Smart Information Systems in Cybersecurity

An Ethical Analysis

Macnish, Kevin

University of Twente

FernandezInguanzo, Ana

University of Twente

Kirichenko, Alexey

F-Secure

Corresponding Author: Kevin Macnish, k.macnish@utwente.nl

Abstract: This report provides an overview of the current implementation of SIS in the field of cybersecurity. It also identifies the positive and negative aspects of using SIS in cybersecurity, including ethical issues which could arise while using SIS in this area. One company working in the industry of telecommunications (Company A) is analysed in this report. Further specific ethical issues that arise when using SIS technologies in Company A are critically evaluated. Finally, conclusions are drawn on the case study and areas for improvement are suggested.

Keywords: Cybersecurity, ethics, smart information systems, big data

Citation: Macnish, K., FernandezInguanzo, A., & Kirichenko, A. (2019). Smart Information Systems in Cybersecurity. *ORBIT Journal*, *2*(2).
https://doi.org/10.29297/orbit.v2i2.105

Smart Information Systems in Cybersecurity: An Ethical Analysis

Increasing numbers of items are becoming connected to the internet. Cisco, a global leader in information technology, networking and cybersecurity, estimates that more than 8.7 billion devices were connected to the internet by the end of 2012, a number that will likely rise to over 40 billion in 2020 (Singer and Friedman 2014). Cybersecurity has therefore become an important concern both publicly and privately. In the public sector, governments have created and enlarged cybersecurity divisions such as the US Cyber Command and the Chinese "Information Security Base", whose mission is to provide security to critical national security assets (Singer and Friedman, 2014, p. 3).

In the private sphere, companies are struggling to keep up with the required need for security in the face of increasingly sophisticated attacks from a variety of sources. In 2017, there were "over 130 large-scale, targeted breaches [by hackers of computer networks] in the U.S.," and "between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches" (Sobers, 2018). Furthermore, cyber attacks affect not only the online world, but also lead to vulnerabilities in the physical world, particularly when an attack threatens industries such as healthcare, communications, energy, or military networks, putting large swathes of society at risk. Indeed, it has been argued that some cyber attacks could constitute legitimate grounds for declarations of (physical) war (Smith, 2018).

Cybersecurity is therefore a complex and multi-disciplinary issue. Security has been defined in the international relations and security studies spheres both as "the absence of threats to acquired values" (Wolfers, 1952) and "the "absence of harm to acquired values" (Baldwin, 1997). Within the profession, cybersecurity is more commonly defined in terms of confidentiality, integrity and availability of information(Lundgren and Möller, 2017). A2014 literature review on the meanings attributed to cybersecurity has led to the broader definition of cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems" (Craigen et al., 2014, p. 13).

Cybersecurity therefore can be seen to encompass property rights of ownership of networks that could come under attack, as well as other concerns attributed with these, such as issues of access, extraction, contribution, removal, management, exclusion, and alienation(Hess and Ostrom, 2007). Hence cybersecurity fulfils a similar role to physical security in protecting property from some level of intrusion. Craigen et al also argue that cybersecurity refers not only to a technical domain, but also that the values underlying that domain should be included in the description of cybersecurity(2014, p. 17). Seen this

way, ethical issues and values form bedrock to cybersecurity research as identifying the values which cybersecurity seeks to protect.

The case study is divided into four main sections. Sections 1 and 2 focus on the literature review: section 1 reviews the technical aspects of cybersecurity, while section 2 presents a literature review of academic articles concerning ethical issues in cybersecurity. Section 3 focuses on the practice of cybersecurity research through an interview conducted with four employees at a major telecommunications software and hardware company, Company A. Finally, section 4 critically evaluates ethical issues that have arisen in the use of SIS technologies in cybersecurity.

1. The use of Smart Information Systems in Cybersecurity

The introduction of big data and artificial intelligence (Smart Information Systems, or SIS) in cybersecurity is still in its early phase. Currently there is comparatively little work carried out on cybersecurity using SIS for several reasons. These include the remarkable diversity of cyber attacks (e.g. different approaches to hacking systems and introducing malware), the danger of false positives and false negatives, and the relatively low intelligence of existing SIS.

Taking these in turn, the diversity of attacks, both in the source of the attack, the focus of the attack and the motivation of the attack is significant. Attacks can be launched from outside an organization (e.g. from a hacking collective, such as Anonymous) or from an insider (e.g. a disaffected employee looking to damage a system). They may come from a single source, typically masked through using the dark net, or from a source who has engaged in a number of "hops" (moving from one computer on a network to another, thus masking the original source) such that the originator could appear to be in a hospital or in a military base. If the attack appears to come from a military base this might encourage the attacked party to "hack back". However, if the military base were an artificial screen presented in front of a hospital, the reverse hack could bring down that hospital's computer networks. The focus of the attack could be on imitating a user or systems administrator (local IT expert) or on exploiting a security flaw in unpatched code (programming in a network that has a flaw which has not yet been fixed, also known as a zero-day exploit). The motivation of the attack can range from state security and intelligence gathering (e.g.US Intelligence spying on Chinese military installations), to financial incentives through blackmail (e.g. encrypting a company's files and agreeing to decrypt them only when the company has paid the hacker a certain sum of money). This diversity means that it is extremely difficulty to develop a SIS that will effectively recognize an attack for what it is.

Secondly, the danger of false positives and false negatives is significant in light of the difficulty of recognizing an attack. If an attack is not recognized by a SIS then as a false negative it may be successful. This is particularly the case if security personnel have come to place undue trust in the automation and so do not provide quality assurance of the SIS, which is known as "automation bias" (Bainbridge, 1983; Goddard et al., 2012). By contrast, the SIS could be so cautious that it may lead to an excessive number of false positives in which a legitimate interaction is falsely labelled an attack and not permitted to continue. This leads to frustration and could entail the eventual disabling of the SIS(Tucker, 2018).

