Hirshberg, D., & Petrov, A. N. (2014). Education and Human Capital. In J. Nymand Larsen & G. Fondahl (Eds.), *Arctic human development report: Regional processes and global linkages* (pp. 347–396). Copenhagen: Nordic Council of Ministers.

Holtgrewe, U., & Werle, R. (2001). De-Commodifying Software? Open Source Software Between Business Strategy and Social Movement. *Science Studies*, (2), 43–65.

Hoogensen Gjørv, G. (2012). Security by any other name: Negative security, positive security, and a multi-actor security approach. *Review of International Studies*, *38*(04), 835–859. https://doi.org/10.1017/S0260210511000751

Hossain, K., Zojer, G., Greaves, W., Roncero, J. M., & Sheehan, M. (2017). Constructing Arctic security: An inter-disciplinary approach to understanding security in the Barents region. *Polar Record*, *53*(01), 52–66. https://doi.org/10.1017/S0032247416000693

Hughes, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. *Social Studies of Science*, *16*(2), 281–292. https://doi.org/10.1177/0306312786016002004

Hughes, T. P. (2012). The Evolution of Large Technological Systems. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The social construction of technological systems: New directions in the sociology and history of technology* (Anniversary ed, pp. 45–76). Cambridge, Mass: MIT Press.

Human Rights Council. (2016). *The promotion, protection and enjoyment of human rights on the Internet* (Resolution Adopted by the Human Rights Council No. A /HRC/RES/32/13). Retrieved September 2, 2019, from United Nations General Assembly website: https://undocs.org/en/A/HRC/RES/32/13

Internet Live Stats. (n.d.). Internet Users by Country 2016. Retrieved December 1, 2017, from http://www.internetlivestats.com/internet-users-by-country/

Kairala, A., Koskinen, J., & Turpeinen, S. (2015). *Software Security In Open and Closed Source Software*. Retrieved April 7, 2019, from University of Oulu website: https://wiki.oulu.fi/download/attachments/58197330/ossd_2015_kairala_koskinen_turpeinen.pdf?version=1&modificationDate=1448956482000&api=v2

Ke, W., & Zhang, P. (2011). Effects of Empowerment on Performance in Open-Source Software Projects. *IEEE Transactions on Engineering Management*, *58*(2), 334–346.https://doi.org/10.1109/TEM.2010.2096510

Kostopoulos, G. K. (2013). *Cyberspace and Cybersecurity*. Boca Raton, Fl: CRC Press.

Latour, B. (2004). *Politics of nature: How to bring the sciences into democracy*. Cambridge, Mass: Harvard University Press.

Lea, G. (2000, July 31). MS' Ballmer: Linux is communism. Retrieved June 11, 2019, from https://www.theregister.co.uk/2000/07/31/ms_ballmer_linux_is_communism/

Li, Y., Tan, C.-H., & Teo, H.-H. (2012). Leadership characteristics and developers' motivation in open source software development. *Information & Management*, *49*(5), 257–267. https://doi.org/10.1016/j.im.2012.05.005

MacKenzie, D. A., & Wajcman, J. (1985a). Introductory Essay. In D. A. MacKenzie & J. Wajcman (Eds.), *The Social shaping of technology: How the refrigerator got its hum* (pp. 2–25). Milton Keynes ; Philadelphia: Open University Press.

MacKenzie, D. A., & Wajcman, J. (Eds.). (1985b). *The Social shaping of technology: How the refrigerator got its hum*. Milton Keynes ; Philadelphia: Open University Press.

Martin, M., & Owen, T. (2014). Introduction. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 1–14). London ; New York: Routledge/Taylor Francis Group.

Ministry of Justice. (2017). *A national cyber security strategy* (No. Skr. 2016/17:213). Stockholm.

Ministry of the Interior. (2015). *Icelandic National Cyber Security Strategy 2015–2026*.

