CANVAS – Constructing an Alliance for Value-driven Cybersecurity

White Paper 1

Cybersecurity and Ethics

*Emad Yaghmaei, Delft University of Technology**
*Ibo van de Poel, Delft University of Technology**

Markus Christen, University of Zurich
Bert Gordijn, Dublin City University
Nadine Kleine, Ostbayerische Technische Hochschule Regensburg
Michele Loi, University of Zurich
Gwenyth Morgan, Dublin City University
Karsten Weber, Ostbayerische Technische Hochschule Regensburg

This report consolidates the findings of Work Package 1 of the CANVAS Support and Coordination Action; * Work Package Leader

The CANVAS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Content

Executive Summary

This White Paper outlines **how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located**. The White Paper is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. For each domain, a systematic literature search has been performed in two databases (Web of Science and Scopus), complemented with snowballing and expertise of the involved authors. The search yielded 74 papers for the health domain, 33 papers for the business domain and 129 papers for the national security domain. Those papers discussed ethical issues of cybersecurity in a significant way and they were chosen for providing an overview on how ethical issues have been discussed in the cybersecurity domain.

A first observation is that the ethics of cybersecurity **not an established subject**, academically or in any other domain of operation. It is actually a rather under-developed topic within ICT ethics, where the majority of published work discusses issues such as "big data" and privacy or ethical issues of surveillance. In those cases, cybersecurity is usually only instrumentally discussed as a tool to protect (or undermine) privacy.

A second observation is that there are both common theme and differences across the three domains examined. In all domains, cybersecurity is recognized as being an **instrumental value**, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is perhaps the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data. The most prominent difference across the three domains regards the value of privacy, that is emphasized in business and health (together with confidentiality), but not in the national security domain, which appears concerned, above all, with the protecting the security and connectivity of infrastructure

The target audience of this White Paper is not only the philosophy and ethics of technology community, but also practitioners in cybersecurity – such as providers of security software, CERTs or Chief Security Officers in companies. This White Paper should provide a first orientation in the growing landscape where cybersecurity and ethics meet. The appendix lists papers identified in the search that allow the reader to explore the issue further.

CANVAS White Papers – Overview

In order to summarize the existing literature on the topics and issues that are relevant for the CANVAS project, the CANVAS consortium has created four White Papers as follows:

- White Paper 1 – Cybersecurity and Ethics: This White Paper outlines how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The White Paper is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. For each domain, a systematic literature search has been performed and the identified papers have been analysed using qualitative and quantitative methods. An important observation is that the ethics of cybersecurity not an established subject. In all domains, cybersecurity is recognized as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data.
- White Paper 2 – Cybersecurity and Law: This White Paper explores the legal dimensions of the European Union (EU)'s value-driven cybersecurity. It identifies main critical challenges in this area and discusses specific controversies concerning cybersecurity regulation. The White Paper recognises that legislative and policy measures within the cybersecurity domain challenge EU fundamental rights and principles, stemming from EU values. Annexes provide a review on EU soft-law measures, EU legislative measures, cybersecurity and criminal justice affairs, the relation of cybersecurity to privacy and data protection, cybersecurity definitions in national cybersecurity strategies, and brief descriptions of EU values.
- White Paper 3 – Attitudes and Opinions regarding Cybersecurity: This White Paper summarises currently available empirical data about attitudes and opinions of citizens and state actors regarding cybersecurity. The data emerges from reports of EU projects, Eurobarometer surveys, policy documents of state actors and additional scientific papers. It describes what these stakeholders generally think, what they feel, and what they do about cyber threats and security (counter)measures. For citizens' perspectives, three social spheres of particular interest are examined: 1) health, 2) business, 3) police and national security.
- White Paper 4 – Technological Challenges in Cybersecurity: This White Paper summarizes the current state of discussion regarding the main technological challenges in cybersecurity and impact of those, including ways and approaches to addressing them, on key fundamental values. It provides an overview on current cybersecurity threads and countermeasures and focuses on ethical dilemmas that emerge when counteracting those threads. It also points to the fact that the cybersecurity community relies much more on interpersonal relations when sharing intelligence and data than in explicit national or supranational regulations. Furthermore, the White Paper presents advanced cryptographic techniques and data anonymization techniques that may help to solve or minimize some of the ethical dilemmas.

All White Papers and additional material are available at the Website of the CANVAS project: www.canvas-project.eu

1. Introduction

1.1 Goal

The increasing use of information and communication technology (ICT) in all spheres of modern life makes the world a richer, more efficient and interactive place. However, it also increases its fragility as it reinforces our dependence on ICT systems that can never be completely safe or secure. Therefore, cybersecurity has become a matter of global interest and importance. Accordingly, one can observe in today's cybersecurity discourse an almost constant emphasis on an ever-increasing and diverse set of threat forms, ranging from basic computer viruses to cybercrime and cyberespionage activities, as well as cyber-terror and cyberwar. This growing complexity of the digital ecosystem in combination with increasing global risks has created the following dilemma: Overemphasizing cybersecurity may violate fundamental values like equality, fairness, freedom, or privacy. On the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure as well as in policy makers and state authorities.

The goal of this White Paper is to show how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The White Paper is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. "Ethics and cybersecurity" is not an established subject, academically or in any other domain of operation. It is actually a rather under-developed topic within ICT ethics, where the majority of published work discusses issues such as "big data" and privacy or ethical issues of surveillance. In those cases, cybersecurity is usually only instrumentally discussed as a tool to protect (or undermine) privacy. Nevertheless, cybersecurity raises a plethora of ethical issues such as "ethical hacking", dilemmas of holding back "zero day" exploits, weighting data access and data privacy in sensitive health data, or value conflicts in law enforcement raised by encryption algorithms. Those issues are in most cases discussed without the claim to gain an integrative view on the ethics of cybersecurity.

Hence, the goal of this White Paper is twofold: first, to identify the emerging landscape of ethical issues, concerns, and topics as they are mentioned in the literature and, second, to provide a value framework as both a philosophical compass and synthetic portray of the emerging ethical issues. The target audience of this White Paper is not only the philosophy and ethics of technology community, but also practitioners in cybersecurity – such as providers of security software, CERTs or Chief Security Officers in companies. All those people increasingly realize the ethical dimensions of their work. This White Paper should provide a first orientation in the growing landscape where cybersecurity and ethics meet.

This White Paper emerges from the Horizon 2020 project CANVAS – Constructing an Alliance for Value-driven Cybersecurity. This consortium unifies technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. Among others, CANVAS aims to create a reference curriculum for value-driven cybersecurity with a focus on industry-training, briefing packages for policy stakeholders, and a MOOC (massive open online course) on value-driven cybersecurity. This White Paper is part of the dissemination strategy of the project. It will serve as a basis for scientific contributions written by members of the CANVAS consortium and will inform participants of future CANVAS workshops that aim to unify stakeholders in the cybersecurity sector for discussing the ethical implications of their work.

1.2 Methodology

The aim of this White Paper is to provide an overview on the existing literature on cybersecurity and ethics. Therefore, the main element of the methodology consists in an extensive literature search in two standard databases: the Web of Science Core Collection and Scopus. The details of the literature search and analysis are outlined in the Appendix – here we only sketch the main steps as follows:

1. We scanned the literature through a systematic literature search for detecting papers within the cybersecurity domain that discuss ethical issues in a relevant way. We did this for three different domains: health, business/finance and national security. We used validated Boolean search expressions as outlined in the appendix; the resulting papers were then evaluated by experts with respect to their relevance. The list of papers identified in that way was complemented by snowballing (i.e., we checked which papers were cited by the identified papers and evaluated them as well with respect to expertise) and further expertise of the involved researchers. The result of this first step is a list of papers per domain that discuss ethical issues of cybersecurity. We used a common visualization tool (word clouds) such that the reader obtains an intuitive overview on the content of those lists.
2. We split in three teams, one for each domain, to read each relevant paper in its entirety and to single out the ethical issues it describes. Those ethical issues were classified in broader groups and the frequency of those issue classes was calculated. The result of this second step is a list of issue classes weighted by the frequency if its appearance.
3. We analysed the issue classes with respect to the values that were at stake. The result of this third step is a domain-specific characterization of values that are considered important in the ethics of cybersecurity discourse.

The results obtained by this methodology are then discussed in order to obtain the following results:

- The final lists of relevant papers for each domain are first characterized by quantitative means using some bibliometric metrics. We analysed the institutional background of the authors including geographic origin and funding, the types of sources and papers, and the disciplinary attribution of the papers and those papers that cite them in order to characterize the information flow across broader disciplinary categories (in terms of citations). We then analysed commonalities and differences between the tree domains.
- We then provided a qualitative evaluation of the results of steps 2 (issue list) and 3 (value characterization) in order to get a more fine-grained picture on how ethical issues of cybersecurity are discussed and to what extent this depends on the characteristics of the domain.
- Finally, using the expert knowledge in ethics of the author team, we identified “blind spots” in the current ethics discourse. Those are either issues that are under-represented in certain domains although it is plausible that they appear there as well, or values that do not show up as points of reference in the discourse, although there is reason to believe that they should play a role.

1.3 Definition of Terms

1.3.1 Cybersecurity

The term “cybersecurity” is a very young term in the scientific literature. Both “Web of Science” and Scopus locate the first papers that explicitly use this term (in title, abstract or keywords) in 2002; 95% of all papers that explicitly contain this term have been published in the last 10 years (i.e., since 2007).

There is furthermore no fully agreed definition of "cybersecurity". In 2008, the International Telecommunication Union (ITU) defined cybersecurity as the…

"(…) collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability, integrity and confidentiality of systems and data, which may include authenticity and nonrepudiation" (ITU 2008).

The more popular definitions entailed in dictionaries put a much narrower focus either on the protection of data[1] or computers[2]. However, the topics associated with this broad spectrum entailed in the ITU definition (and the dictionary definitions) are certainly much older and have been discusses for quite some time within computer science. We therefore used rather broad set of keywords for characterizing the cybersecurity domain (as explained in the Appendix). Nevertheless, also this broad keyword set yields – in quantitative terms – a clear emphasis of the publication activities in the last few years (Figure 1). The time series also indicates some dynamics; i.e. we find a first local maximum in 2010 (we did not further analyse the reason for this phenomenon).

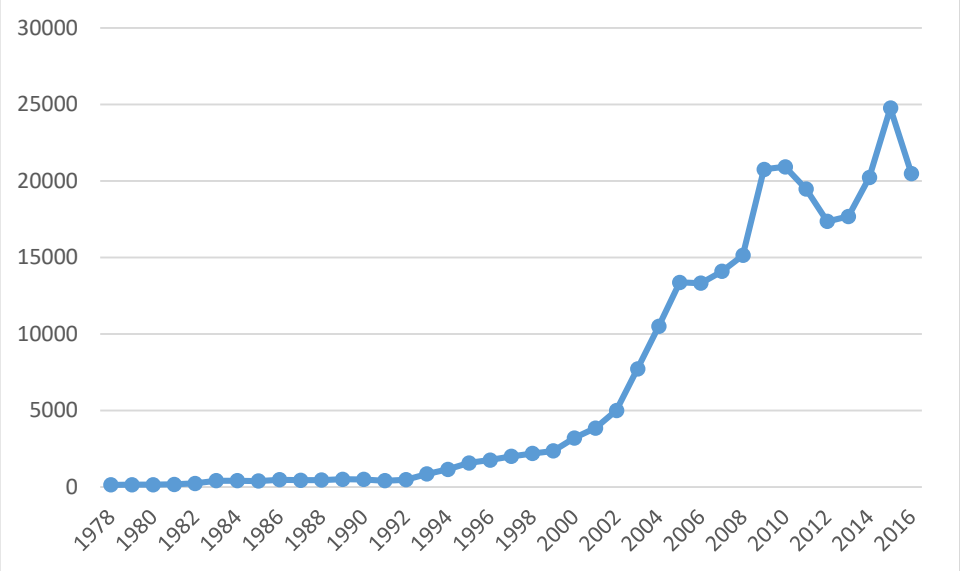

Figure 1: Number of cybersecurity papers: Time series showing the publication dynamics of the general cybersecurity literature in absolute numbers (database: Scopus). The y-axis shows the absolute number of publications

1.3.2 Ethical Issues

Another key term in this White Paper is "ethical issue". By this term, we denote any instance of a real world effect of a certain cybersecurity measure, policy, action etc. that has been described using an ethics terminology. By "describing" we mean that this instance has been regarded as a measure that

[1] The Oxford Dictionaries defines 'cybersecurity' as: *The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this*; see http://www.oxforddictionaries.com/definition/english/cybersecurity?q=cyber+security

[2] The Merriam Webster dictionary defines 'cybersecurity' as: *Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack*; see http://www.merriam-webster.com/dictionary/cybersecurity

either helps to enforce or protect an ethical value, norm or virtue, or that this instance is endangering or in conflict with an ethical value, norm or virtue. The notion of an "ethics terminology", respectively "ethical" value, norm or virtue is not precisely defined in the literature. Referring to the huge literature body in moral philosophy and research in empirical ethics (see e.g., Christen et al. 2014 for an overview), people associate ethical values (norms, virtues, etc.) usually with something that claims to be universally valid and whereas its corresponding actions are judged as right or wrong (philosophical dimension of morality; setting aside moral relativism), that usually refers to the goals of a community, common interest or the relationships among individuals (social dimension of morality), and that often refers to the collaboration, cooperation or communication between human beings or institutions (anthropological dimension of morality; see Christen et al. 2014b for details). In the following, we will use those characteristics as "markers" for ethical issues.

1.3.3 Values

Yet another key term in this paper is "value", that we take here as the standard point of reference with respect to an ethical orientation (i.e., we will not use the notion of "norm" or "virtue", although some instantiations of what we call "value" in this white Paper can reasonably also be called a "norm" or in some cases even a "virtue"). In very general terms, we denote by ''value" any term that individuals or institutions consider being a positive goal worthy of achievement. For example, profit is a positive orientation in business and beauty is a positive one in art. Certainly, not all those positive orientations are ethical values – those would be values where we reasonably can assume that they are in line with the characterizations given in Section 1.3.2. The number of potential moral values is large (see e.g. the Study of Christen et al. 2016 that investigated 460 value terms). However, the number of values we consider important is manageable, but varies considerable when comparing the different perspectives analysed in the four White Papers (Table 1) and consists of the following:

Values investigated in ethical research	"European" Values	Values investigated in empirical research	Values referred to in the technical domain
Autonomy	Human dignity	Privacy	Privacy
Beneficence	Freedom	Security	Fairness
Dignity	Democracy	Trust	Autonomy
Equality	Equality		
Fairness	Non-discrimination	*Suggested data protection goals:*	*Practical goals of cybersecurity technology:*
Freedom	The rule of law	Availability	Availability
Justice	Respect for human rights	Confidentiality	Confidentiality
Privacy	Pluralism	Integrity	Integrity
Responsibility	Tolerance	Intervenability	
	Justice	Transparency	
	Solidarity	Unlinkability	
	Protection of EU citizens		

Table 1: Different outline of the value landscapes that emerged in the four perspectives analyzed by the CANVAS White Papers: ethics (White Paper 1), law (White Paper 2; "European values"), empirical research (White Paper 3) and cybersecurity technology (White Paper 4).