Thirdly, and despite some hype in the media, SIS are still at a relatively unintelligent stage of development. Computer vision systems designed to identify people loitering, for example, recognize that a person has not left a circle with radius x in y number of seconds, but cannot determine why the person is there or what their intent may be. As such, the inability to determine intentions from actions renders automated systems relatively impotent.

Despite these concerns, there are some potential grounds for use of SIS in cybersecurity. The most effective is in scanning systems for known attacks, or known abnormal patterns of behaviour that have a very high likelihood of being an attack. When coupled with a human operator to scan any alerts and so determine whether to take action, the combined human-machine security system can prove to be effective, albeit still facing the above problems of automation bias and excessive false positives (Macnish, 2012).

2. Literature Review - Ethical Issues of Using SIS in Cybersecurity

In this section we will conduct a literature review of the most fundamental ethical issues in cybersecurity that are being proposed in the academic environment. Our goal is to compare them with the interview that has been conducted in a major telecommunications software and hardware company, Company A, in order to give an overview on the ethical issues in cybersecurity.

The literature review was carried out through a combination of online search using generic engines such as Google and Google Scholar and discipline-specific search engines on websites such as PhilPapers.org and the Philosophers' Index. Selected papers were then read and, where appropriate, the bibliographic references were used to locate further literature. Generic search on Google also provided links to trade publications and websites that were a further source of background information.

The ethical issues to arise from the literature review were informed consent; protection from harm; privacy and control of data; vulnerabilities and disclosure; competence of research ethics committees; security issues; trust and transparency; risk; responsibility; and business interests and codes of conduct.

2.1 Informed consent

Acquiring informed consent is an important activity for cybersecurity, and one that has been at the heart of research ethics and practice for decades (Johnson et al., 2012; Miller and Wertheimer, 2009).Consent is variously valued as the respect for autonomy (Beauchamp, 2009) or the minimization of harm (Manson and O'Neill, 2007).The justification for informed consent is a considerable challenge for data analytics, then, where anonymised data may be used without explicit consent of the person from whom it originates. This is also true within global cybersecurity, where a number of complicating issues arise such as the complexity of informing users about detailed technical aspects in order to provide necessary information, as well as language barriers (Burnett and Feamster, 2015).This, though, is the case for many other areas of research such as medical or social sciences, and the scripts need not be different in cybersecurity (Macnish and van der Ham, 2019).

Nonetheless, challenges of complexity, and of conveying that complexity in a manner that is sufficiently informative for a non-expert to make a decision, remain. Wolter Pieters notes that information provision does not correspond merely to the amount of information communicated, but how it is presented, and that the type of information given is justified and appropriate. "One cannot speak about informed consent if one gives too lit-

tle information, but one cannot speak about informed consent either if one gives too much. Indeed, giving too much information might lead to uninformed dissent, as distrust is invited by superfluous information" (Pieters, 2011, p. 61).

2.2 Protection from Harm

Cybersecurity has the potential to cause harm to its users, even when that harm is not intended. Concerns exist regarding the disclosure of vulnerabilities (such as a flaw in a security program which would allow for a hacker to break into the network with relative ease), for example, such as whether they should be disclosed publicly once a company has failed to address them. If not then the vulnerability entails that a person may be at risk of attack, which is particularly concerning if the device at risk is medical in nature, such as a pacemaker (Nichols, 2016; Spring, 2016). However, disclosure could bring the vulnerability to the awareness of potential attackers who had not considered it previously. This is true of cybersecurity generally, whether involving SIS or not.

2.3 Privacy and Control of Data

Privacy is a central issue in cybersecurity, as increasing amounts of personal data are gathered and stored in the cloud. Furthermore, these data can be highly sensitive, such as health or bank records (Manjikian, 2017, pp. 81–112). While the data at risk from attack is private, in order to identify an attack, particularly when SIS are involved, an effective cybersecurity system must maintain an awareness of "typical" behaviour so that "atypical" behaviour stands out more obviously. To do this however, requires ongoing development of personal profiles of users of a particular system, which in turn involves monitoring their behaviour online. In cases of both attack and prevention of attacks then, users' privacy risks are compromised.

A related issues is that of control of data, which may be seen as an aspect of privacy (Moore, 2015, 2003) or additional to privacy concerns (Allen, 1999; Macnish, 2018). In either case, the control of data is a critical factor, as once an attack has been successful control is lost. The data may then be used for a variety of ends, not only relating to violations of privacy but also for political or other gain, as was the case with Cambridge Analytica(Cadwalladr and Graham-Harrison, 2018), where the problem was not only privacy concerns, but also the control of users' data, which enabled discrete, targeted political advertising concerning the UK's referendum on membership of the EU and the US presidential election, both in 2016 (Ienca and Vayena, 2018).

While the European Union has sought to resolve concerns with privacy and control of data through the introduction of the General Data Protection Regulation (EU Parliament, 2016), this has raised its own concerns. While European companies must follow strict regulations in developing SIS-related algorithms when it comes to accessing personal

data, the same only applies to non-European companies when they practice in Europe. This leads to a concern of

"data dumping, in which research is carried out in countries with lower barriers for use of personal data, rather than jump through bureaucratic hurdles in Europe. The result is that the data of non-European citizens is placed at higher risk than that of Europeans" (Macnish and van der Ham, 2019, p. 8).

Incidental findings also fall under this category, as data derived from regular scans with the goal of profile-building can uncover new information about an individual which they did not want to reveal. Decisions should be made in advance on how to reveal that information and to whom it should be revealed; for example, the discovery that an employee is looking for another job.