Moseley, C. (Ed.). (2010). *Atlas of the World's Languages in Danger* (3rd ed.). Retrieved September 10, 2019, from http://www.unesco.org/culture/languages-atlas/en/atlasmap.html

Nadella, S. (2018, June 4). Microsoft + GitHub = Empowering Developers. Retrieved June 11, 2019, from The Official Microsoft Blog website: https://blogs.microsoft.com/blog/2018/06/04/microsoft-github-empowering-developers/

Nicol, H. N., & Heininen, L. (2014). Human security, the Arctic Council and climate change: Competition or co-existence? *Polar Record*, *50*(01), 80–85. https://doi.org/10.1017/S0032247412000666

Nuss, S. (2010). Private property and public goods of information in view of copyright and copyleft. *Library and Information Science Critique*, *3*(2), 11–18.

Nuss, S., & Heinrich, M. (2002). Freie Software und Kapitalismus. *Streifzüge*, *1*, 39–43.

OECD. (2019a). Access to computers from home (indicator). Retrieved September 2, 2019, from OECD website: https://doi.org/10.1787/a70b8a9f-en

OECD. (2019b). Internet access (indicator). Retrieved September 2, 2019, from OECD website: https://doi.org/10.1787/69c2b997-en

Open Source Initiative. (2018, October). History of the OSI. Retrieved June 10, 2019, from Open Source Initiative website: https://opensource.org/history

Pettersen, B. (2011). Mind the digital gap: Questions and possible solutions for design of databases and information systems for Sami traditional knowledge. *Diedut*, *1*, 163–192.

Porokello. (n.d.). Retrieved November 30, 2017, from http://porokello.fi

Public Safety Canada. (2018). *National cyber security strategy: Canada's vision for security and prosperity in the digital age*. Retrieved May 24, 2019, from http://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2018/18-27/publications.gc.ca/collections/collection_2018/sp-ps/PS4-239-2018-eng.pdf

Rammert, W. (1997). Innovation im Netz. Neue Zeiten für technische Innovationen: Heterogen verteilt und interaktiv vernetzt. *Soziale Welt*, *48*(4), 397–416.

Rammert, W. (2016). *Technik - Handeln - Wissen: Zu einer pragmatistischen Technik- und Sozialtheorie* (2., aktualisierte Auflage). Wiesbaden: Springer VS.

Raymond, E. S. (2002). *The Cathedral and the Bazaar* (v. 3.0). Retrieved April 4,2019, from http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/

Red Hat. (n.d.). Red Hat Reports Fourth Quarter and Fiscal Year 2019 Results. Retrieved June 11, 2019, from U.S. Securities and Exchange Commission website: https://www.sec.gov/Archives/edgar/data/1087423/000115752319000688/a51958812ex99_1.htm

Reinmerker. (2012). Retrieved July 26, 2018, from https://www.reinmerker.no/

Roe, P. (2008). The 'value' of positive security. *Review of International Studies*, *34*(4), 777–794. https://doi.org/10.1017/S0260210508008279

Salminen, M. (2018). Digital security in the Barents region. In K. Hossain & D. Cambou (Eds.), *Society, environment and human security in the Arctic Barents region* (pp. 187–204). London ; New York, NY: Routledge.

Salminen, M., & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: An appraisal for the European High North. *Polar Record*, 1–11. https://doi.org/10.1017/S0032247418000268

Schrape, J.-F. (2016). *Open-Source-Projekte als Utopie, Methode und Innovationsstrategie: Historische Entwicklung - sozioökonomische Kontexte - Typologie*. Glückstadt: vwh, Verlag Werner Hülsbusch, Fachverlag für Medientechnik und -wirtschaft.

Secretariat of the Security Committee. (2013). *Finland's Cyber security Strategy* [Government Resolution January 24, 2013]. Retrieved December 17, 2019, from www.yhteiskunnanturvallisuus.fi/en

Sen, A. (2014). Birth of a discourse. In M. Martin & T. Owen (Eds.), *Routledge handbook of human security* (pp. 17–27). London ; New York: Routledge/Taylor Francis Group.