The exact understanding of those values is subject of extensive philosophical debates (e.g., there is a rich literature on the notion of "autonomy"), and some authors would argue that certain values are entailed in other values or that some values are much closer connected to each other than others. Furthermore, there is also evidence that people even in the same culture may understand values differently based on their professional background (Christen et al. 2014b). Therefore, it will be important to capture – at least to a certain degree – the differences in understanding of those values.

2. Results

2.1 Health Domain

2.1.1 The "moral character" of the Health Domain

In Western culture, at least since the time of ancient Greece, there has been a great deal of thought given to the value of health for a successful life. It is not for nothing that the Hippocratic Oath still refers to the eponymous physician and philosopher, even though he lived almost 2500 years ago. Epicurus, who lived in the third century B. C., also gives us thoughts on the importance of health. This thinking continues to this day. It is probably no exaggeration that health, despite all the problems of a precise definition, enjoys high priority in all cultures. Therefore, in order to protect health, the WHO has formulated the right to health as a central human right.

If one agrees that health is an important, if not most important, value to human beings then a health care system that can provide effective and efficient help in case of medical problems also is most valuable. In this White Paper we will not discuss questions of justice with regard to health care and we will also not discuss the benefits and burdens or the moral justifications of the different ways to maintain and finance an effective and efficient health care system. However, such a health care system needs resources and providing these resources is becoming more difficult. As Nancy Lorenzi (2005: 2) puts it, currently "[a]lmost every major economy in the world experiences the effects of the high cost of health care, and many, if not most, national and regional governments are in some stage of healthcare reform."

In many, if not almost all, attempts to reform an existing health care system, the development and implementation of information and communication technology (ICT) to support the provision of health care services is a major part of those reforms. One of the main purposes of ICT systems in health care is the administration of information about patients and treatments that "[…] is a vital but complex component in the modern health care system. At a minimum, health care providers need to know a patient's identity and demographic characteristics, recent and distant medical history, current medications, allergies and sensitivities, chronic conditions, contact information, and legal preferences." (McClanahan 2007: 69). But McClanahan (2007: 69) also stresses that "[t]he increased use of electronic medical records has created a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain".

Employing ICT in health care therefore creates new value conflicts or at least makes old conflicts and problems more visible or increases their urgency. At the same time, it has to be stressed that "[i]mprovements in the health status of communities depend on effective public health and healthcare infrastructures. These infrastructures are increasingly electronic and tied to the Internet. Incorporating emerging technologies into the service of the community has become a required task for every public health leader." (Ross 2003: v) In other words, stakeholders like patients, health care professionals, health care providers, or insurance companies as well as societies as a whole are confronted with competing or even contradicting aims with regard to the health care system, for instance:

- increasing efficiency,
- reducing costs
- improving quality, and
- keeping information secure.

Simultaneously, the moral values mentioned above also shall be protected and supported, either as fundamental moral values in European societies and/or as moral values, which are constitutive for the relationship between patients on the one side and health care professionals on the other side. Such conflicts of aims and values raise moral concern since it has to be decided which aim and which value should be prioritized.

In fact, the situation is even more complicated because there are not only the above-mentioned conflicts, but also medically related conflicting goals and values. One example is the conflict between beneficence and autonomy: When ICT is used in the health sector, it shall be aimed at ensuring that patients themselves determine when which information is revealed to whom – password protection and encryption are common measures to maintain that aim. However, in emergencies, when patients are no longer able to make this decision, there is now a risk that important medical information will no longer be accessible. Moreover, it might be very helpful to widely share medically relevant patient information among health care professionals to improve the quality and efficiency of treatment. However, the goal of protecting patients' privacy and autonomy may be at odds with this aim. Additionally, as the literature search described below shows, in scholarly debates it is often mentioned that to provide cybersecurity it might be necessary to compromise privacy. This raises particular concern, because it is obvious that both the protection of patients' privacy and the security of information systems and the patient data organized in them must be important objectives in health care. Without privacy, the confidence necessary for medical treatment is jeopardized and without certainty that patient data will not be tampered with or stolen, the treatment itself is at risk.

2.1.2 Summarizing the result of the literature search

Based on the structured literature search of the UZH team, a list of 1361 results regarding ethics in cybersecurity and health was provided (see Appendix A.1 for details). The titles and abstracts of these results were evaluated. Criteria for exclusion were:

- Papers written before 1996.
- Papers written in a language other than English.
- Papers which have no significant content-related relevance.

After sorting out obviously irrelevant results, 108 findings remained and were examined in a further full-text review. Finally, 36 papers could be classified as relevant. In the next step, we checked additional papers that are cited or mentioned in these findings. Within a two-round-snowballing-process, a further 36 relevant papers were found. To complete the list, 3 papers were added based on the expertise of the group. This process yielded 75 papers that we estimate as being relevant for ethics in cybersecurity regarding health. Notably, these include technically oriented papers with the focus on architecture and design of technologies, overviews about ethical issues that may accompany these, and guidelines about how to deal with them.

The findings of the literature reflect the importance of specific ethical issues related to data and information technology that are quite widely discussed in the biomedical ethics community. It becomes apparent that in this context, it is not necessarily completely new, but rather well-known ethical issues and values which play a role.

The results show that only a few texts refer directly and explicitly to ethical issues and values related to cybersecurity and health. Most of the texts touch on such questions only indirectly. It should be noted that the topics described in more detail below are certainly also discussed in numerous other papers, which are not listed here due to our focus and method.

In order to provide a first overview on the ethical issues that were discussed in the final list of papers, we generated a word-cloud[3] that displays the frequencies of terms related to the issues.

[3] For creating the word cloud, all papers were characterized with a standardized set of keywords. The image has been created using the word cloud generator made available by https://www.jasondavies.com/wordcloud/ with a rectangular shape and a linear (n) scale and 6 different orientations.

Figure 2: Word cloud of issues identified in the final list of ethics papers of the health domain.

The majority of those papers discuss ***health related electronic information***, more precisely the storage, exchange and usage of patients' (big) data.

- Above all, that requires electronic information databases such as *Electronic Healthcare Records* (EHR), which are increasingly implemented in health facilities. The major advantage of these records, besides cost efficiency, is the fast and uncomplicated exchange of health related data between organizations (i.e. van der Linden et al. 2009; McGraw et al. 2009; Laur 2015). The employment of electronic information is diverse: It plays, for example, an important role in the emergency department (Ayatollahi et al. 2009) or is used in connection with maternal and child health registries (Myhre et al. 2016). Furthermore, electronic health information has a seemingly big impact on counselling and psychological therapy (Barros-Bailey & Saunders 2010; Allen & Roberts 2011; Kotsopoulou et al. 2015). The use of electronic data is changing the relationship of patients and health professionals (Kluge 2011). Many papers address security and privacy problems regarding EHR (i.a. Barrows & Clayton 1996; Dong et al. 2011; Ozair et al. 2015; Rahim et al. 2013; Stahl et al. 2014). In those papers, different approaches of how to deal with security and privacy could be identified: particularly, that includes technical solutions (e.g. biometric authentication (Rodriguez & Santos 2013), secure systems (Xiao et al. 2008)) and ethical guidelines (Buckovich et al. 1999; de Abajo et al. 2007; The Academy of Medical Sciences 2006).
- Another form of relevant health related data is *genomic data*. This covers whole genome sequencing (Gutmann et al. 2012), large-scale genetic data sets (Wjst 2010) and human biobanks (Cambon-Thomsen et al. 2007). Two use cases of genomic data become especially apparent:
  - First, personal genome testing (Bunnik et al. 2011), which can be used for insurance and employment (Godard et al. 2003); the best-known example of a broad databank of personal genome testing data is the deCODE genetics database project in Iceland (Árnason 2004).

  - Second, the use of genomic data for research (Docherty & Lone 2015) under particular consideration of different ethical values (Caulfield et al. 2008; Hoedemaekers et al. 2007; Lowrance 2006; Peddicord 2010; Vayena et al. 2016; World Medical Association 2013).

- *Geographic information* (Olvingson et al. 2003) and *geospatial data* (Lane & Schur 2010) play also a role for the health domain.
- *Biomedical data collected via apps*, provided by individuals themselves (Vayena et al. 2016)

Some of the papers discuss explicitly the ***security of different technologies*** that are relevant for health and healthcare.

- Technologies used in *telemedicine* are mentioned (Kaplan & Litewka 2008) as well as the potential for life improvement (Devillier 2016) and the importance of their users' acceptance (Saigí-Rubió et al. 2016; Tieu et al. 2015).
- Design and architecture of technologies for *home care and for support of an independent life* at home, so-called Ambient Assisted Living (AAL) systems are also discussed (Ikonen & Kaasinen 2009; Rothenspieler et al. 2011; Spitalewsky et al. 2013).
- Other papers focus on *mobile applications* such as personal health apps (e.g. Project HealthDesign, Olmsted et al. 2015) and apps for self-tracking one's own body function and behaviour (e.g. sexual and reproductive activities, Lupton 2015).
- The design of *implantable medical devices* entail challenges, too: On the one hand, devices, e.g. brain-computer interface technologies (BCIs) (Ienca & Haselager 2016) have to be protected (Camara et al. 2015), on the other hand they have to remain available for everyone (i.e. Altawi & Youseff 2016).

Moreover, it becomes apparent that ***vulnerable groups*** and those with special needs must be taken into particular consideration.

- Due to the '*digital divide*', people who have little or no experience with the application of electronic or digital technologies can face disadvantages regarding health related services (Chang et al. 2004).
- This also applies to people with *limited health literacy* (e.g. in case of use of online portals, Tieu et al. 2015).
- The literature shows that particularly the *elderly* form a group with special needs and interests which could present a barrier by the adoption of health related technologies (Devillier 2016; Young et al. 2014).
- People with *dementia, Alzheimer's, or other cognitive handicaps* present a special case (i.e. Batchelor et al. 2012).

2.1.3 Outlining the identified ethical issues

Based on the literature found, a list of ethical issues regarding cybersecurity in the health domain could be revealed as follows.

26 papers address ***technical security issues*** in a health context, both in general (i.a. Chow-White et al. 2015; Kaplan & Litewka 2008; Rothenspieler et al. 2011; The Academy of Medical Sciences 2006) as well as specific problems. These include:

- difficulties with *storage & communication* of data (Dong et al. 2012; Kotsopoulou et al. 2015),
- difficulties concerning *reliability* (Ikonen & Kaasinen 2008; Ozair et al. 2015; Spitalewsky et al. 2013),

- difficulties regarding *usability* (Kaplan & Litewka 2008; Spitalewsky et al. 2013; Young et al. 2014),
- *open access* (Greenbaum et al. 2011; McCormack et al. 2016), and especially
- the *risk of hacking and other forms of attacks* (Motti & Caine 2015; Mulligan & Schneider 2011; Tieu et al. 2015; Yang 2016), which could directly affect the physical and psychological safety of affected individuals (Camara et al. 2015; Ienca & Haselager 2016).

Security issues, among other factors, could lead to another crucial issue that was mentioned in 28 papers: the ***loss of control***.

- This regards firstly the concerns regarding *access control*, which comprises everything from an unclear data access authorization (Dong et al. 2012; Stahl et al. 2014) over lacking some control (Ikonen & Kaasinen 2008; Motti & Caine 2015; Olmsted et al. 2015; Olvingson et al. 2003) to a complete loss of control with regard to personal information (Barrows & Clayton 1996; Caulfield et al. 2008).
- The consequence could be *unauthorized access* by others (Buckovich et al. 1999; Greenbaum et al. 2011; Myhre et al. 2016), e.g. in a professional medical context (Ayatollahi et al. 2009; Caldicott & Manning 2013; McGraw et al. 2009; van Allen & Roberts 2011; Wallace 2015; Wang et al. 2013; Xiao et al. 2008).
- The other type is the *loss of control over one's own data* (Barrows & Clayton 1996; Caulfield et al. 2003; Mascalzoni et al. 2015). This is noticeable regarding a lack of possibilities to manage one's own data (Bourret & Pestana 2015; Thilakanathan et al. 2016), a lack of control over the concrete use of the data (Greenbaum et al. 2011; Ienca & Haselager 2016; Rodrigues & Santos 2013; Vayena et al. 2016) and, in the worst case, the risk of losing ownership of one's own data (Kluge 2011). This loss can be a risk to the empowerment of the patients (Bourret & Pestana 2015; Spriggs et al. 2012).

The less security and control one has over one's own data, the more urgent the ethical issue of ***misuse of data*** becomes, as discussed on different levels in 41 papers.

- A form of misuse is *unauthorized modification* (Barrows & Clayton 1996; Stahl et al. 2014; Wang et al. 2013), *manipulation* (Kaplan & Litewka 2008; Kluge 2011), or *sabotage* of data (Williams 2008).
- Furthermore, *data theft* (i. a. Buckovich et al. 1999; Myhre et al. 2016; Ozair et al. 2015; Thilakanathan et al. 2016) and thus identity theft (Peddicord et al. 2010; Rodrigues & Santos 2013; Rothenspieler et al. 2011) are crucial issues.
- However, the most important risks of misuse of data are the *disclosure of information* (mentioned by 32 papers, i. a. Abbas & Kahn 2014; McGraw et al. 2009; Wjst 2010) and a possible identification via the data (mentioned by 14 papers, i. a. Chow-White et al. 2015; Lane & Schur 2010; The Academy of Medical Sciences 2006), which may increase the risk of surveillance (Mulligan & Schneider 2011; Ozair et al. 2015; Rothenspieler et al. 2011).

The stated issues seem to have at least some effect on confidentiality; 21 papers outline ***confidentiality & trust issues***.

- On one hand, there is a *lack in confidentiality* related to technologies (Rahim et al. 2013; Saigí-Rubió et al. 2016) and security systems (Olvingson et al. 2003; Tieu et al. 2015).
- On the other hand, the *trust in professionals and medical staff* is also an issue (Ayatollahi et al. 2009; Visvanathan et al. 2011; Williams 2008); confidentiality seems to be crucial (Caldicott & Manning 2013; France 1998; Wallace 2013), especially in counselling settings (Barros-Bailey & Saunders 2010; Kotsopoulou et al. 2015; van Allen / Roberts 2011).
- Due to the use of technologies and electronic data in the context of health, the *relationship between professionals and patients* is about to change (Kaplan & Litewka 2008; Visvanathan

2011; Williams 2008; Yang 2016), which stresses the role of trust within that relationship even more (Kluge 2011).
- Moreover, *trust in medical research*, esp. genome testing, is lacking (Bunnik et al. 2011; de Abajo et al. 2007; Lowrance 2006).
- Another notable point is the issue of trusting (quantified) data without questioning the *validity* (Godard et al. 2003), which could lead to psychological harm (Bunnik et al. 2011).