2.4 Vulnerabilities and disclosure

An awareness or a duty to find vulnerabilities in a network which leave it open to an attack can help cybersecurity professionals understand the magnitude of a particular attack. However, disclosure of vulnerabilities to a particular authority, such as the company responsible, also risks the leak of that vulnerability from the responsible authority to communities of hackers so that that network or others may be exploited (Macnish and van der Ham, 2019, p. 9). If vulnerabilities are made public then the public visibility of a system and therefore its commercial viability may be threatened. For example, Wolter Pieters has pointed out the challenge of exposing vulnerabilities in e-voting systems: prior to an election and the systems will not be trusted; after an election and the election result will be called into question. However, if the vulnerability is not disclosed then an attack may occur which genuinely compromises the election. A related issue here is whether cybersecurity researchers looking at the techniques and practices of hackers should have a duty to expose vulnerabilities as an act of professional whistle blowing. By rendering this a duty, there is less pressure on the professional to have to decide what is the right thing to do in a particular case, such as when competing financial interests may argue against such revelations (Davis, 1991). As noted above, ethical issues arising from vulnerability disclosure are true of cybersecurity generally, whether involving SIS or not.

2.5 Competence of Research Ethics Committees

Within universities and many research institutions, Research Ethics Committees (REC or Institutional Review Boards)oversee applications for research to provide protection for research participants. However, RECs are often composed of experts in ethics who have limited awareness of cybersecurity practice, or computer scientists who lack ethical expertise. An example of this occurred when potentially harmful research was carried out on non-consenting individuals in totalitarian states which effectively tested the firewalls of those states (Burnett and Feamster, 2015). While this research clearly put individuals

at risk without their consent, at least two RECs determined that the research was not of relevance for ethical review because it did not concern human participants or personal data. It did, however, concern IP addresses which could easily be linked to a human person, putting that person at risk (Macnish and van der Ham, 2019).In the case of research using SIS, the potential for obscurity of the data could render the link with individuals more difficult to recognise still. Furthermore, it should be noted that these are concerns which arise in institutions with access to a REC. As pointed out by Macnish and van der Ham (2019), many private companies do not have any ethical oversight facilities.

2.6 Security issues

Given the aforementioned definition of security as the absence of threat to acquired values, the maintenance of good security is an ethical issue, as without it commonly-held values may be compromised. “Insufficient funding, poor oversight of systems, late or no installation of “patches” (fixes to security flaws), how and where data are stored, how those data are accessed, and poor training of staff in security awareness” (Macnish, van der Ham, 2018, p.11-12) are therefore all instances of ethical concern.

2.7 Trust and transparency

Trust is an issue which connects the cybersecurity expert to the users who are being protected. Relating back to concerns regarding the risks inherent in publicizing vulnerabilities, there are pressing issues concerning transparency, such as

“how far to push transparency: should it extend to government agencies or even other companies? On one hand sharing information increases vulnerability as one’s defences are known, and one’s experience of attacks shared, but on the other it is arguably only by pooling experience that an effective defence can be mounted” (Macnish and van der Ham, 2019, p. 14).

Pieters argues that trust in a person goes hand-in-hand with the explanation that a person gives(Pieters, 2011). Artificial agents hence need to explain their decisions to the user, such as how security is maintained in online transactions(Pieters, 2011, p. 53). He argues that there is a need for better understanding of the relationship between explanation and trust in Artificial Intelligence (AI) and information security. Glass et al. concluded that trust depends on both the detail of explanations provided and on the transparency of the system(Glass et al., 2008). From a cybersecurity perspective, what matters is how to communicate *whether* the system is secure, *why* it is secure, or *how* it is secure. In SIS, explanations are typically provided by the system itself, while in information security the explanations are provided by the designer (Bederson et al., 2003). Pieters argues that the role of explanations consists, at least in part, in acquiring and maintaining users' trust. He further exposes the concept of "black boxes" which, together with trust and explanation, is a fundamental concept in cybersecurity, where the precise algorithm and associated decision-making techniques may become invisible within SIS systems (Pieters, 2011).

From a cybersecurity perspective, what matters is how to communicate *whether* the system is secure, *why* it is secure, or *how* it is secure.

Furthermore, through applying Bruno Latours' actor-network theory (Latour, 2005) Pieters highlights several issues with explanations and trust in information systems. He notes that explanations can be different depending on the actors who are explaining the system or technology. For example, a government seeking to protect the democratic credentials of an election, or a business with a commercial interest in keeping the source code secret, will have different explanations for an e-voting system(Pieters, 2011, p. 57). In the same way, Pieter notes that delegation of technical aspects relating to the SIS will lead to a new actor who will not necessarily have the same abilities to explain the system as the designer.

Pieters also notes that explanations can have different goals, such as transparency versus justification. He argues:

"Explanation-for-trust is explanation of how a system works, by revealing details of its internal operations. Explanation-for-confidence is explanation that makes the user feel comfortable in using the system, by providing information on its external communications. In explanation-for-trust, the black box of the system is opened; in explanation-for-confidence, it is not"(Pieters, 2011, p. 57).

In the field of cybersecurity, as elsewhere in security, explanation of the security capabilities of the system to the user is an important requirement. “This is especially true because security is not instantly visible in using a system, as security of a system is not a functional requirement” (Pieters, 2011, p. 58). For example, it is not possible to infer that if a system gives good results then that system is secure. As Pieters warns, a criminal might have changed the results of voting without anyone noticing. Uncertainty is a feature within these systems and given that security is often added to the system without being integral to it, it is feasible that the system can function without compromise being detected. The challenges of trust are exacerbated when the system operates using data analytics and potentially opaque algorithms that cannot be understood, still less challenged, by those affected (O’Neil, 2016).

2.8 Risk

Consideration of who will decide what risks will be taken, what are the acceptable risks, and how risk is calculated(Hansson, 2013; see also Wolff, 2010) is important in cybersecurity. One of the arguments given for not requesting informed consent in the case described by Burnett and Feamster regarding the non-consensual importing of malware onto user’s computers to test firewalls was that, in the opinion of the researchers, there was only a limited risk of harm to the subject(2015, p. 664). However, it does not take much reflection to identify the risk to users who live in states where censorship is an issue, leading to potentially difficult situations(Byers, 2015; Macnish and van der Ham, 2019). Furthermore, it has been demonstrated that different groups of society tend to assess risk differently, with the acceptable risk threshold of white men being significantly higher than that of women or ethnic minorities (Hermansson, 2010, 2005).