Sheehan, M., & Gulbrandsen, K. S. (forthcoming). Human Cyber-Security and Social Exclusion in the European High North. In G. Zojer (Ed.), *Enablement besides Constraints: Human Security and a Cyber Multi-disciplinary Framework in the European High North* (p. tba). University of Lapland Printing Centre.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford ; New York: Oxford University Press.

Skolt Sámi Museum. (2017, May 20). Main exhibition. Retrieved September 12, 2019, from Skolt Sámi museum website: http://www.skoltesamiskmuseum.no/main-exhibition.6000069-414107.html

Sogsakk. (n.d.). Datanomi. Retrieved May 24, 2018, from Sámi education institute website: http://www.sogsakk.fi/fi/Hakijalle/Koulutustarjonta/Datanomi

Sowe, S. K. (2012). Conclusions. In S. K. Sowe, G. Parayil, & A. Sunami (Eds.), *Free and open source software and technology for sustainable development* (pp. 315–320). Tokyo, New York, Paris: United Nations University Press.

Sowe, S. K., Parayil, G., & Sunami, A. (Eds.). (2012). *Free and open source software and technology for sustainable development*. Tokyo, New York, Paris: United Nations University Press.

Stallman, R. (2019, April 28). Why Open Source misses the point of Free Software. Retrieved June 10, 2019, from GNU Operating System website: https://www.gnu.org/philosophy/open-source-misses-the-point.html

Takeishi, A., & Lee, K.-J. (2005). Mobile music business in Japan and Korea: Copyright management institutions as a reverse salient. *The Journal of Strategic Information Systems*, *14*(3), 291–306. https://doi.org/10.1016/j.jsis.2005.07.005

Tamnes, R., & Offerdal, K. (Eds.). (2014). *Geopolitics and security in the Arctic: Regional dynamics in a global world*. Oxon and New York: Routledge.

The Danish Government. (2018). *Danish cyber and information security strategy*. Ministry of Finance.

The Ministry of Foreign Affairs of the Russian Federation. (2016). *Doctrine of Information Security of the Russian Federation* (Decree of the President of the Russian Federation No. 646). Retrieved May 15, 2019, from http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

The Ministry of Government Administration, Reform and Church Affairs. (2013). *Cyber Security Strategy for Norway*. Norwegian Government Administration Services.

The White House. (2018). *National Cyber Strategy of the United States of America.*

Touraine, A. (1971). *The post-industrial society: Tomorrow's social history: classes, conflicts and culture in the programmed society*. London: Wildwood House.

UNDP. (1994). *Human development report 1994*. New York: Oxford University Press.

UNDP. (2015). *Human development report 2015. Work for human development*. New York, NY: United Nations Development Programme.

von Hippel, E. (2005). *Democratizing innovation*. Cambridge, Mass: MIT Press.

Windeler, A. (2018). Reflexive Innovation. On Innovation in Radicalized Modernity. In W. Rammert, A. Windeler, H. Knoblauch, & M. Hutter (Eds.), *Innovation Society Today. Perspectives, Fields, and Cases* (pp. 65–106). Wiesbaden: Springer VS.

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136.

World Economic Forum. (2016). *Digital Transformation of Industries: Societal Implications* [WEF White Paper].

Young, J. C. (2019). The new knowledge politics of digital colonialism. *Environment and Planning A: Economy and Space*, *51*(7), 1424–1441. https://doi.org/10.1177/0308518X19858998

Zojer, G. (2019). The Interconnectedness of Digitalisation and Human Security in the European High North: Cybersecurity Conceptualised through the Human Security Lens. *The Yearbook of Polar Law*, *10*, 297–320. https://doi.org/10.1163/22116427_010010014