It becomes apparent that ***consent problems*** also play an important role in cybersecurity and health; 30 papers address this issue, mostly with regard to genomic data.

- The problem regarding a general (Greenbaum et al. 2011) or presumed consent (Caulfield et al. 2003) is based on the uncertain use.
- While informed consent relates to a specific use (Ikonen & Kaasinen 2008), it does not include the further use of samples (Cambon-Thomsen et al. 2007; Chow-White et al. 2015; Spriggs et al. 2012; Vayena et al. 2016).
- Unauthorized use of data is in ongoing processes, e.g. clinical and research trials, is almost inevitable (Ienca & Haselager 2016; Mascalzoni et al. 2015; McCormack et al. 2013). The future use of data is unpredictable for individuals (Árnason 2004; Caulfield et al. 2008; also for non-medical use e.g. for insurance or employment purposes: Godard et al. 2003), and it is difficult (if not, due to anonymous donations, impossible) to re-contact the donor of the information in every new case of use (U.K. Biobank 2007). The lack of possibilities to establish contact is also evident in the case of unintentional findings or findings, which should be communicated to the persons concerned if necessary. (Bunnik et al. 2011).
- Besides the organizational difficulties, there are also problems due to a lack of capacity to give informed consent (Batchelor et al. 2012). That includes children (Hens et al. 2011) and people with cognitive deficiencies like Alzheimer (Devillier 2016).
- Moreover, the characteristics of genetic data provides information about relatives and (yet unborn) descendants of the original donor without their consent (Caulfield et al. 2008; Godard et al. 2003; Wright et al. 2013).
- It is generally possible to (re-)identify people (e.g. their health status, relationship link, dispositions) based on genetic information (i.a. Docherty & Lone 2015; Lowrance 2006; Vayena et al. 2016; Wright et al. 2013) and to commercialize this knowledge (Cambon-Thomsen et al. 2007; Lupton 2015).

These issues, among others, could indirectly bring ***harm to vulnerable groups***, a risk which is addressed in 19 papers.

- It is possible to monitor health related behaviour through collected electronic information and therefore, would be possible to punish unhealthy lifestyle choices (Spriggs et al. 2012).
- However, concrete behaviour is not the only possible factor leading to disadvantages: People could have a disadvantage due to a limited health literacy (Tieu et al. 2015) or due to lack of knowledge about technology use ('digital divide': Chang et al. 2004).
- The information about current or potential health issues can also lead to unfair treatment (Godard et al. 2003; (McGraw et al. 2009).
- Stigmatization, discrimination and exclusion of vulnerable groups based on genetic data (i. a. Bunnik et al. 2011; Mascalzoni et al. 2015; McCormack et al. 2016), is imaginable, e.g. of specific ethnic groups (de Vries et al. 2012).
- In order to make sure that everyone has access (Ikonen & Kaasinen 2008; Olmsted et al. 2015), it is crucial to consider the special characteristics and needs of individuals and groups when implementing technology in health related settings (World Medical Association 2013; e.g. dementia: Batchelor et al. 2012).

When considering different ethical issues regarding cybersecurity and health, two major conflict sets become apparent.

1) First, the ***competing interests of the individuals concerned***: The request for guaranteed privacy and security by using technical devices and electronic data contradicts with beneficence (Yang 2016); health information has to be accessible, e.g. in order for health professionals to take care of individuals in the right way (Barrows & Clayton 1996; Buckovich et al. 1999). The identification of a person (and their specific needs) facilitates the promises of health related technologies such as individual, fast, self-determined and comfortable treatment of patients (Laur 2015; Motti & Caine 2015). This, however, is not in line with a privacy-enabling, secure system (Kaplan & Litewka 2008). Confidentiality of patient's data can also contradict with the necessary access, esp. in emergencies (Ayatollahi et al. 2009; Lane & Schur 2010; Rock & Congress 1999). This dualism of privacy, security and confidentiality on one side, and transparency, accessibility and accountability on the other side (Wynia et al. 2011) is a main unsolved issue regarding health and cybersecurity.

2) The second major issue is the ***conflict between individual and public interests***. While individuals, as already stated, show great interest in security, privacy and confidentiality of data, health organizations aim to reduce costs and make patients' treatment more efficient and thus, more useful – not just on the individual level, but for the public as a whole (Mascalzoni et al. 2015; Saigí-Rubió et al. 2016). That also includes the importance of accessible health data for significant information about the public health status: the collection and sharing of as much health related data as possible could be used to find new information about diseases and possible treatments (Olvingson et al. 2003; Vayena et al. 2016). Genomic research is especially seen as a promising approach to bring about progress in public health (Caulfield et al. 2008); it could even be argued that participating in biobanks is an act of solidarity (Hens / Lévesque / Dierickx 2011; Hoedemaekers et al. 2007). However, public use of health information is in conflict with individuals' privacy (Caldicott & Manning 2013; de Abajo et al. 2007; Lowrance, 2006) and, not any less, autonomy (Hoedemaekers et al. 2007). The dualism of private and public interest is an ongoing issue that has to be taken under consideration when dealing with cybersecurity and health (Mulligan & Schneider 2011).

2.1.4 Domain-specific value characterization

As can be seen above, the papers address, directly or indirectly, different ethical values regarding cybersecurity and health. It becomes obvious that some values are considered unambiguously as relevant. Again, for providing an overview on the ethical values that were present in the final list of papers, we generated a word cloud using the same methodology as in Figure 2. This overview outlines a still strong presence of "classic" values attributed to cybersecurity such as privacy and confidentiality (Fig. 3).

In the following, we provide a more specific description on how the values are understood in the health domain. We provide pairs of values that are usually coupled, which is denoted by "↔":

- Non-Maleficence/Beneficence ↔ Safety: An important set of ethical values regarding health and cybersecurity relate to the physical and psychological *safety* of the individual: Physical and psychological integrity of each person has to be remained and must not be violated by the (direct and indirect) use of technologies. That includes *non-maleficence*: the protection of any harm for individuals and groups, particularly in consideration of their vulnerabilities. On the contrary, the use of technologies in health related fields should pursue the idea of *beneficence*, i.e. become active to improve the health situation both for individuals as well as for the public in general. That aim is also discussed under the term solidarity.
- Privacy ↔ Security: These two values play an important role with everything related to cybersecurity. The *security* of hardware, software and collected data (partly under the term data or information safety) has to be protected against any threats and unauthorized use. Security is thus an essential part of enabling *privacy*. That contains protection of data, control of access

and sovereignty for data subjects: the final decision over data must be up with the person concerned. An important factor is the right to anonymity.

Figure 3: Word cloud of values identified in the final list of ethics papers of the health domain.

- **Trust ↔ Confidentiality:** A value often associated with security in health is *confidentiality*. That means that the devices, systems, and collected data must be confidential for all involved parties (e.g. patients, nurses, doctors, medical administration). The confidentiality of systems used has a direct impact on *trust* between patients and health professionals and health care providers. Due to the increasing use of ICTs, particularly the interaction between patients and doctors does not longer takes place only face-to-face. The rigid assignment of social and professional roles vanishes, not least because more and more stakeholders have access to patients' own data. However, maintaining a confidential relationship is an important task.
- **Autonomy ↔ Consent:** *Consent* of individuals is a fundamental value in health related fields, especially with regard to any use of their data. Due to the unpredictable future use of data, the focus is on informed consent: Everyone should, if required, be informed about exactly what the data is used for and what information is generated from it. Furthermore, it should be possible to change, copy, withhold or delete data at any time. Decision-making authority is an essential prerequisite for *autonomy*: The individual must be able to determine his or her own interests independently. An important aim of autonomous determination is the empowerment of the patient.
- **Equality ↔ Accessibility:** Since health is an issue for all people, *accessibility* is indispensable. This means that access to healthcare must be made possible in all ways, including through new technologies. No one shall be excluded for health, cognitive, social or other reasons. Rather, an improved inclusion, especially of vulnerable groups, should also be aimed at. *Equality* should be guaranteed; among other things that means that use of technology must not lead to unequal treatment, but compensate it. Discrimination has to be prevented.
- **Fairness ↔ Justice:** This leads directly to the value of *fairness*: fair treatment of all stakeholders involved, with special attention to disadvantaged groups. In this context, the value of *justice* is often mentioned. Technology in general and ICT in particular shall be designed and employed

to maintain and strengthen social justice in the field of healthcare. To obtain cybersecurity, not only with regard to healthcare, often implies to face increased costs of technology. These costs must not be an additional burden for already economically disadvantaged persons and social groups.

2.2 Business Domain

2.2.1 The "moral character" of the Business Domain

Businesses interact in cyberspace on a daily basis enabling them to store, process and analyse information such that they can quickly adapt to the rapidly changing business environment. Securing cyberspace, or cybersecurity, involves three things: protecting the technology that enables cyber interactions (software and hardware); protecting the valuable information held within the technology (data); and protecting the user who engages with the technology. Striking a balance in securing data security and protecting privacy appears to be a lengthy, convoluted task and has created an entirely new species of ethical issues for stakeholders (e.g. employers, employees, hacker, clients and consumers). Ethical issues are oftentimes context relative (depending on the technology, its function and how it is used) and can affect a number of different industries. With this in mind, the aim of this section is to illustrate that ethical issues can arise when using various technologies and cybersecurity measures within the business domain.

Information communication technology (ICT) has the potential to increase efficiency, reduce operational costs, increase quality of service and keep information secure. However, keeping data secure can be problematic. Data can include anything from personal information to business assets, trade secrets and intellectual property. Protection is required from outsider attacks (for example, from hacktivists) and from insider attacks (for example, from an employee). The literature identified has revealed some thematic issues that arise in attempting to secure cyberspace in business. Information security and data security dominate the discussion where issues such as protection, responsibility, privacy, ownership, accesibility, availability, control. monitoring, surveillance, trust, threats, risks, offhosring and outsourcing and usability are all mentioned. Other problems in cybersecurity were identified specifically in e-banking and cloud computing as these areas have a higher risk of attack due to the provided. The main issue in e-banking related to protection whereas literature regarding cloud computing was much broader as it included problem areas related to trust, confidentiality, availability and integrity, accountability, responsibility, control and ownership. Cybersecurity problems appear to arise in literature relating to the usefulness of codes of ethics, hacker ethics and social networking sites use of personal information.

A reoccurring theme throughout the literature was breaches in cybersecurity as a result of unauthorised access to personal of valuable information. This perpetuated various discussions in respect of confidentiality, consent, autonomy, fairness and justice. A loss of control of information, data leakages, computer abuses and the secondary use of data were also addressed. The literature indicates that these issues affect a number of ethical values such as trust, justice, freedom, fairness, consent, respect, integrity, autonomy, anonymity, self-determination, dignity, well-being and honesty. Security technology in the cybershpere thus appears to be value laden as its use for security purposes within the business domain affects both individual values and business values wherein benefits and harms can be caused to each party. A number of conflicts between individual value systems and business values arise as different stakeholders place certain emphasis on particular values. For example, a business may endeavour to respect the value of privacy, but pays more head to increasing business security. In such cases, the business may choose to utilise surveillance measures in the workplace to monitor employees ICT interactions. Herein, the value of security for the business takes precedence over the value of privacy and may be argued to infringe on the employee's privacy. A second example of a stakeholder conflict is

where a businesses chooses by its violation to outsource IT services and adopt cloud computing technology to reduce cost, and increase operability. The benefits for the business are clear however there is a cost of engaging with cloud services which is an increase in security risks. Risks include data breaches, misuse of data by a third party, a data leakage, data loss and thus a loss of ownership and an indefinite life of data in unknown locations increasing the risk of exposure to malicious attack.

It has been argued that maintaining computer security may be morally necessary to protect correlated rights and interests such as privacy, property and freedom (Brey 2007). Similarly, it has been argued that computer security can also work to undermine rights and harm basic ethical values such as autonomy, respect, dignity and integrity (Brey 2007). Kowalski gives four reasons why ethics needs to appear in computer security: 1) ethics will widen the control gap in commercial information systems including technological gap, socio-technical gap and social gap. The technological gap is between what the reality and expectations of the capabilities of security enforcing functions. The socio-technical gap is the inconsistency between socially expected norms and computer security policies. The social gap refers to individuals not acting according to expected social norms; 2) ethics may be the common language for specialists in different areas; 3) current systems are so large that there are no implicit control structures that are built on the framework of ethical principles; and 4) there is the need for a top-down approach – such as adding non-technical layers (such as to existing security policies in order to reach agreements between users and systems) (Leiwo & Heikkuri 1998).

Leiwo & Heikkuri (1998) suggest merging information security ethics and common computer ethics and addressing four major topics: privacy, accuracy, property and accessibility within which security, accountability, control, ownership, and rights to information are intertwined. Some research suggests that highlighting the importance of both micro-ethics (right choices made by individuals) and macro-ethics (right choices made by groups, societies and organisations) will provide computer science and engineering college students with the tools they need in order to make ethically prudent decisions (Dodig Crnkovic 2017). Leadership style and incentive provided to employees can directly affect whether employees embrace a more formalistic or utilitarian viewpoint in their work (Lowry et al. 2014). Within a business, efforts should be made to focus training on ethical decision-making process to recognise the importance of IT ethical abuse, judging something wrong, feeling an obligation to do something and then doing something about the violation. D'Arcy & Hovav (2009) argue that businesses create specialised security programs for those workers who spend more working days outside the office to combat the deindividuation problem. They argue that this will aid employees understanding that organisational security measures apply equally whether in or out of the physical boundaries of the office.

2.2.2 Summarizing the result of the literature search

Our methodology had a two-pronged approach, which involved technical searches and a systematic manual selection process (see Appendix A.1 for details). The technical searches gave rise to 1450 potentially relevant articles relating to ethics, cybersecurity and business. After an abstract and title review, 271 papers proved to have any significant relevance to the topic of discussion. After a full paper review of the 271 papers, 26 relevant references were discovered (with 1 paper of relevance which was uncovered from the healthcare domains technical and systematic searches). 24 papers were snowballed from the relevant papers. After a full paper review, 6 papers proved to be relevant to ethics and cybersecurity and business. Expert searches revealed 3 additional relevant sources. The total number of relevant papers is 33.

Again, we use a word cloud (Fig. 4) for providing a first overview on the ethical issues that were discussed in the final list of papers (see footnote 2 for details). In the following, we outline in some more detail, which ethical issues have been identified in the final list of papers. Those issues will be discussed in more detail in the next section:

Figure 5: Word cloud of issues identified in the final list of ethics papers of the business domain.