2.9 Responsibility

The locus of responsibility for protecting against, and paying for protection against, cyber attacks is an ongoing issue (Guiora, 2017, pp. 89–111). It is not clear whether companies should be left to fend for themselves against hostile state-sponsored attacks, or whether governments should provide at least some financial support for them. Given the aforementioned potential to view cyber attacks as justification for declaring war, it is important to ask the degree to which the state should shoulder “responsibility for protecting its own economy on the internet as it does in physical space, by providing safe places to trade” (Macnish, van der Ham, 2018, p.14).

Cybersecurity is usually taken to concern attacks from outside an entity rather than inside, for example using firewalls against incoming traffic (Cleeff et al., 2009). Yet the development of technology allows for a global environment in which many businesses provide third parties access to their own networks, thus expanding the boundaries of what, or who, may be seen as “inside”. This extends to “mobile devices [that] can access

data from anywhere, and smart buildings [which] are being equipped with microchips that constantly communicate with each other" (Cleeff et al., 2009, p. 50). Cleeff et al refer to this as "deperimeterization", implying that not only is the border of the organization's IT blurred, but also that the accountability for that border is dispersed (a problem exacerbated in data analytics and AI where responsibility for decision-making is not always clear (Sparrow, 2007). For example, "if the organization makes a decision to apply a certain data protection policy in its software, the data may in fact be managed by a different organization. How will the organization that actually manages the data implement and verify this?" (Cleeff et al., 2009, p. 51).

2.10 Business interests and codes of conduct

Competing interests are frequently perceived in security and profit. This may be seen as a zero-sum game in which any money spent on security is money which cannot be spent on increasing profit. However, this is clearly a flawed approach given the financial costs incurred in suffering a successful cyber attack. An example here is the decision of Marissa Meier, then CEO of Yahoo, not to inform the public of attacks in 2013 and 2014 regarding their accounts, most likely because such a revelation could have led to a loss in profit. Yet, when it became known, it devastated the company (Stone, 2017). In response to similar concerns, Macnish and van der Ham argue for the necessity of guidance on disclosure of vulnerabilities:

"public-spirited motivations should be protected from predatory practices by companies seeking to paper over cracks in their own security through legal action. However, current conventions as to how to proceed with disclosure of vulnerabilities seem to be skewed in the favour of corporations and against the interests of the public" (Macnish and van der Ham, 2019, p. 9).

They note that ethical problems cannot be solved easily, but propose creating a code of conduct for cybersecurity to provide guidance and a degree of consensus within the cybersecurity community regarding appropriate action in the face of attacks.

3. The Case Study of a Cybersecurity company using SIS

The literature review demonstrates a variety of ethical issues in cybersecurity. In this section our goal is to present the ethical problems that arise in practice. We aim to compare practice with academic literature concerning ethical issues of SIS in cybersecurity. This will help to inform both sides if there is a lack of understanding of the problems, and to enable mutual learning.

This case study focuses on the ethical challenges that SIS bring in cybersecurity to shed some light on the risks of this sector and how they are currently minimized. The interview was conducted with four employees as a group at Company A Headquarters in Scandinavia. All are experts in the Company A cybersecurity research team: Interviewee 1, a doctoral student; Interviewee 2, a researcher who focuses on core network security; Interviewee 3,a researcher who focuses on trusted computing; and Interviewee 4, a researcher with background in machine learning (see Table 1, below). The methodology employed for the interview can be found in *Understanding Ethics and Human Rights in Smart Information Systems: A Multi Case Study Approach*(Macnish et al., 2019).

3.1 Description of SIS technologies being used in Company A

Background research was initially conducted through investigating Company A's website and public documents from conferences. This was then supplemented by the interviewees' explanations of the technical capabilities of the technologies used at Company A.

Company A is a global digital communications company. It is involved in cloud computing, artificial intelligence, machine learning, internet of things and the infrastructure of mobile networks, including 5G. Company A's website refers to a combination of analytics and augmented intelligence, but the company also specialize in research and development (R&D) through Bell Labs, where it conducts research. Marcus Weldon, president of Bells Lab, in his book *The Future X Network*, shows the development of technology and the relation with global economy and society, by acknowledging the "scale of changes wrought by a nexus of global, high-speed connectivity, billions of connected devices (IoT), cloud services and non-stop data streaming, collection and big data analytics" (Marko 2015).

Clients' data gathering capability has expanded faster than their data analysis capability, so that they increasingly gather data that has no obvious purpose.

These technologies are changing our world and Company A sees itself as driving innovation and the future of technology to power this digital age and transform how people live, work and communicate. These technologies use data, including personal data from customers and metadata from phone networks. During the interview, Interviewee 1 argued that they do not use AI, but they do use statistics and analytics, such as products that use machine learning (ML) and data collection to identify malware. They also use analytics to create rules for developing effective firewalls for the network. However, Interviewee 3noted that AI is still part of the research and the internal projects:

"we do not sell a brain… or the giant quantum computing brain that solves all the problems, but for a very long time, planning has been used in many products, you can consider some configuration algorithms that can be considered as AI, these things exist, but not in the futuristic sense" (Interviewee 3 2018)

The term "cybersecurity" appears in different articles across Company A's website. The cybersecurity research team at Company A developed a report on security for 5G networks which has served as guidance for the European Union. They analyse bulk datasets to help clients (communications providers rather than end users) maximize efficiency and thus profit, while at the same time providing security such as malware detection to protect the end user from attacks.

SIS applications vary due to the amount and variety of data that Company A gathers from its customers, as well as the diverse needs of those customers. Many of these needs could not be met without SIS technology, as they would be impossible to perform by hand. For the most part, Company A's cybersecurity research team use rule-based applications for sorting information which is then evaluated by a person. Interestingly from an ethical point of view, Interviewee 1pointed out that clients' data gathering capability has expanded faster than their data analysis capability, so that they increasingly gather data that has no obvious purpose.