The majority of papers used relate to ***data security and information security.***

- 9 papers focus on issues relating to protecting data: Leiwo & Heikkuri, 1998; Conger et al, 2013; De Veiga, 2016; Simshaw & Wu, 2015; Gunarto, 2014; Brey, 2007; Posey et al, 2011; D'Arcy & Hovav, 2007; Taddeo, 2013; Matwynsyn, 2010.
- 3 papers focus on with whom does the responsibility lie to protect data information be it the data owner's responsibility, businesses' responsibility or society as a whole: Leiwo & Heikkuri, 1998; Matwynsyn, 2010; McReynolds, 2015.
- 1 paper discussed security issues relating to responsibility, trust and the ownership of data along with issues such as managing access to data and providing constant availability of data: Leiwo & Heikkuri.
- 5 papers outline potential threats to data security: Leiwo & Heikkuri, 1998; Matwynsyn, 2010; Bonner & O'Higgins, 2010; Gattiker & Kelley,1999; McReynolds, 2015.
- 4 papers address privacy issues in relation to data security: Conger et al, 2013; Rifaut et al, 2015; Walters, 2001; Gunarto, 2014.
- 1 paper discusses issues which emerge from outsourcing and offshoring data: (Robertson et al, 2010).
- 2 papers focus on the control of data flow and monitoring employees in the workplace via surveillance techniques: Posey et al, 2011; D'Arcy & Hovav, 2007.

The second most popular issue discussed in the literature relates to the ***security issues in cloud computing***. Cloud computing security issues generally relate to data and information security but are explicitly separated in this analysis as cloud services exposes information and data to new threats.

- 5 papers focus on issues relation to protecting information held in the cloud: Pearson, 2013; Bennasar et al, 2015; Alouane, 2015; Kouatli, 2016; Pieters, 2011.

- 3 papers address privacy issues that may arise in the cloud: Pearson, 2013; Alone, 2015.
- 4 papers discuss trust issues in the cloud: Pearson, 2013; Alone, 2015, Pieters, 2011.
- 1 paper discusses confidentiality issues in the cloud: Alouane, 2015.
- 2 papers mentioned security issues relating to accessibility to information stored in the cloud and the indefinite life the cloud gives that information: Bennasar et al, 2015; Alouane, 2015.
- 1 paper addresses the issue of maintaining data integrity in the cloud: Bennasar et al, 2015
- 3 papers address responsibility (Alouane, 2015), control (Alouane, 2015, Pieters, 2011) and accountability (Alouane, 2015; Kouatli, 2016) in the cloud.
- 2 papers focus on mobility in respect of the use of mobile devices and the security risks associated with using cloud services for both personal and professional purposes (Kouatli, 2016; Pieters, 2011).
- 1 paper distinguishes between security related issues in the cloud and outsourcing and offshoring security issues (Pieters, 2011).

Some papers mentioned in the literature pertain to the Usefulness of Ethical codes:

- 3 papers deliberate over the protection that ethical codes bring to a business in respect of cybersecurity: Dodig-Crnkovic, 2004; Harrington, 1996; Matwynsyn, 2010.
- 2 papers write about the responsibility of businesses and IT professionals have in relation to compiling useful ethical codes of conduct and implementing them in practice: Shakib & Layton, 2014; Matwynsyn, 2010.

A couple of papers discussed Hacker Ethics:

- 2 papers consider the motivations and intentions of hackers and how Hacker Ethics differs from Information Security Ethics: Leiwo & Heikkuri, 1998; Brey, 2007.

Other papers deliberate over security issues that arise in the E-banking sector:

- 2 papers talk through how best to protect E-banking services: Abreu et al 2015 and 2016; Venkatraman, 2008.

And other papers focus on security issues in social networking and information sharing:

- 1 paper juxtaposes the interoperability capabilities of social networking sites and the benefits these services offer to consumers, against issues of transparency in respect of consumer's data being used for unknown secondary uses: Salman et al, 2013.
- 1 paper highlights the risks and benefits associated with information sharing contrasting them with issues of consumer autonomy, freedom, self-determination and informed consent: Bodle, 2011).

2.2.3 Outlining the identified ethical issues

The moral character of cybersecurity involves protecting data information from harm. We address reoccurring ethical issues in order of which the arise in the literature; i.e., the most frequently occurring topic is discussed first and so on. We firstly address the issue of data/information (used interchangeably) security in which we address the most discussed ethical issues such as protection of information, privacy, threats, insider attacks, trust and so forth. We separately discuss ethical issues that arise in cloud computing mentioning the security risks and benefits associated with adopting to the cloud. The usefulness of ethical codes appeared in a number of resources and their application in managing cybersecurity in business is addressed. Hacker ethics and the rationale behind self-identified hackers is then discussed closely followed by cybersecurity issues in e-banking. Lastly, we discuss some literature that

focused on the responsibility of corporations to protect personal data from security breaches highlighting the lack of consumer transparency as to how their personal information is used, mined, analysed and collected by businesses and their third party partners. This literature specifically referred to interoperability applications used by social networking sites which we briefly discuss from an information and data security perspective.

Data & Information Security: Information security raises ethical problems when security breaches occur. Security breaches in business can involve a breach to security resources or information security. Resources such as hardware or software can be damaged or corrupted causing a loss of service, time and money for a business. When information security is breached, this can cause an economic loss for a business but in cases where data is lost, stolen or modified that contains personal, cultural or social value this can cause psychological or emotional harm for the client and consumer (Brey 2007). An information security breach may be more detrimental for one business than another. For example, a law firm contains highly valuable data including corporate records, personal information relating to clients, intellectual property and trade secrets thus substantiating a duty on lawyers to use reasonable and adequate cybersecurity measures to prevent unauthorised access to client data as an information breach may threaten the very survival of the firm (Simshaw & Wu 2015).

As securing private information is a core aspect of cybersecurity, privacy is valuable to the business and consumer. Privacy protects individuals from external threats such as defamation, harassment, manipulation, blackmail, theft, subordination and exclusion (Brey 2007). Walters (2001) argues that a threat to privacy is a threat to personal integrity. Definitions of privacy in respect of cybersecurity range from privacy being a fundamental human right (Dean et al. 2016), to a necessary condition for autonomy (Brey 2007), to an articulation of the core value of security which is meant to protect people from all kinds of harm done by others (Brey 2007). In respect of security of private and personal information, Schoeman states: "A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body" (cited in Brey 2007). This suggests that protecting the privacy of an individual in the cybersphere encompasses securing the processing of personal information, including technologies that may observe and interfere with human behaviours and relations and their body and their personal belongings (Brey 2007).

Sharing Personal Information: It could be argued that businesses who benefit from processing, storing and analysing personal information have an ethical obligation to adequately secure their data. For example, businesses that utilise and benefit from data mining techniques (a tool that enables a company to analyse an individuals' behaviour and uncover patterns and information not previously known which may be considered confidential or private; Simshaw & Wu 2015: 33) include financial services, consumer products, manufacturing, the pharmaceutical industry, technology/services, retail, telecommunications, energy, and transportation (Dean et al. 2016). Furthermore, businesses that couple data mining technologies with Open Application Programming Interfaces (API), such as social networking sites, may too have an ethical obligation to provide adequate security measures to protect valuable data as such techniques have been said to have "unforeseen ethical consequences" (Gattiker & Kelley 1999: 223). For example, the social networking giant *Facebook* uses both aforementioned tools enabling its users to navigate from site-to-site and comment, cross-post, "Like", and recommend something to another member, while Facebook tracks, traces and disseminates the members personal information (including "name, profile picture, gender, networks, user ID (UID), list of friends…") with articulated networks and with third-party sites and services (Bodle 2011). Bodle (2011: 321)argues that there is a lack of transparency and a loss of control for users as they are unaware as to what information is being collected, and how this information is being used, inevitably undermining privacy, data security, contextual integrity, user autonomy and freedom. Other tools include Facebook's Open stream (which allows outsiders to access a user's entire Facebook real-time activity stream) and Instant Personalisation Pilot Program (which allows third party access to members' data from which third parties can tailor content to the user's tastes respectively). These tools require enhanced security such as authentication preventing anonymity and inhibiting free movement online (Bodle 2011). Biletzk's makes the argument that the very

concept of "security, whether on line or not, is a rhetorical instrument in the hands of interested parties…" (Taddeo 2013). Bodle (2011) acknowledges that soliciting members data flows increases data portability and tailoring personalised content is drawn from information emanated from the individual themselves, however he makes the argument that the extensions of these techniques are used at the expense of user autonomy. Bodle further notes that members lack of awareness inhibits individuals' ability to make informed decisions thus relinquishing self-determination and suggests a more human-centric business approach based on values and principles including transparency, privacy, security, autonomy, and user control as alternatives to various forms of market enclosure. Nissenbaum suggests ethical or value-sensitive approaches to social network design (Bodle 2011: 334). From a utility perspective, one can weigh up the benefits and cost of these business tools and their security. For example, technologies enable society to benefit from online social engagement via increased interoperability between businesses and individuals, but the price of engagement is paid by the individual who is encouraged to completely surrender their personal privacy on the internet; as the core principle of security is privacy, one could question whether the engagement benefits are greater than the potential harm (Shakib & Layton 2014).

Control of Information: As security must protect the purpose of data processing and the actual data processing (Rifaut et al. 2015), some argue that failing to strike a balance between the two affords cybersecurity the potential to promote or inhibit the safety, security, privacy and civil liberties of individuals and organisations (Da Veiga 2016). One purpose of data mining can be to stereotype whole categories of individuals (Brey 2007). Conger et al. (2013) argue that ethical conflict arises when the individual has not given informed consent for this type of analysis of their private data whether it takes place before, during or after a transaction is complete. Whether informed consent is obtained for data to be shared with third party partners should be raised, as the individual may be unaware that once shared the personal data is no longer controlled by its first and second party donors. Dean, Payne & Landry (2016) analyse data mining from the Golden Rule's perspective – one should do unto others as he would have others do unto him – and suggest that data miners ought to consider three moral requirements: 1) that the actor treat all acted upon equally and in like manner to action he would accept, 2) that the person acted upon be regarded as inherently valuable and not just as a tool to attain the actor's own ends, and 3) that freedom of the person acted upon be respected. In doing so, the first looks at how information is collected, stored online and/or shared with others, the second considers how the collection or use of data benefits the data subject and the third commands the data miner to acknowledge and respect the autonomy of all rational beings (Dean et al. 2016: 489-490).

Information Availability: Van den Hoven argues that access to information has become a moral right of citizens in the information age because information has become a primary social good: a major resource necessary for people to be successful in society (cited in Brey 2007). The high availability rates of the internet and online storage, enable businesses to readily use on-demand services in the form of cloud computing. However, high availability comes with security risks during the process of transferring information between parties (Pieters 2011). Responsibility and accountability issues can also be a concern as it is unclear whether data is secured at all times and whom takes responsibility for the maintenance and backup of the information held in the cloud (Kouatli 2016). Locating data due to the practice of data replication in the cloud can also prove very difficult as the system in use may automatically replicate data to different locations all across the world. This raises a further security, ethical and potentially legal issue as data might be lost or stolen in a country where legislation on data protection and information security is not as stringent as the host's country (Kouatli 2016). Pearson (2012) suggests that security need not suffer in moving to the cloud as outsourcing security to security experts can provide greater protection than previously obtained – the key is to select suitable service providers who have controls in place that respect privacy and are context-dependent.

Insider attacks: Industry surveys report between one-half to three-quarters of all security incidents originate from people within an organisation (D'Arcy & Hovav 2009; Da Veiga 2016). Another study reveals that the most significant threat to cybersecurity related to data leaked accidentally or intentionally by

employees (Da Veiga 2016). Malicious insiders may be motivated by job dissatisfaction, greed, pressing financial problems, have political or social activism motives or may seek to compromise client data for financial gain (Simshaw & Wu 2015; Leiwo & Heikkuri 1998). Managing this "peopleware", as defined by Neumann (Kouatli 2016)), not only involves implementing anti-virus technology, it involves proper management of people (Kouatli 2016). Traditional ways to block negative employee behaviours involve implementing technical measures such as authentication and identification, passwords and pass phrases, firewalls, intrusion detection, rights management, countermeasures and system controls (Lowry et al. 2014). Additional approaches include policies, and procedures, computer monitoring, audit trails, IT audits, IS risk analyses, IS security counter measures and general violation-prevention strategies. Other approaches include psychology methods such as using fear appraisals, leveraging employee perceptions of IT policy so that policies appear more mandatory, countering neutralisation techniques and using general deference theory or related penalty-oriented techniques (Lowry et al. 2014).

Surveillance: The consent issue arises in the context of cybersecurity measures implemented in the workplace to combat insider attacks. Employers are reported to surveil employees with or without the consent of their employees (Gunarto 2014; Leiwo & Heikkuri 1998; Posey et al. 2011). One study revealed that 21.6% of corporations search employee files (emails, network messages, voicemail) on the authority of executive managers and in 66.2% of such cases, employees were not warned (Leiwo & Heikkuri 1998). A security conflict emerges wherein employers must protect the business from insiders, and employees have limited protection against employers' electronic surveillance (Gunarto 2014). Surveillance in the workplace could be regarded as an infringement of employee privacy (Brey 2007) despite the law appearing to support employers' rights to read electronic mail and other electronic documents of their employees (Gunarto 2014).

An extension of traditional workplace surveillance is a method called dataveillance, which entails the large-scale computerised collection and processing of personal data in order to monitor people's actions and communications (Brey 2007). This technique not only records and processes static information about individuals; it records and processes actions and communications which can be extended to customers (customer surveillance) raising ethical concerns over consent, privacy and security of information, namely justice (Brey 2007). The notion of justice is based on the belief that a just person treats others fairly and undeserved/unearned benefits should not be attained at the expense of others. For example, each party to a transaction should get out the reasonable equivalent of what they put in (Dean et al. 2016). DeGeorge's argues that surreptitious surveillance and wiretapping are violations of privacy not merited except in certain limited circumstances (in Dean et al. 2016). Further noting that no one person or institution has the right to know personal facts and information of another unless necessary to prevent harm to others. Posey et al.'s (2011) research suggests that increases in organisational monitoring may lower commitment and may increase workplace deviance on the basis that monitoring efforts can result in perceived privacy invasions and subsequent breaches of procedural and distributive justice. For example, email monitoring. They suggest that perceived procedural and distributive injustice may contribute to unethical behaviour such as "cyber-loafing" (the unauthorised personal use of the internet in the workplace) and privacy invasion is said to violate expectations about fairness such as being treated with respect and dignity and having rights to interpersonal space (Posey et al. 2011).

Control in the Cloud: Cloud computing is a common business tool used by corporations that can be vulnerable to both outside and insider threats. The cloud enables businesses to reduce operational costs bypassing the need for an in-house IT department and renting the infrastructure from their provider, relieving the businesses from buying the hardware themselves (Alouane & Bakkali 2015; Kouatli 2016; Pieters 2011). However, the ease and efficiency of the cloud comes with privacy risks and the issue of control over data processing (Bennasar et al. 2015) as customer's data is processed remotely in unknown machines (Alouane & Bakkali 2015). Pearson (2012) argues that there needs to be an appropriate level of access control within the cloud environment to protect the security of resources as cloud computing may increase the risk of access to confidential information. Control over the infrastructure is available in five formats: public, private, hybrid, managed and community-owned. This is indicative, as

it can be unclear as to who controls the information and infrastructure, and who owns it (Pieters 2011). For example, in a managed cloud, a company owns its own IT infrastructure but outsources the management to a third party. In the case of public clouds, they are owned and managed by third parties and are possibly accessible to anyone including competitors and are the most challenging when it comes to security (Pieters 2011). Therefore choosing the most suitable cloud to meet the businesses needs and, in addition, to ensure adequate security for the protection of the business, client and consumer is important. Most corporations utilise a hybrid cloud where they host most of their insensitive applications and data in the public cloud and secure their sensitive data and application in an in-house built private cloud. Kouatli (2016: 415) proposes that "special cloud ethics" needs to be developed "to maintain an ethical and secure environment for the service providers' clients".

Closely related to the control issue is responsibility in the cloud. Responsibility can be a challenge in cloud computing in respect of which parties are responsible for which aspect of security (Pearson 2012). A number of threats coincide with cloud computing such as abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage and account/service hijacking. Pearson (2012) notes that if entities are involved in the provider chain that have inadequate security mechanisms in place, this can exacerbate the problem of unauthorised access. Noting that the potential damage caused in the cloud is greater than non-cloud environments due to the scale of operation, the presence of certain roles in cloud architectures and the fact that data may remain in the cloud for long periods of time often results in a greater exposure time for an attack. De-perimeterisation is the fading of the boundaries of organisations and their information infrastructure (Pieters 2011), which can raise similar control issues in the cloud. It is noteworthy to mention that de-perimeterisation can also be an issue when businesses hire consultants from third parties or allow employees to use mobile devices as such structural changes to an organisation challenge the containment-based approach to information security and force organisations to implement data-level security instead (Pieters 2011).

Cost & Data Quality: Structural changes such as offshoring and outsourcing can also raise some concerns. For example, in financial institutions security and privacy are the main risks associated with offshore outsourcing, as security breaches at offshore locations are harder to detect where "ensuring physical protection of data at a foreign site is more difficult than doing so at a local site" (Robertson et al. 2010: 173). Poor data quality in the cloud can also be an issue. When data is of poor quality this has two implications; the first is that the security of an enterprise becomes compromised as security is directly linked to the accuracy of data (Dillon et al. 2016). The second is that usability of a system comes into question if the system and data therein are not useful or if the data is out of context. This typically results in a loss of ownership and very serious security problems (Dillon et al. 2016). Quality of data and information security are viewed as value-based issues, which vary in their moral intensity and can have a significant effect on ethical decision-making (Robertson et al. 2010). It is argued that investors view offshore/outsource decisions more favourable than consumers on the basis that investors perceive it as a means to improve profitability and firm competitiveness while consumers will have concerns over product safety, service quality and data security. Business ethics scholars substantiate the issues of quality and data security as ethical issues based on the mere obligation that a business has to keep customer information in confidence as well as ensuring product safety (Robertson et al. 2010). Trevino and Nelson characterise these problems as ethical issues as they "involve obligations to primary or key stakeholder group…" (cited in Robertson et al. 2010), which includes the consumer, shareholders, employees and the community. The decision to offshore or outsource is discretionary and affects the lives and well-being of others leading Trevino and Nelson to the conclusion that offshoring is a moral issue as it is an action made with volition which has both beneficial and harmful consequences for others.

Codes of Ethics: In terms of managing ethical issues in relation to cybersecurity in the business domain, corporations can construct rules of conduct and codes of ethics (Kouatli 2016) to clarify responsibility and deter unethical behaviour (Harrington 1996). Codes of ethics ("Code") keep employees abreast of laws and regulations and clearly outline unacceptable or illegal behaviour and in the absence of a Code,

it is easier to rationalise irresponsible behaviour (Harrington 1996). Pearson and Wiener argue that rationalisations are a way of neutralising the norms generally embraced by an individual, allowing the individual to drift into unethical behaviour (cited in Harrington 1996). Codes can be the basis for internal sanctions that have a deterrent effect and can thus affect an employee's intentions. Assuming that they have an impact on the decision-making process of the employee, they can contribute to any one of the following: (i) increase awareness that an ethics issue exists and a potential computer abuse can occur; (ii) aid the employee in making a judgment about right and wrong by clarifying right or wrong behaviour regarding the abuse; (iii) encourage employees to abide by their judgments to place the value of doing right above other values and establish ethical intentions for behaviour; and combining points (i) through (iii) cause the employee to behave in an ethical manner (Harrington 1996). In saying that, codes have received criticism for being used as a public relations gimmick or a means for protecting the corporation from legal liability with some researchers noting that codes lack much impact (Harrington 1996). Codes have also been accused of being nothing more than pseudo-ethics as they simply codify existing rules and standards of behaviour and do not encourage ethical reasoning when an individual is faced with new or difficult issues such as those which confront IS personnel (Harrington 1996).

Informed Consent: The requirement for businesses to obtain informed consent from individuals in respect of how organisations store, use or exchange personal and private information emanates from the principle that a person should not be used as an instrument for advancing some goal, but should be fully informed and have freely consented to engage in an activity wherein their interests are respected (Brey 2007; Dodig 2017). This approach entangles the value of trust, which can be viewed as a consequence of progress towards security and privacy objectives as trust revolves around the "assurance" and confidence that people, data, entities, information or processes will function or behave in expected ways (Alouane & Bakkali 2015). When trust is undermined, a power struggle emerges wherein one party has more power than the other (Kouatli 2016; Pieters 2011). This reiterates previous arguments that encourage businesses that engage with technologies that process personal data to implement adequate cybersecurity measures that balance individual privacy with corporate use of data security (Conger et al. 2013).

Hacker Ethics: A significant difference appears to exist between insider attacks from for example, a disgruntled employee who seeks revenge on their employer, and an outsider attack from for example, a hacker who seeks to reveal information, which will identify problems in systems and cause no harm to institutions (Leiwo & Heikkuri 1998). A typical approach among hackers is the belief that by gaining unauthorised access into a system, they are providing a good outcome for the information security community as they believe that all information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world (Brey 2007). Tavani counter-argues each point respectively noting that the ideal of information being free undermines privacy, integrity and accuracy of information (as it could be freely modified at will) and states that information cannot be free as this runs counter to the very notion of intellectual property and would imply that creators of information have no right to keep information to themselves nor have the opportunity to profit from it (in Brey 2007). Tavani argues that the helpfulness of hacking pointing out security weaknesses may not outweigh the harm it causes as activities in cyberspace do inflict harm in the real world. The code of ethics of Knightmare includes the following statement: "Never harm, alter or damage any computer, software, system, or a person in any way" and if the damage is done, the hacker should do what is necessary to correct the damage and prevent it from occurring again (Leiwo & Heikkuri 1998: 215). Leiwo & Heikkuri suggest that hackers see themselves in a similar light to how the Greek philosopher Plato saw himself as the hacker is attempting to achieve something that goes beyond information systems which is similar to Plato's differentiation between one person's love of wisdom and another person's love for knowledge noting "vulgar curiosity does not make a philosopher" (1998: 215-216). In contrast to hacker ethics, information security specialists tend to deontologically specify what ethical behaviour is (Leiwo & Heikkuri 1998). From a deontological perspective, virtue is seen as an end of ethical activities. In contrast, hackers tend towards consequential ethics. According to consequential

ethics, the nature of what is done is not essential but the value of activities is determined by the outcome, and virtue is seen as a means to achieve the desired good outcome. Leiwo & Heikkuri's research acknowledges that cultural relativism plays a role in cybersecurity ethics because each judgment is based on personal values informed by the individual's culture. They argue that hacker ethics and information security ethics result from different cultures. Moral agents in these scenes are thus incapable of judging each other's values.

Usability: Bruce Schneier states, "The more secure you make something, the less usable it becomes" (cited in Dillon et al. 2016) suggesting conflict arises when security and usability are not considered collectively. Research indicates that most users prefer usability over security, particularly in the context of graphical passwords (Dillon et al. 2016). In relation to the use of secure emails, users prefer integrated solutions where neither security nor usability are compromised. Usability problems within a systems security context include authorisation of entities, definition of a security policy for a resource, revocation of rights, checking validity of a set of credentials, privacy of users and distinguishing trusted channels. Privacy enhancing technology (PET) are technical and organisational concepts that aim at protecting personal identity and usually involve encryption in the form of digital signatures, blind signatures or digital pseudonyms (Walters 2001). Walters argues that these technologies may promote and protect privacy and security rights and suggests that smart cards and biometric technologies can utilise PETs in ways that protect privacy and thus human freedom and well-being.

Biometrics: Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioural characteristics (Brey 2007). For example, a person can be recognised by traits such as fingerprints, hand geometry, signature, retina or voice (Venkatraman & Delpachitra 2008). It can be a reliable method of access control and personal identification for organisations such as financial institutions however there are a significant number of security threats in implementing biometric technologies such as the following: changes in lighting and photo angles in face recognition affect the reliability of data; masking a finger to avoid a match in fingerprint technology can affect the validity of matching accuracy; hijacking of contour data in palm scanning/hand geometry could affect confidentiality and privacy; inability to execute liveliness testing in iris/retina scanning opens the potential to print iris patterns on contact lenses; and signature recognition can threaten data accuracy and reliability due to variable trait data (Venkatraman & Delpachitra 2008). There is also a risk with privacy and confidentiality if biometric information is stolen or is misused. Thus moderating cybersecurity of biometrics is not just an operational challenge but also an ethical challenge for businesses (Venkatraman & Delpachitra 2008). There is also the potential for the monitoring organisation to trace the movements and actions of individuals exposing insights into individual behaviour, which may be leaked or used against the individual in the future (Brey 2007). A paradox exists at the heart of biometrics as on one hand the technology can be a threat to privacy as it is a technology of surveillance. On the other hand, biometric technologies can be utilised as security mechanisms that protect privacy (Walters 2001). A trade-off also exists between usability and security, as users could be greatly inconvenienced trying to update their biometric data if fault tolerant procedures are not in place (Venkatraman & Delpachitra 2008). The widespread use of biometrics could also have the undesirable effect of eliminating anonymity and pseudonymity in daily transactions, as individuals would leave traces of themselves everywhere they went (Brey 2007).

Other problem-areas to be explored: Considering a large percentage of security breaches go undetected, it is likely that figures released by industry surveys regarding computer crime underestimate the actual level of insider information systems misuse (D'Arcy & Hovav 2009). Commentators note that businesses do not report illegal activity to law enforcement or impose severe sanctions on computer abusers. Reporting is shunned, prosecution is complex, detection is uncertain, conviction is rare and rewards such as golden parachutes and well-paid consulting jobs are made available to convicted computer criminals (Harrington 1996). The effect is that computer abusers are rarely caught or punished - a fact well-known by potential computer abusers.

Future ethical issues for cybersecurity: New technologies such as ubiquitous computing involve the movement from the single workstation and entail embedding microprocessors into everyday working and living environments in an invisible and unobtrusive way (Brey 2007). Ambient intelligence is an advanced form of ubiquitous computing as it incorporates wireless communication and intelligent user interfaces that use sensors and intelligent algorithms for profiling. This entails the recording and adapting to user behaviour patterns and involves context awareness to adapt to different situations. In order for ambient intelligence to function, it requires possibly hundreds of intelligent networked computers that are aware of an individual's presence, personality and needs enabling the technology to perform actions and or provide information based on the perceived needs (Brey 2007). Securing this technology and data from criminals while also endeavouring to protect the privacy of the individual may prove extremely difficult as dozens of smart devices record activity and are connected to the developers computers as well as third parties.

2.2.4 Domain-specific value characterization

Again, we use a word cloud for providing a first overview on the ethical values that were discussed in the final list of papers (see footnote 2 for details). We see a strong dominance of the "protection" orientation.

Figure 6: Word cloud of values identified in the final list of ethics papers of the business domain.

We now provide a more detailed domain-specific characterization of the values that usually appear in combination:

Security Breaches & Confidentiality: Businesses have adopted the use of technologies in the cybersphere that aid user access. Corruption or damage to technological resources causes harm in the form of loss of service, time and money. Data lost, stolen or modified can result in a breach of confidentiality, integrity and availability for both the business and the user. For the consumer, this can invoke psychological

and emotional harm. As privacy is a condition of autonomy and is viewed as a core principle of security, a threat to privacy is a threat to not only data security but also data integrity.

Security, Transparency & Control: As there is no consensus on the ethical aspects of information security, the law enforcement is taking the role of providing guidelines on ethical behavior (Brey 2007). In order to fight computer fraud research suggests that transparency must be increased within businesses and within society as a whole as this will enable the general public to better understand and manage cybersecurity breaches and simultaneously reduce the excessive control currently held by security departments (Abreu et al. 2015 and 2016). In respect of sharing information in cyberspace, there is a lack of transparency as to how data is being used by businesses and their third party associates. This results in a loss of control for the consumer undermining privacy, security, contextual integrity, autonomy and freedom. Surrendering privacy is the cost of social online engagement despite access to information being considered a moral right. The risk of privacy invasion increases in the cloud as locating data breaches can be difficult especially when data is automatically replicated to unknown locations. A lack of awareness over data use also relinquishes self-determination and inhibits the ability to give free, informed consent. While sharing increases portability and personalised content it also undermines privacy. Certain sharing tools require enhanced security (authentication) preventing anonymity and inhibiting free movement online.

Security Compliance, Costs & Benefits: In relation to the cloud, Pearson (2012) argues that cloud usage is a question of trade-offs between security, privacy, compliance, costs and benefits wherein trust and transparency play a significant role. Further stating that privacy and security issues need to address a combination of issues including the speed and flexibility of adjustment to vendor offerings, which brings benefits to business and motivates cloud-computing uptake but also brings a higher risk to data privacy and security (Pearson 2012). Cloud technologies enable businesses to reduce costs, but while information is being transferred, it is unclear who is accountable and ultimately responsible if data is lost, stolen or misused.

Access, Privacy & Data Integrity: Hacker ethics promotes the free flow of information with unlimited access to computers advocating that this does not cause harm to the real world. This is in conflict with privacy, as well as integrity and accuracy of information. Information being free is in direct conflict with the notion of intellectual property. In contrast, information security experts base their actions on their duty to act ethically whereas the hacker believes the value of actions is determined by the outcome.