Description	Organisation 1
Organisation	Company A
Location	Scandinavia
Sector	Cybersecurity/Telecommunications
Name	Interviewee 1 Interviewee 3 Interviewee 2 Interviewee 4
Length	136 minutes

Table 1

3.2 The effectiveness of using SIS by Company A

As noted above, the use of AI and ML is due to the complexity and amount of data retrieved from clients' systems. According to Company A's website, cloud computing, AI, ML, IoT and 5G Networks are changing the world and they have the power to transform how we live, work, and communicate. Much of this is due to the fact that the operations now performed would previously have been impossible owing to the sheer volume and complexity of the data.

Company A has been using SIS in cybersecurity for some time. SIS allows the team to discover attempted hacks or other misuse such as fraud or the use of fake base stations (imitating a legitimate mobile phone tower in order to collect personal data). Current technology allows pre-filtering and sorting, but is less effective at identifying or responding to targeted attacks which are more sophisticated than bulk attacks. Interviewee 4 described a detection system they had worked on:

"one of their security teams was working on malware detection for telecom software for operators. That software ended up in systems that will protect end-users from malware that could be installed into phones. This is more at the operator level, not like an anti-virus which is for a phone users-level" (Interviewee 4 2018).

4. Ethical Implications in Cybersecurity

In this section we will look in greater depth at the ethical issues discussed during the interview conducted with the four employees at Company A. The issues which were uncovered in the interview widely reflect those found within the literature. It is however important to note that SIS use is growing rapidly: the technology is evolving and huge amounts of data are being collected. Generally, the interviewees explained that there is a lack of joint efforts from the ethical review boards within Company A and there is a need to continue and improve the dialogue between the ethical and technical fields.

The ethical issues discussed in the interview comprised of privacy; internationalisation, standardisation and legal aspects; monetisation issues; anomalies; policy issues, awareness and knowledge; security; risk assessment; and mechanisms to address ethical issues. Each of these will be discussed in greater depth in this section.

4.1 Privacy

Company A takes privacy seriously. Interviewee 2pointed out that they were involved in drafting the document for 5G networks concerning privacy and the future of 5G security, which became a guideline for the European Parliament and for national legislatures. Privacy was seen during the interview as one of the most important underlying ethical issues. Concerns about users' and companies' privacy were evident. Some discussion was held around the issue of "quantifying privacy" (how does one measure privacy?). However, further problems arise in sharing data with customers, which to Company A are telecommunications providers rather than end users, as the team often do not know what the customer knows. Hence, data that may be anonymous in one dataset may be re-identified when cross-referenced with another dataset which is proprietary to the customer.

"Sometimes if you manage to monetise your data, whatever data we're talking about, not just telco, and a buyer also has access to other sources of data that cross-correlate with your data, or have similar identifiers, you can never predict this as a seller of data. The end result is that your customer basically gets access to something that he can just map back to the original data, pretty much, by just looking at two fields and just cross-correlating. And you can never predict this. In that sense it's already doomed from that point of view, but it's a best effort sort of thing, and within a narrow context it still works"(Interviewee 4 2018)

Differential privacy, a technical "fix" for privacy concerns employed by Apple, among others(Apple, 2018) was also discussed. The team noted that differential privacy does not work with complete reliability because you can never be sure of what the data can lead to. Hence uncertainty also becomes an important issue in relation to privacy. Furthermore, Interviewee 3 considered that we should have a numerical measurement for privacy but that, they suggested, would not be possible.

4.2 Internationalization, standardization and legal aspects

Given the global nature of telecommunications, international cloud computing and the IoT, there is an increasing need for global regulation. Interviewee 4 introduced the problem of an application on mobile phones that sends data to China every 5 minutes: in such cases, which state's laws should be followed, those of the country where the user currently is, those of the state in which the user is registered as a citizen, those of the country where the operator is located, or those of the country of origin of the application operator, in this case China. Interviewee 2 argued that one of the issues that they have encountered is that the customer data comes from everywhere in the world. As Company A is a global company, it works also in places such as the Middle East or Asia, and not only receives information from European customers but from other parts of the world. She raised the question as to whether it would be ethical to see data from everywhere in the world when there are no clear guidelines. Interviewee 3 also pointed out the issues with different regulations:

"Northern Europe is doing well; Germany is most strict. Italy, Spain, Portugal strict. [Some others do not] really care"(Interviewee 3 2018)

Interviewee 2explained that European laws are much stricter than most other nations, and in following the European laws Company A restricts data sharing. It hence does not share data with third parties and has just one person looking at data

There was … general agreement that what mattered was not just being compliant with the letter of the law, but also the spirit.

unless there is a clear need for more. Interviewee 4 also pointed out that there is a Company A "sensitive data handling policy", which involves rules for data encryption and storage, which is closely monitored. Furthermore, special clearances are required to access some data, although the cybersecurity research team is in a "privileged" position to receive such data. Interviewee 4 noted that some data is not allowed to be copied, just processed on the server.

Interviewee 3 added that governments are also involved and there is a need for standardised practices:

"In telco we have some interesting issues that are coming up. It's not just telco versus attacker. You have two other players. Standardisation, where you try and make a level playing field for everyone. Then you've got governments, [say] security services, who might say, "Well, let's get rid of encryption, because bad guys use encryption" (Interviewee 3 2018).

Interviewee 3 explained that the spirit of GDPR is not about compliance but about risk management, and companies have to show that they are doing due diligence and minimizing the risks as much as possible. As an example of this, Interviewee 2suggested that in order to review data, you can ask for one group of phones instead of having access to the whole network, which would compromise a large number of people. In contrast, Interviewee 3 argues that according to US laws, the National Security Agency (NSA) are allowed to collect data of domestic individuals which they then send to the UK for analysis. There was also general agreement that what mattered was not just being compliant with the letter of the law, but also the spirit. The team noted that Finnish regulators in particular are not only concerned with compliance but also the motivations behind activities, and where the boundaries lie as to the limits of acceptable practice, which speaks of a high ethical standard.

4.3 Monetization issues

The team felt that the existence of public clouds and data sharing with different companies such as Amazon increases the potential for monetization of data. Different stakeholders are looking to monetize data, which is very privacy sensitive. Interviewee 1 argued that these new advances and technologies are helping to monetize customer's data, like targeted advertisements. Interviewee 4 added that some companies are seeking to monetize data within the current regulations, which is something that, according to Interviewee 4, must be questioned:

"are we doing the best we can before we monetize it, selling it, whether using it for mining – Is anonymization and privacy worth it? Can we prove to certain knowledge, mathematically, that this is anonymized… can we quantify that point?" (Interviewee 4 2018)

Some operators and senior managers … are guilty of "off-loading perfect expectations to machines" (Interviewee 1 2018).

However, the team agreed that not all operators have cybersecurity people, and not many people are working on telecommunications cybersecurity within operators. Thus, people that have expert knowledge are rare in this field. As Interviewee 2pointed out, there are relatively few European security teams; companies such as KPN and Orange have one, but not every operator does.

Furthermore, and related to the lack of security expertise, the team felt that there is a need to manage customers' expectations. Many customers place a high value on SIS even though they do not understand it *or* the level of security it can engender. Some customers "want perfect security right from the start" (Interviewee 3 2018). In addition, these expectations also hold true among some operators and senior managers who are guilty of "off-loading perfect expectations to machines" (Interviewee 1 2018).

4.4 Anomalies

Interviewee 4pointed out that in cybersecurity there is a need to search actively for anomalies. These have arisen for the team in the case of identifying fake base stations. Interestingly, Interviewee 4 mentioned that the U.S. has been trying to stop the news about these fake base stations because knowledge of their existence may damage the trust that people put in the networks.

"in China you have fake antennas or fake base stations which can push advertisements etc. to people's phones, and there have been thousands in China… In France, these fake base stations are used by the police to catch all the phones, not to do something malicious because is kind of the police enforcement, these are the so-called anomalies, when you have for a short period of time a phone for which service is delayed" (Interviewee 4 2018)

Interviewee 2 explained that they did not encounter many fake stations, but rather, they see attacks which seem to come from other network operators. e.g. a telecommunications provider in Barbados asking another telecommunications provider in Finland for the location of a Finnish subscriber, when there is no obvious technical need (such as to enable roaming). In such cases there is clearly no reason to give that information. Company A also makes use of firewalls to prevent attacks, but these need to be tailored to avoid false positives and blocking too much legitimate traffic.

4.5 Policy issues, awareness and knowledge

Company A holds mandatory ethics training for all staff, which covers privacy compliance. However, Interviewee 3suggested that it could be far more effective than is currently the case:

"it appeals to the lowest common denominator for everyone, when it says things like – you should apply privacy by design, you should use methods and processes…" (Interviewee 3 2018)

However, Interviewee 2 offers a more positive perspective, arguing that it is making both companies and users aware of the problem:

"at least the message gets through to every employee, that somehow we care, that you should think about that" (Interviewee 2 2018)

Interviewee 3noted that customer data is strictly regulated at Company A, with codes of conduct and legal frameworks to guide behaviour. The company's legal framework also provides a base from which to determine ethical decisions. Interviewee 4 explained that they had a data-security course which was mandatory, and so there are serious attempts to deal with the ethical implications of the work. Moreover, Interviewee 3 argued that users should also have technical knowledge and the technical competence regarding practicing safe behaviour online.

Compliance training could be improved, but it gets the message agree that privacy is important.

The team agreed that there is a need for more regulation. Interviewee 3 argued that privacy and data analytics should become regulated industries, similar to car management software, or software for medical devices, in which industries you have to keep the source code for 50 years, and it has to be documented and signed before it can be used. Interviewee 3 also mentioned that it is worth paying attention to the level of training for engineers regarding the need for an ethical background. Interviewee 3 explained that every engineer has to make ethical decisions at some point. As such it is important that engineers are free to object and refuse to participate in certain projects. Interviewee 2 added that they have an Ethics section in Company A that helps with these issues, providing support to employees who may have concerns. Furthermore, they stated that there is no code of conduct for cybersecurity.

4.6 Security

Interviewee 3 described how IT departments in some companies send internal "phishing mails" (emails attempting to trick the recipient into giving private information) to test their security, and the problem is that employees tend to have a high record on clicking on them, demonstrating a weak level of security awareness. Interviewee 3also explained that Company A, amongst other companies, have a "hackathon" every year to discover security flaws. Interviewee 4 mentioned that they have companywide encryption policies for some sensitive materials, which is easy to use now, but that was not the case in the past. Interviewee 4 felt that security is of importance at Company A, but, as Interviewee 1 pointed out, most research is conducted internally so that there is a lack of publications, at least for the public space. This leaves a number of unanswered questions, such as:

"who is attacking your system and what are they after - this hasn't been researched properly, or has been researched but not publicly available" (Interviewee 3 2018)

4.7 Risk Assessment

Interviewee 4noted that there is a lack of risk assessment regarding some key aspects of security, such as the risk of not having security protocols, or the comparative risk of predictive versus reactive strategies. Interviewee 3said that they had a PhD student currently studying cybersecurity attacks, and one of the things that came out of this research is that the attackers do not necessarily go for the weakest part of the system, because that is not where "the big game are". Therefore, this shows the need to have cybersecurity teams that will look for security pitfalls in every part of the system, even in the parts that are considered more secure by design.

Interviewee 3 further stated that there is a problem in that the technology they work with can be misused, e.g. used for spying on different countries. Interviewee 2 continued that even if the government has access to this information, the question still remains as to the extent to which citizens can be sure that no one else has the same access. What if a government's position changes, such as that of Germany in the 1920s and '30s? There is very little that can be done under such circumstances.