Security, Profit & Data Accuracy: A businesses choice to offshore or outsource activities is a moral issue as it has both beneficial and harmful consequences. Offshoring improves profit and competitiveness but increases the risks of a cybersecurity breach, which is often difficult to detect in a foreign state. There is a greater risk that data will be of poor quality and accuracy, which effects security as security, is based on data accuracy. Usability of data is thus decreased if data is out of context resulting in a loss of ownership and a potential breach of confidentiality. As data quality and security have a moral intensity, the aforementioned issues can affect the wellbeing of others.

Consent & Trust: Consent is inherently linked to trust, and providing security in the business domain entails respecting others by being fair, just and avoiding harm and dishonesty. A power struggle pervades when actions are not morally balanced. Surveilling employees in the interest of protecting the business comes at the expense of the employee. Surveillance can be in conflict with privacy when consent has not been obtained. This violates the notion of justice on the basis that expectations of fair treatment such as respect, dignity and rights to interpersonal space are not met. The impact of codes of ethics on reducing cybercrime in business is unclear. However, they can clarify responsibilities, outline punishments for unacceptable /unethical behaviour and increase awareness and aid decision making.

Security, Acceptability & Usability: Critics argue that an assumption of ethics as the foundation for security is far too optimistic and cannot be enforced due to the heterogeneity of public networks but note

that ethics can be enforced within groups that agree upon common ethical norms and terms of acceptable usage of information systems (Pearson 2012). The motivating factors could be common business interests and on the individual level driving factors could be terms of employment or codes of conduct within the peer group. Leiwo & Heikkuri suggest an ethics negotiation phase (where organisations negotiate the content of ethical communication agreement over specific communication channels) and an ethics enforcement phase (where each organisation enforces changes in ethical codes of conduct by specifying administrative and managerial routines, operational guidelines, monitoring procedures and sanctions for unacceptable behaviour.

2.3 National Security Domain

2.3.1 The "moral character" of the National Security Domain

Reliable ICT networks and services are since long a critical element in ensuring public welfare, economic stability, law enforcement, and defence operations. In addition to the health and business domains, malicious attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human errors all affect the proper functioning of essential public services that rely on public ICT networks. Such disruptions reveal the increased dependency of our society on these networks and their services. In the national security sphere, however, state actors like the police, and national security agencies have privileged access to ICT services. While this may be needed for law-enforcement, defence operations and counter-terrorism and therefore may increase security, at the same time it might endanger values like freedom and privacy.

Although value conflicts with respect to cyber security in the national security domain are regularly phrased in terms of security versus privacy, at closer inspection they are often more complicated. Take for example the discussion about end-to-end encryption in WhatsApp. Governments and security agencies have argued that they need to be able to access such encrypted communication for security reasons, e.g. to be able to early detect possible terrorist attacks. Opponents of such access by the police and security agencies do not only point at privacy considerations, but also at the fact that encrypted communication that cannot be accessed by governments and their agencies might be important for the democratic process, and that it enables opposition movements in countries with totalitarian or suppressive regimes.

A similar issue has arisen in relation to the Tor network. "Tor is free software and an open network that helps ... defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy (Tor project 2017)." The networks operates as "a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet (Tor project 2017)." In the aftermath of the hacking of the Democratic Party during the US elections, it turned out that a Dutch private Tor server had probably been used in the hacking (Zenger 2017). The Tor server was owned by Rejo Zenger, A Dutch Bits of Freedom employee. Bits of Freedom describes itself as "the leading Dutch digital rights organization, focusing on privacy and communications freedom in the digital age (Bits of Freedom 2017)". While Zenger recognized that Tor servers can be misused by hackers, and are in that sense a threat to cybersecurity, he believes that this is a price worth paying, not only for reasons of privacy but also because these servers may be crucial for whistle blowers to reveal abuses. Again, the value that is at stake here is not just privacy but also a range of civil liberties that are seen as crucial for democracy and the democratic process.

Another example is profiling. In this case, values like non-discrimination and absence of bias are at stake and are potentially conflicting with security. In profiling, people are approached, judged or treated in a certain way because these have characteristics that fit a certain profile and that are associated with certain other traits (i.e. traits other than by which they are identified as belonging to the profile). Profil-

ing is used for a wide range of purposes. It may be used by the police or security agencies to find criminals or terrorists; by airports to decide who to check more carefully, by (internet) companies to target certain consumers, by banks in deciding who to give a loan (and against what percentage). As these examples already suggest sometimes profiling serves security objectives. At the same time, profiling may inflict all kinds of undeserved harm on people, from nuisance to false accusations to even, in extreme cases, imprisonment of innocent people. Although profiling may involve privacy violations, because personal information is gathered to fit somebody into a profile, the main issue at stake is not privacy. Rather the issue is that a generalization is made based on limited information about a person. This generalization is based on statistical information about a group to which a person belongs while, due to its probabilistic nature, this information may say nothing about that particular person. Profiling may lead to stereotyping and discrimination. For example, the use of facial recognition technologies by the police and security officers has led to such concerns. Some studies suggest that facial recognition cognition algorithms are less accurate for certain social groups or races (Klare et al. 2012), which may lead to racial bias in their use (Introna, Wood 2004; Garvie et al. 2016).

Another value issue that might arise due to the collection of data by certain organizations for security reasons and that is not completely covered by privacy is the creation of power imbalances. Economic monopolies or oligarchies are often considered undesirable, and in democracies, balancing the (political) power between citizens and their government is an important concern. Maintaining certain power balances is therefore considered important by many for a healthy economy and for democratic politics. What seems to be less recognized is that in the information age, the possession of information about others and their behavior is increasingly a source of power. This also means that organizations that collect or possess large amounts of (personal) data may have increasingly power over other actors, which may lead to the disruption of existing power balances and the creation of new power imbalances. This applies to companies like Google or Facebook that collect large amounts of data about users and consumers, but also to governments and security agencies that may collect large amounts of data about citizens—and to providers of cybersecurity technologies as well, as they activities may involve the access to highly sensitive data. It should be noted that the accumulation of large amounts of data in the hands of a few may lead to new power imbalances and may be problematic even if such data is anonymized, or if people have given their informed consent for the collection, storage and use of their data. This means that even if privacy concerns are properly addressed, the accumulation of large amounts of data in the hands of a few may be considered problematic for economic as well as political reasons.

2.3.2 Summarizing the result of the literature search

We adopted a systematic review approach in which systematic searches and formal summaries of the literature are used to identify and classify results of major studies on cybersecurity in the national security domain. We searched our database for articles that contained specific processes/ technical terms/ frameworks related to national security in the topic field. The topic field includes the title, key words, abstract, and introduction in the database. We skimmed through the content, because in most papers, ethical issues or values were not mentioned or described explicitly. The initial search yielded 107 relevant papers that we downloaded to a local database in July 2017. For all papers, we read the introduction to gather the structure of the paper and we then read the core of the article to identify ethical issues and find relevant values. Sometimes, values were explicitly mentioned. The values that were most often mentioned explicitly were security, vulnerability, safety, connectivity, awareness. Other values were only suggested implicitly. We gathered them by taking quotes from the text. A researcher from our team associated one or more values with a certain quote. This was then independently checked by another researcher from our team. In addition, the identified values were also classified as conflicting with, or supportive for security.

When nation cyber security threats were accompanied by a citation of reference, we look the reference up in the bibliography, checked the title of the paper, and if it was indeed relevant we added the paper to the list of literature as a snowballed paper. This snowballing method resulted in 10 additional papers.

Furthermore, we also added 12 papers through expert opinion to the final list. Thus, the total number of papers is 129.

While the result may not be a complete list of cybersecurity papers in national security, the steps taken in data collection ensure that there is no bias towards any particular set of authors. In addition, we have chosen this approach to make the literature study as transparent and repeatable as possible.

Again, we use a word cloud for providing a first overview on the ethical issues that were discussed in the final list of papers (see footnote 2 for details).

Figure 7: Word cloud of issues identified in the final list of ethics papers of the national security domain.

2.3.3 Identified ethical issues

Based on the literature found, a list of ethical issues and conflicting values regarding cybersecurity in the national security domain were found. They are described below.

Cyber Terrorism/Cyber Warfare: Sekgwathe et al. (2011, p.171) argue that "Cyber-crime is typically understood to consist of accessing a computer without the owner's permission, exceeding the scope of one's approval to access a computer system, modifying or destroying computer data or using computer time and resources without proper authorization. Cyber-terrorism consists essentially of undertaking these same activities to advance one's political or ideological ends." A total of 49 papers addresses this ethical issue of cyber warfare in the national security context. Terrorism and the Internet were highlighted in two main ways. First, the Internet has become a forum for terrorist groups and individual terrorists, both to spread their messages of hate and violence, as well as to communicate with one another and their sympathizers. Second, individuals and groups have tried to attack computer networks, including those on the Internet. This second issue is described as cyber terrorism or cyber warfare (Bucci, 2012). Phahlamohlaka (2008) argues that the security risks associated with information and communication technologies, which go beyond national boundaries, are not fully in line with the value of data protection of all states. She sees a need of developing and implementing agile security related ICT policies to mitigate the value conflict between data protection and security in the national security do-

main to avoid cyber warfare. Building on this value conflict, Deibert (2011) discusses the growing pressure on governments to develop capacities to fight cyber wars. He notes (2011, p.1) that "today's deteriorating cyber-environment poses immediate threats to the maintenance of online freedom and longer-term threats to the integrity of global communications networks". His study highlights the value conflict between the data protection and security due to cyber wars.

Security of Critical National Infrastructure: The importance of critical national infrastructure protection was discussed in 27 papers. To protect critical information assets, enable safe communications, and conduct effective military operations in cyberspace, an increasing pressing issue for the government is to compel adversaries to stop conducting intrusions that already have been highly successful, rather than deterring them from choosing to conduct new hostile intrusions in cyberspace (Jakobson and Schmitt, 2012). This requires a significant control in the cloud against hostile intrusions in order to achieve security.

State Security vs. Individual Security: This ethical issue was discussed in 23 papers. Dunn Cavelty (2014) discusses a lack of focus on humans in the efforts of states to achieve security in the building of ICT and other critical infrastructures. As a result, he argues, state security is not aligned with individual security. In fact, the focus on state's security crowds out consideration for security of individuals resulting in detrimental effect of the whole system which allows the state actors to militarize cyber-security and to override the different security needs of individual humans in the cyberspace.

Cyber-Espionage: Cyber espionage is the use of electronic capabilities to illegally gather information from a target. This ethical issue was mentioned in 17 papers. For all nations, the information technology revolution quietly changed the way governments operate. The asymmetrical threat posed by cyber-attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. The achievements of cyber espionage - to which law enforcement and counterintelligence have found little answer - hint that more serious cyber-attacks on critical infrastructures are only a matter of time (Geers, 2010). Still, national security planners should address all threats with method and objectivity. As dependence on IT and the Internet grows, governments should make proportional investments in network security, incident response to the cyber espionages, and manage technical training for those (Geers, 2010; Lehto, 2013).

Data Breach: The release of data to an untrusted environment could lead to another crucial issue called data breach that was mentioned in 16 papers. The recent massive critical data leaks by Wikileaks suggest how fragile national security is from the perspective of data breach. In the absence of strong cybersecurity in the national security domain, there is apparently a major value conflict between connectivity and security (Adeel et al., 2005). This value conflict is highlighted in the existence of technology progress where technology was considered as a key contributor in the progress of any country, but also has created severe problems in the form of cyber security (Geers, 2010). Data breach raises several concerns. Firstly, critical infrastructure such as military and diplomatic systems may be vulnerable to security breaches. Secondly, such leak causes far-reaching damage to public interests, national security and economic sustainability. And thirdly, both technology and law seem incapable of dealing with such situation.

Lack of Cyber Law: The literature review reveals that legality problems play an important role in cybersecurity in the national security domain. The lack of cyber law was mentioned in 13 papers. Lawyers are faced with insufficient and vague cybersecurity legislations, which are incompatible with the requirements for effectively dealing with cyber-crimes (Faqir, 2013). At the same time, cyber laws become much critical than before in data and information security, as one can see in the growth of cyber-criminal activities. Hui et al., (2007, p.11) argued that "… digital crimes (e-crimes) impose new challenges on prevention, detection, investigation, and prosecution of the corresponding offences". Widely accessible systems must be made in a way that one can detect and investigate digital crimes more efficiently and effectively.

Surveillance: The ethical issue of monitoring of computer activities and data on the cyberspace by police and national security authorities was discussed in 12 papers. When considering different ethical issues regarding cybersecurity and national security, another major conflict set becomes apparent, i.e. the conflict between privacy and security. A critical issue in cyberspace lies in the inability of companies and private businesses to exchange information with the government. This causes insufficient information collection, skewing analyst results, and preventing the states from collecting sufficient data on cyber-attacks and developing better defences (McNally, 2013). The Google cyber-attacks illustrate the vulnerability of information stored in the cloud, online surveillance, and private sector collaboration with government agencies to prevent the increasing potential for catastrophic loss and global terrorism. Hiller and Russell (2013) state this fact again and argue that cyber infrastructure is owned and operated mainly by private rather than public entities; the states therefore should select the most effective cybersecurity strategy and regulate the private sector in order to reduce overall cybersecurity risk and address privacy concerns on cyberspace.

Profiling: The profiling issue, mentioned earlier as an example in this national security section, was not addressed explicitly in the identified literature, but it is mentioned in four papers implicitly.

2.3.4 Domain-specific value characterization

Again, we use a word cloud for providing a first overview on the ethical values that were discussed in the final list of papers (see footnote 2 for details). The word cloud for national security looks different because the researcher identified a greater number of "thick" (descriptive and practical) values. This domain seems to avoid appealing to abstract principles (such as those of bioethics) and ethical-theory terms. It is rather oriented towards valuing a larger number of more practical, concrete desiderata at the political and organizational level.

Figure 8: Word cloud of values identified in the final list of ethics papers of the national security domain.

The literature search emphasises the multiplicity of relevant values in relation to cyber security in the national security domain. Much of the literature in our database views cybersecurity as a necessary

complement to national security strategies. National cybersecurity strategies need to be mindful of national cultures and ethical and technical values, yet compatible with international strategies and the global nature of the Internet.

Some papers recognize the need to respect ethical and moral values such as security, freedom of expression, privacy protection and the free flow of information. In addition, other papers stress the rule of law and accountability as key values. Several papers explicitly state that cybersecurity became the top priority in dealing with the terrorism.

In the following, we provide a more specific description on how the values are understood in the national security domain. We provide pairs of values that are usually coupled, which is denoted by "↔":

Accessibility ↔ Security: These two values play an important role in national security domain. With lower costs associated with information accessibility and retrieval, higher consumer and producer accessibility to global markets and transnational communication are achieved. Many internet users, however, are not fully aware of cyber threats and they are not trained to protect themselves against these threats, leaving them vulnerable to online exploits, so increasing insecurity in cyberspace.