4.8 Mechanisms to address ethical issues

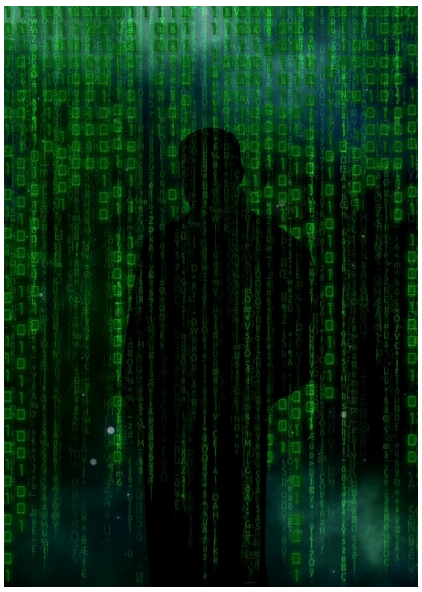
During the interview it was noted that there is a need for a culture of openness and challenge in organisations, and that the current paradigm of ethical standards in the use of SIS in cybersecurity is present but not developed. While the GDPR has improved general levels of awareness of cybersecurity and the importance of privacy, there is a need for ethical training for current engineers, as well as to develop stricter codes of conduct for this sector. The external regulations of, for example, targeted advertising and the issues of internationalization require consideration. Furthermore, while GDPR has a strong impact on privacy in Europe, other countries allow companies to gather data more freely.

Company A has a number of security strategies which go some way to addressing ethical concerns. Mandatory training sessions are held annually and policy documents provide guidance. These are supplemented by a culture of challenge and openness in which employees feel free to share their concerns and step back from working on a project with which they have ethical concerns. There are also security measures put in place to keep sensitive data secure, such as limiting the machines on which the data can sit, and operating a security clearance system such that only certain people are cleared to access the data.

Engagement with different stakeholders, such as the internal Company A units, the academic community, regulators and government agencies, clients and end users was deemed both desirable and beneficial for all.

5. Conclusion

The literature review and the interview highlight a correlation between academic understanding of the ethical issues in cybersecurity and those working for the cybersecurity industry. However, both have also shown a lack of joint efforts from academia and engineering, and the need to improve the dialogue between the two. There is concern that the level of technical abstraction of university-based development stifles ethical oversight of the development of new SIS technologies in computer science. At the same time, there is a need to include ethical oversight in industry, with clearer codes of conduct for the cybersecurity community. One of the strongest arguments from the team at Company A was the lack of clear codes for international practice. As SIS technology is being developed with cloud computing, and the facility to acquire data from all over the world grows, so there is a need to improve ethical protocols for companies.



One of the strongest arguments from the team at Company A was the lack of clear codes for international practice

Overall, it was shown that ethical concerns regarding SIS in cybersecurity go further than mere privacy issues. As it is a sector that will grow in the coming years, incorporating ML and the IoT, the importance of cybersecurity, and thereby the ethics of cybersecurity, will become more important.

Among the ethical issues we found the following: informed consent, protection from harm, disclosure of vulnerabilities, biases, the nature of hacking, trust, transparency, the necessity for a risk assess-

ment in cybersecurity, responsibility between companies, government and users. Interestingly, the issue of monetization (how far can one ethically go to monetize customer's data) appeared in the interview but is not one that has been widely discussed in the academic literature (see Table 2, below).

Issues arising in Literature Review	Issues arising in Interview
Similarities	
Protection from harm	Protection from harm
Privacy and control of data	Privacy and control of data
Competence of research ethics committees	Competence of research ethics committees
Security issues	Security issues
Risk	Risk Assessment
Business interests	Monetization issues
Codes of conduct	Policy issues (awareness and knowledge) and mechanisms to address ethical issues
Responsibility	Internationalization, standardization and legal aspects
Differences	
Vulnerabilities and disclosure	Anomalies
Trust and transparency	
Informed consent	

Table 2

5.1 Implications of this report

This report exposes some of the weakest part of SIS technology and the importance of cybersecurity, by supporting the claim that there is a need to improve the ethics of research in SIS. The cyber world is forming an important part of society and in some areas

at least, albeit not among the interviewees for this case study, there is a lack of understanding of the ethical problems that come with this, which can bring damage to many stakeholders.

5.2 Future research

This report argues for the need for multi-disciplinary studies between academia and the technical community to prevent ethical concerns from being undervalued. Future research goes hand in hand with legal implications, particularly at the international level, as well the need to create clearer codes of conduct for businesses and international practices, and the necessity to increase the cybersecurity teams within companies.

References

Allen, A.L., 1999. Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. Conn. L. Rev. 32, 861.

Apple, 2018. Privacy - Approach to Privacy [WWW Document]. Apple (Latin America). URL https://www.apple.com/lae/privacy/approach-to-privacy/ (accessed 12.17.18).

Bainbridge, L., 1983. Ironies of Automation. Automatica 19, 775–779. https://doi.org/10.1016/0005-1098(83)90046-8

Baldwin, D.A., 1997. The concept of security. Review of international studies 23, 5–26.

Beauchamp, T.L., 2009. Autonomy and Consent, in: Miller, F., Wertheimer, A. (Eds.), The Ethics of Consent: Theory and Practice. OUP USA, Oxford ; New York, pp. 55–78.

Bederson, B.B., Lee, B., Sherman, R.M., Herrnson, P.S., Niemi, R.G., 2003. Electronic Voting System Usability Issues, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '03. ACM, New York, NY, USA, pp. 145–152. https://doi.org/10.1145/642611.642638

Burnett, S., Feamster, N., 2015. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests, in: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication, SIGCOMM '15. ACM, New York, NY, USA, pp. 653–667. https://doi.org/10.1145/2785956.2787485

Byers, J.W., 2015. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests–Public Review. Technical Report http://conferences. sigcomm. org/sigcomm/2015/pdf/reviews ….

Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian.

Cleeff, A. van, Pieters, W., Wieringa, R.J., 2009. Security Implications of Virtualization: A Literature Study, in: 2009 International Conference on Computational Science and Engineering. Presented at the 2009 International Conference on Computational Science and Engineering, pp. 353–358. https://doi.org/10.1109/CSE.2009.267

Craigen, D., Diakun-Thibault, N., Purse, R., 2014. Defining Cybersecurity. Technology Innovation Management Review 4, 13–21.

Davis, M., 1991. Thinking like an engineer: The place of a code of ethics in the practice of a profession. Philosophy & Public Affairs 150–167.

EU Parliament, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L.

Glass, A., McGuinness, D.L., Wolverton, M., 2008. Toward establishing trust in adaptive agents, in: Proceedings of the 13th International Conference on Intelligent User Interfaces. ACM, pp. 227–236.

Goddard, K., Roudsari, A., Wyatt, J.C., 2012. Automation bias: a systematic review of frequency, effect mediators, and mitigators. J Am Med Inform Assoc 19, 121–127. https://doi.org/10.1136/amiajnl-2011-000089

Guiora, A.N., 2017. Cybersecurity: Geopolitics, Law, and Policy, 1 edition. ed. Routledge, Boca Raton, FL.

Hansson, S.O., 2013. The Ethics of Risk: Ethical Analysis in an Uncertain World. Palgrave Macmillan.

Hermansson, H., 2010. Towards a fair procedure for risk management. Journal of Risk Research 13, 501–515. https://doi.org/10.1080/13669870903305903

Hermansson, H., 2005. Consistent risk management: Three models outlined. Journal of Risk Research 8, 557–568. https://doi.org/10.1080/13669870500085189

Hess, C., Ostrom, E., 2007. Understanding knowledge as a commons. The mit press.

Ienca, M., Vayena, E., 2018. Cambridge Analytica and Online Manipulation [WWW Document]. Scientific American Blog Network. URL https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/ (accessed 7.10.18).

Johnson, M.L., Bellovin, S.M., Kromytis, A.D., 2012. Computer Security Research with Huma Subjects: Risks, Benefits and Informed Consent, in: Danezis, G., Dietrich, S., Sako, K. (Eds.), Financial Cryptography and Data Security. Springer, Berlin, pp. 131–37.

Latour, B., 2005. Reassembling the Social: An Introduction to Actor-Network-Theory. OUP Oxford, Oxford.

Lundgren, B., Möller, N., 2017. Defining Information Security. Sci Eng Ethics. https://doi.org/10.1007/s11948-017-9992-1

Macnish, K., 2018. Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World. Journal of Applied Philosophy 35, 417–432. https://doi.org/10.1111/japp.12219

Macnish, K., 2012. Unblinking eyes: the ethics of automating surveillance. Ethics and Information Technology 14, 151–167. https://doi.org/10.1007/s10676-012-9291-0

Macnish, K., Ryan, M., Stahl, B., 2019. Understanding Ethics and Human Rights in Smart Information Systems. 1 2. https://doi.org/10.29297/orbit.v2i1.102

Macnish, K., van der Ham, J., 2019. Ethics and Cybersecurity Research. Journal of Science and Engineering Ethics.

Manjikian, M., 2017. Cybersecurity Ethics, 1 edition. ed. Routledge, London ; New York.

Manson, N., O'Neill, O., 2007. Rethinking Informed Consent in Bioethics. Cambridge.

Miller, F., Wertheimer, A. (Eds.), 2009. The Ethics of Consent: Theory and Practice, 1 edition. ed. OUP USA, Oxford ; New York.

Moore, 2015. Privacy, Security and Accountability: Ethics, Law and Policy. Rowman & Littlefield, London ; New York.

Moore, A., 2003. Privacy: Its Meaning and Value. American Philosophical Quarterly 40, 215–227.

Nichols, S., 2016. St Jude sues short-selling MedSec over pacemaker "hack" report [WWW Document]. The Register. URL https://www.theregister.co.uk/2016/09/07/st_jude_sues_over_hacking_claim/ (accessed 7.4.18).

O'Neil, C., 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown/Archetype.

Pieters, W., 2011. Explanation and trust: what to tell the user in security and AI? Ethics Inf Technol 13, 53–64. https://doi.org/10.1007/s10676-010-9253-3

Singer, P.W., Friedman, A., 2014. Cybersecurity: What Everyone Needs to Know. OUP USA.

Smith, P.T., 2018. Cyberattacks as Casus Belli: A Sovereignty-Based Account. Journal of Applied Philosophy 35, 222–241. https://doi.org/10.1111/japp.12169

Sobers, R., 2018. 60 Must-Know Cybersecurity Statistics for 2018 [WWW Document]. Varonis Blog. URL https://www.varonis.com/blog/cybersecurity-statistics/ (accessed 12.17.18).

Sparrow, R., 2007. Killer Robots. Journal of Applied Philosophy 24, 62–77.

Spring, T., 2016. Researchers: MedSec, Muddy Waters Set Bad Precedent With St. Jude Medical Short. The first stop for security news | Threatpost. URL https://threatpost.com/researchers-medsec-muddy-waters-set-bad-precedent-with-st-jude-medical-short/120266/ (accessed 7.4.18).

Stone, N., 2017. The Yahoo Cyber Attack & What should you learn from it? [WWW Document]. Cashfloat. URL https://www.cashfloat.co.uk/blog/technology-innovation/yahoo-cyber-attack/ (accessed 12.17.18).

Tucker, E., 2018. Cyber security – why you're doing it all wrong [WWW Document]. ComputerWeekly.com. URL https://www.computerweekly.com/opinion/Cyber-security-why-youre-doing-it-all-wrong (accessed 12.17.18).

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

Wolff, J., 2010. Five Types of Risky Situation. Law, Innovation and Technology 2, 151–163. https://doi.org/10.5235/175799610794046177