Legality ↔ Safety/Security: A value often associated with safety and security in the national security domain is legality. This value refers to the effectiveness of laws in assisting the police and the juridical system in combating cyber-crimes and computer-related crimes. While it is possible to protect information resources and communication networks against criminal assault with cryptography; legal mechanisms should are needed to secure systems and deal with cyber-crimes.

Privacy/Protection of Data ↔ Security: A lack of focus on humans from states in the efforts of achieving security in the building of ICT and other critical infrastructures causes a tension between individual and state security. In addition, counter-terrorism measures and tools that tackle cyber-crime often invade privacy in the most brutal ways and, at the same time, lack of personal online security leads to breaches of that same privacy. Security is thus an essential part of enabling privacy in the national security domain. That contains data security; data protection; data ownership; access control, information and computer security.

Confidentiality ↔ Trust: Confidentiality prevents the disclosure of information to unauthorized individuals or systems; Network information will not be leaked to unauthorized users or entity institutions. The impact of cyber-threats could reduce public confidence, damaging reputation of internet transactions. Thus, assuring a trusted and resilient information and communications infrastructure is needed. A reliable, resilient, trustworthy digital infrastructure for the future enhance online choice, efficiency, security and privacy.

Connectedness ↔ Equity of Access: Globally interconnected digital information and communications underpins almost every facet of modern society and provides critical infrastructure. Based on the literature review, inclusion and equity of access, consumer and producer accessibility to global markets, transnational communication, learning, and entertainment should be guaranteed along connectedness;

Accessibility ↔ Prosperity: Internet usage increases productivity, as a platform for innovation, and as a venue for new businesses; The value of accessibility therefore is an asset and an economic necessity. Since the private and public bodies offer more services online over time, once cyber-threats are addressed and systems are secured, the value of accessibility supports the value of prosperity accordingly.

Interconnectivity ↔ Security: The urgency for nations to develop strategies, frameworks or suitable legal policies to defend and protect from cyber-attacks were discussed in several papers. At the same time, it is often mentioned that cyber-attacks are beyond borders. It is becoming increasingly difficult and complex to handle cyber-attacks counter measures. In fact, whereas interconnectivity boosts economic growth and makes people's life easier, it also gives potential attackers more opportunities to commit crimes.

Cyber Awareness ↔ Security: Raising awareness about cyber-security threats and vulnerabilities and their impact on society has become vital, but seem to be missing in the society, comparing to the leadership that the governments of nations try to establish. Through awareness-raising, individual and corporate users can learn how to behave in the online world and protect themselves from typical risks. Awareness activities occur on an ongoing basis and use a variety of delivery methods to reach broad audiences. The awareness-raising, however, varies across countries. Security awareness activities may be triggered by different events or factors, which may be internal or external to an organisation. Major external factors could include: recent security breaches, threats and incidents, new risks, updates of security policy and/or strategy. Among the internal factors are new laws, new governments etc. Some of the papers were case based studies among countries such as USA, South Africa, South Korea, and EU countries.

3. Discussion

3.1 Bibliometric Analysis of Key Publications

Here we analyse bibliometric trends about ethics and cybersecurity for the key publications identified by our literature search (list A2, at the end of this document)[4] in the different social domains (health, business and national security). The analyses below are based on slightly different datasets, depending on the availability of data for the data field under consideration. The indicators of temporal development (3.1.1.) are available for the entire dataset (100% of the data)[5], including the three domains (72 records for Health, 35 for Business, 125 for National Security).[6] The indicators of geographic origin (3.1.2) include data retrieved from both WoS and Scopus together (59 for Health, 24 for Business, 105 for National Security), which is a significant proportion of the total (82%, 69% and 84% for each domain respectively). The indicators for WoS (disciplinary) categories only include data retrieved in WoS (46% for Health, 78% for Business, 53% for National Security), because Scopus does not provide this information. The indicators for funding are scarcely available (30% of records in health, 16% in business, and 10% in national security from the WoS dataset, 0% from the SCOPUS dataset), so only the analysis of the health domain may be significant.

3.1.1 Temporal development

Here, we compare the temporal development of papers selected from each domain (health, business, and national security) with each other. For each domain, we detect a distinct pattern in the number of publications relevant to the ethics in cybersecurity: they are growing over time. This is in line with the publication dynamics of the general cybersecurity literature outlined in Figure 9.

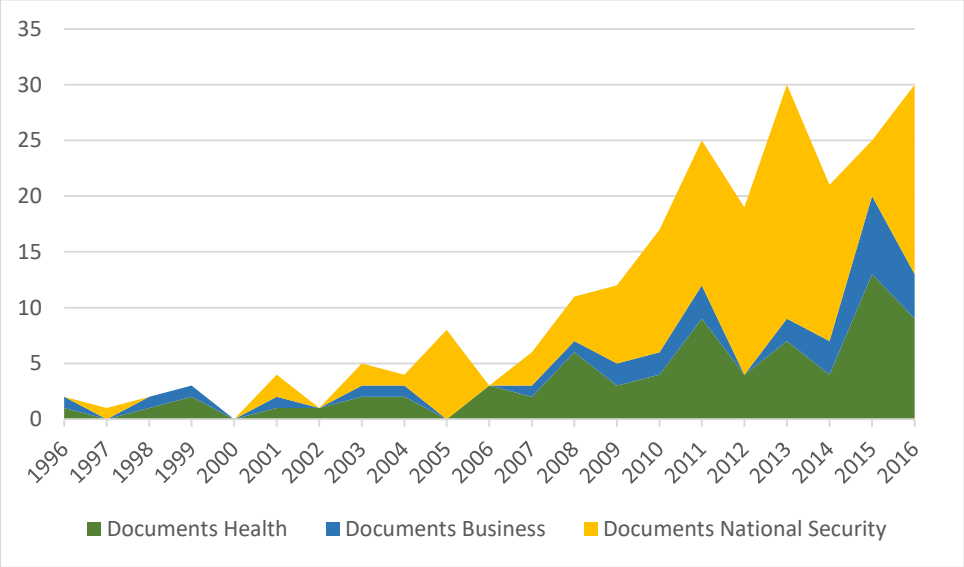

Figure 9: Number of papers published per year and per domain. The y-axis shows the absolute number of publications per year

[4] Some references in the final list have been added after the bibliometric research was performed. These are indicated with the symbol "×" in the list A2.

[5] Here, and in what follows, all figures do not consider the five additional records marked with "×" in A2, which were added after the completion of the bibliometric analysis.

[6] See note 5.

3.1.2 Geographic origin

Here we consider the geographic distribution of the papers in our list. Both WoS and Scopus provide information about the country of origin (affiliation) of the authors. This information is obviously important as it affects the validity of our value analysis as representative of a global vs. local community of investigation, and the possibility of cultural bias, produced at the source by the data availability. Both WoS and Scopus provide information about the *nation* or *state* associated with the documents (for example, USA, Canada, Italy, France, Malaysia, Lebanon, South Africa, Morocco, or Brazil), which we have grouped in seven "macro-regions":

1. North America (including only USA and Canada)
2. Central and Southern America
3. Europe (including UK and Turkey)
4. Asia and Middle East (including Israel),
5. Africa (including north African countries)
6. Central and South America (including Mexico and Brazil)
7. Australia and New Zealand

The graph below (Fig. 10) represents the proportion of WoS or Scopus *country-mentions* in our literature for each domain (e.g. with respect to 59 publications in health,[7] WoS and Scopus mention 88 countries) belonging to each of the above defined macro-regions (e.g. North America). For each publication, WoS and Scopus provide a single *country-mention* for each distinct country (of the institutional affiliation) of its authors. (For example, if a publication is co-authored by ten researchers affiliated with a US institution and one with a Swiss affiliation, both USA and Switzerland obtain one country mention, which translates into one mention for North America and one mention for Europe in our regional grouping.)

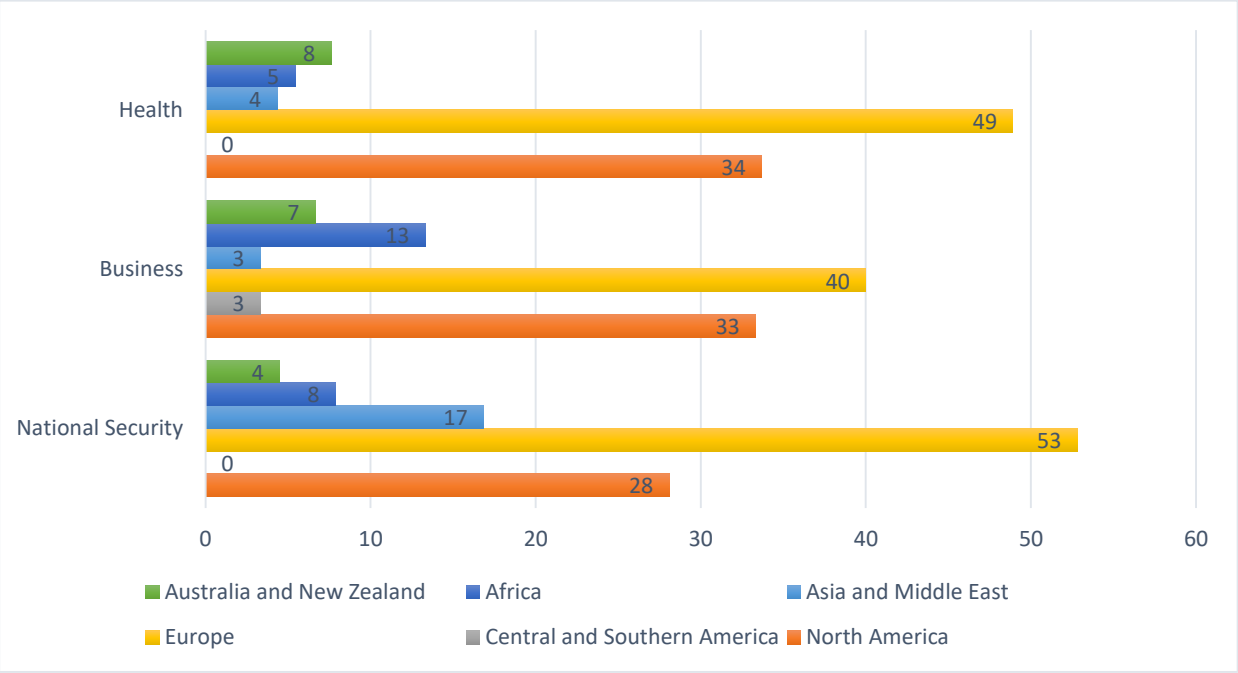

Figure 10: Geographic origin of papers. The x-axis shows the percentage of representation of each macro region.

The most obvious geographical pattern in the literature we considered is that if we put together the country mentions of North America, Europe, Australia and New Zealand we account for three quarters (or more) of all country-mentions in each and every domain. The second obvious trend is that more

[7] The total number of publications considered for the health domain is 72, but only for 59 we could retrieve country data in either WoS or Scopus.

country-mentions are from Europe than from any other region. The third trend is less obvious and emerges from considering the high percentage of country mentions of North America, Australia and New Zealand, and of the UK (as a proportion of European countries). UK is the *European* country with the highest number of country mentions, in both WoS and Scopus, across all domains (on average twice as much as the second country, which varies across domains). The almost total absence of Central and South American country-mentions is also noteworthy and it is possibly explained by linguistic, not only geographical reasons, i.e. the fact that we have examined the full text of publications in English. Had we examined the literature in Spanish (or Portuguese), we would have probably obtained a different result. Yet in at least one domain, we have a significant number of publications from Spanish researchers,[8] which may be explained by the fact that Spanish researchers have special incentives to publish in English, due to the context of European collaborations, compared to their Spanish speaking counterparts in Central and South America.

Let us now consider the publications citing those in our list ("citing publications"), to see if they confirm the geographical trend from our reference list (Fig.11).[9]

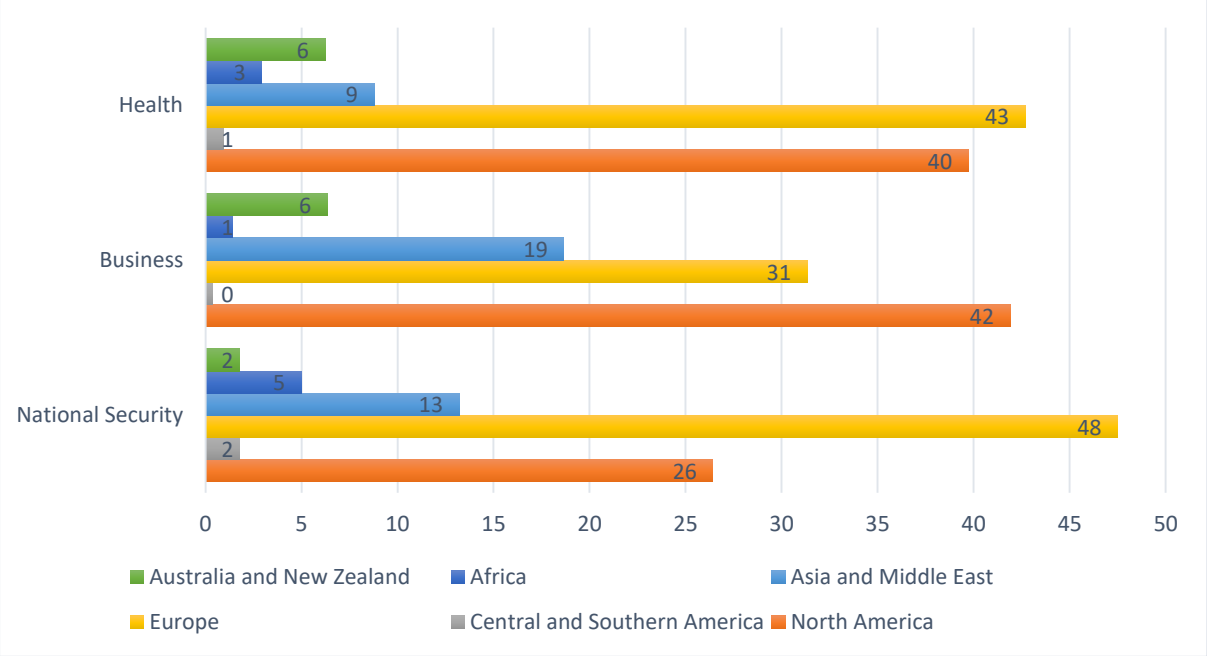

Figure 11: Geographic origin of citing papers. The x-axis shows the percentage of representation of each macro region.

The analysis of citing publications shows, *for the Health and Business domain only,* a strengthened dominance of the English speaking "dominant group" (North America, Australia and New Zealand, and UK within Europe), with the National Security domain only partially confirming this trend. As the graph shows, the proportion of European contributions among citations shrinks slightly.

One possible hypothesis for this increased dominance of North-American countries in the "citing publications" set is that researchers in the dominant group are cited more often than researchers from other countries, and, since – let us suppose – they are cited predominantly by other researchers in the dominant group, there is a greater proportion of these country in the citing publications set. A different one is that researchers from the highly citing English speaking countries cite researchers from other European countries and the rest of the world more often, than the other way around. Either way, the result

[8] E.g., 50 country mentions for Spain in WoS for health, compared to 123 for UK and 76 for Germany.

[9] In this case we retrieve data from WoS and Scopus about the geographic origin of the citing documents (96%-100% have such data); these are the publications citing the 82%, 69% and 84% (for Health, Business and National Security, respectively) of the items from our final list, those which can be found in WoS and Scopus.

would be proportionally more country mentions of North America among citing publications, than among those in our original list. A look at some significant data points suggests that both phenomena might be occurring.[10] It is also possible in that the databases we used (WoS and Scopus), publication venues where most North American publish are generally overrepresented (*i.e.* thus including a greater number of irrelevant records), but this overrepresentation is mitigated by the qualitative criteria we used to select pertinent papers, while such bias is expressed again in the (unfiltered, uncontrolled) list of citing publications.

In conclusion, the citation data show dominance of "Western" (= North American + Europe + Australia+New Zealand) publications, with a further dominance of English speaking countries, such as North America (especially the US) and UK within Europe. However, Asia and, to some extent, Africa, are represented in our list.

3.1.3 Funding

Information about the funding of the research is important to determine the plausibility and extent of cultural or economic bias, of research reflecting the agenda of powerful funders, be they companies or governments. It is therefore also interesting to analyse data about funding, where available. Unfortunately, we lack such information for a large proportion of publications in our list (70% without information in health, 84% in business, and 90% in national security – for WoS, with no integration of data from Scopus). It is interesting that the Health domain contains most of the available information, presumably because it contains a larger proportion of journals from medical and related disciplines, where norms concerning the disclosure of interests are presumably stricter.

With respect to our representation of the data, we depart from WoS, which produces a list of *individual* funding agencies (such as European Union Seventh Framework Programme Fp7, Wellcome Trust, University Of Bergen Norway, UK Medical Research Council, [US] National Institute of Health), by grouping such funders in seven distinct groups, divided by institutional type:

1) National governments and government agencies
2) Research centres (except those which are direct emanations of government agencies)
3) Foundations (if predominantly private)
4) Universities (both public and private)
5) EU institutions and programs (including both research "framework programs" and research carried out by, or for, specific EU governmental bodies)
6) Companies (*i.e.* for profit entities, both public and private).
7) Other civil society organization (which are not universities, private research centres, or foundations, such as, for instance, professional organizations).

The limited sample at our disposal suggests that *national governments and government agencies* are the greatest funders of research in every domain. Moreover, the scope of governments and agencies funding such research appears to be significantly diversified. It is also noteworthy that only in the health domain a significant proportion of funding comes from foundations. This is presumably because there might be more, or more well-resourced, charitable foundation operating in health than in any other domain related to cybersecurity.

[10] For example, the top cited publication of the Health domain, (co-authored by one Canadian and two French researchers) is cited predominantly by researchers in continental Europe (46%) but also in UK (11%) and North America (36%) (remember that the categories overlap, as the same publication can be a collaboration from authors of different regions, and is in that case counted as contributing to all). The second most cited publication (co-authored by several researchers from Canada, USA, England and Australia), is cited predominantly by Canadian (49%), US (26%), UK (10%) and Australian (10%) researchers, but also – in smaller percentages – by researchers based in continental Europe. In the Business domain, the highest cited publication is by a US researcher and 69% of its citations are by US researchers, while the second highest cited publication is by a Dane and a Canadian and, yet, 57% of its citation are by US researchers.

3.1.4 Citation Patterns

All domains are characterized by a skewed distribution of citations, with few top publications at the top of the distribution responsible for a large number of citations and many publications in the middle and the bottom of the distribution, scoring very few. While all three domains are very similar in this respect, their similarity is only visible if figures are analysed in relative terms. For example, in health, the most cited publication has 150 citations, *7.5* times more citations than the *average* publication in that domain (which has 20). In business, the top scoring publication has 116 citations, *9* times more citations than the average (12.7) of that domain. In national security, the most cited publication has 15 citations, which is *11* times the average for that domain (1.32). Therefore, the three domains have similarly steep curves, as far as citation counts go, in spite of significant differences in total scores.[11] A similar pattern (see fig. 9) emerges by considering the SCOPUS data for the National Security domain, pertaining to other 53 documents (not found in WoS), generating 158 citations.

As far as *absolute values* are concerned, each domain is characterized by different average *citations per publication* (within WoS). Publications in the health domain tend to generate, on average, the highest number of citations (20 cit/pub), with business a close second (13 cit/pub), and national security one order of magnitude below the other two domains (1.3 cit/pub). It is therefore not surprising that top publications of health and business have roughly the same number of citations (150 and 116, respectively), while the top publication of the national security domain has only 15 citations.[12]

Let us now analyse the kind of impact the literature in our list has on different disciplines. One measure of impact is the disciplinary audience of the literature we selected, which is indicated by the "Web of Science Category" attributed to each publication (by WoS). Since most WoS research categories are too fine-grained to be of interest to our analysis, we represent the data about seven macro-disciplinary categories, which we form by aggregating the Wos Categories along the following scheme:

1. Focal category for the domain (e.g. medical informatics in the health domain)
2. Information Systems Science
3. Computer science general
4. Ethics and Humanities
5. (Applied) Social/Health Sciences
6. Broad category including sciences in the domain (e.g. "other medical disciplines" in the health domain)
7. Even broader category including sciences related to the domain (e.g. "life sciences" in the health domain) [not in every domain]
8. Other interdisciplinary fields
9. Hard natural science and mathematics [not in every domain]

The rationale of such grouping is as follows: first, we are interested in knowing how many publications contribute to the narrowest WoS category related to the domain under investigation; furthermore, we want to know how many publications contribute to disciplinary fields that are progressively less pertinent to the field of investigation. Our macro-disciplinary categories (2), (3), (4), (5), (6), (7), (8) and (9) include Wos Categories that can be considered *neighbouring* scientific fields, or fields that are more inclusive (and general), than the focal category.[13]

[11] The steepness of this distribution is also confirmed by other indicators, e.g. the ratio between the citations of the top publication overall to the top publication of the 8th decile (*4.7* for Health, 9 for Business, and *5* for National Security times more) and the proportion of total citations which is due to publications in the 10th decile of the distribution (60% in health, 70% in business, 50% in national security).

[12] This pattern is confirmed by comparing the least cited publication in the 10th decile (respectively the 6th, 2nd, and 5th most cited publication, for health, business and national security) in each domain (53 citations, 42 citations, 5 citations). It disappears if one looks at the bottom of the distribution, but that is because this contains the same number of citations (=0) in all domains.

[13] Consider, for example, the health domain: our first macro-category includes only the WoS category of medical informatics, which is the focal category of that domain. The second macro-category ("information system science") includes the less specific

For each document in our list, WoS assigns one mention to each of the Wos Categories that the document contributes to (e.g. an article published by the *Journal of Medical Ethics* is mentioned as contributing to four distinct Wos Categories: "ethics", "medical ethics", "social issues" and "social sciences biomedical"). In what follows, we speak loosely about the "relative weight of publications" from a given disciplinary group, but the reader should be aware of the fact that we do not attribute this weigh by counting how many publications belong to a given "macro" group of WoS categories, relative to the total number of publication in the domain. Rather, our methodology gives more weight to publications that have a more diversified impact across disciplines of the macro-group, contributing to a greater number of distinct WoS categories, as we explain the footnotes.[14]

We begin our analysis with the *health* domain. Our graph represents, for any macro-disciplinary-group (e.g. "applied social/health sciences"), the weight of the different disciplinary groups.[15]

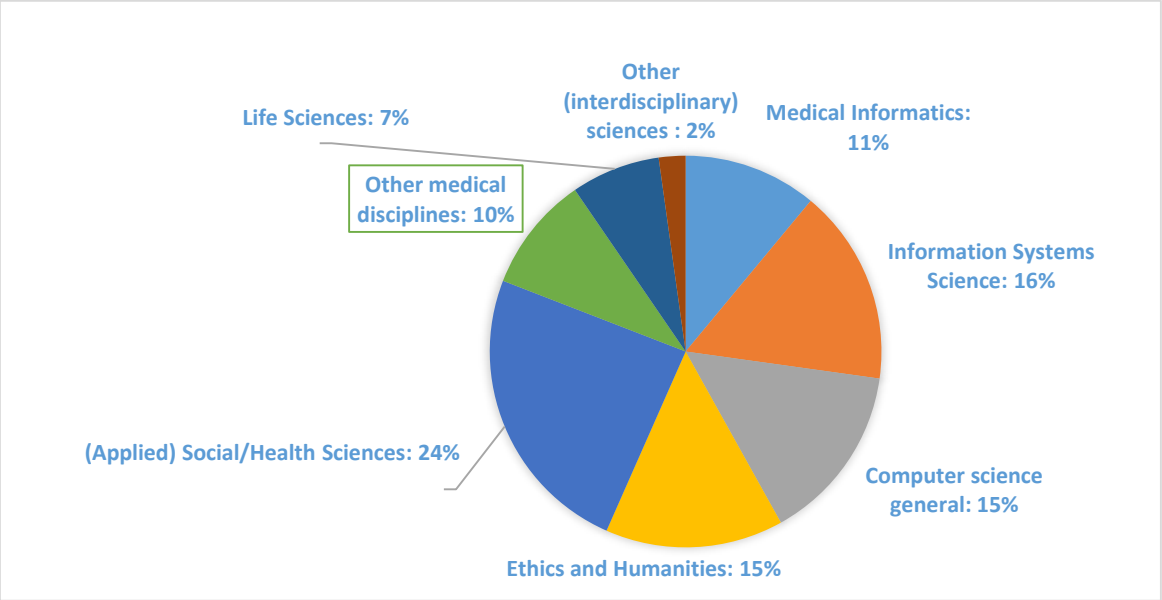

Figure 12: Subject category distributions for the health domain.?

"computer science information systems" and "information science library science", where one expects to find documents concerning cybersecurity, but not exclusively about health. Our fourth and fifth macro-categories include several "non-technical" Wos Categories which are important for the discussion of the ethical and social aspects of cybersecurity. In particular, the label "social/health sciences" includes both social sciences, such as economics, and "biomedical social sciences", such as "social sciences biomedical" and "health care science services". The macro-categories (6) and (7) include (non ICT-related) disciplines related to the domain (health) such as medical disciplines. Our macro-category (7) includes Wos Categories that may contain relevant records, but are very broad. For this domain, we have not found publications in mathematics and hard natural science (9).

[14] Our special way of aggregating data about Wos Categories in our macro-categories preserves one important aspect of the granularity of WoS data, since an article's individual contribution to the score of a macro-category is a function of how many distinct Wos Categories included in that macro-category there are, that the article contributes to. For example, if we have *one* publication associated with two different Wos Categories (e.g. "social issues" and "social sciences biomedical"), our methodology treats this as *two* scores for the macro-category "applied social/health sciences", which includes each of them. In other words, we count the article in question as a mention of *two* WoS categories (namely *"*social issues" *and "*social sciences biomedical"), and furthermore, we treat *each* of these two mentions of WoS categories as contributors to the total weight of the macro domain "applied social/health sciences".

[15] More rigorously, it expresses the weight of mentions of Wos Categories included in that macro-disciplinary-group (*i.e.* 33 distinct Wos Categories), as a proportion (*i.e.* 25%) of the *total* number of *all* mentions of distinct Wos Categories (*i.e.* 130), related to the total set of publications in the health domain (57 publications).

The weight of the WoS category of "medical informatics" is 11%, lower than the weight of non-technical macro-areas, such as "(Applied) Social/Health sciences (24%) and "Ethics and Humanities" (15%). A possible hypothesis is that discussion of the ethical issues of cybersecurity takes place predominantly within bioethics journal, classified as social science / ethics / humanities journals, but this hypothesis needs to be tested against further and different data.[16] On the other hand, "ICT-related" technical fields ("Medical Informatics, Information Systems Science and Computer science general"), taken together, include 42% of mentions of WoS Categories related to the literature in this domain. So, the debate on the ethics of cybersecurity in health (of our literature review) emerges from both the technical and the social science/humanities community, without any clear dominance of either side.

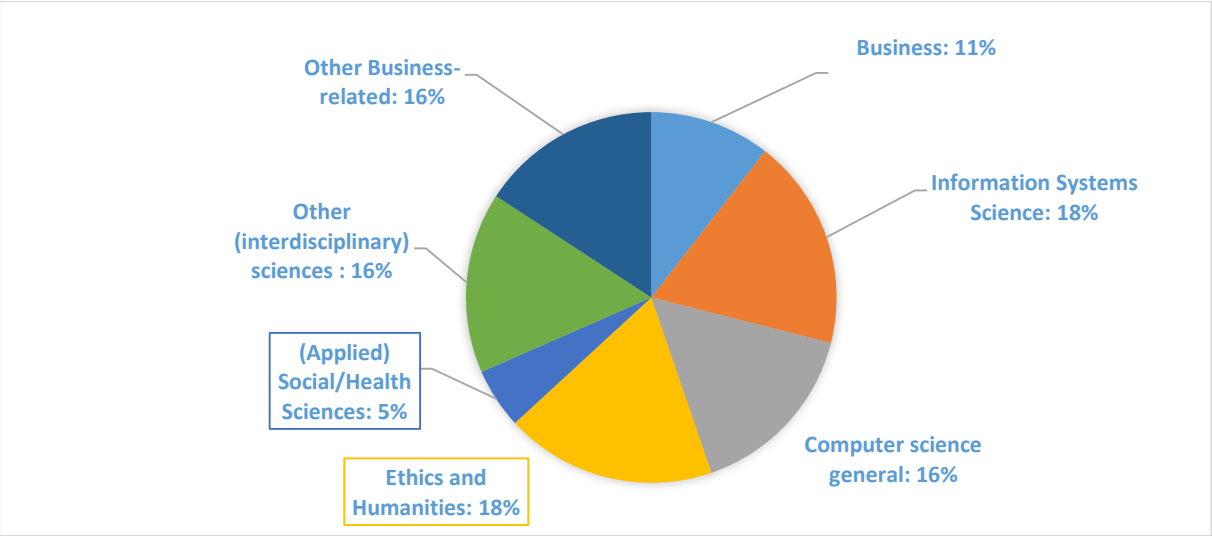

Figure 13: Subject category distributions for the business domain.

We find that the ethics of cybersecurity in business is more strongly discussed in informatics (Computer Science 18% + Information Systems Science 16%). Second, we find that disciplines in the "ethics and humanities" are also strongly represented (18%). Only 11% of the WoS category mentions refer to the focal category of business (as defined by WoS), while management and similar disciplines contribute another 16% to the debate. This represents, again, a very balanced distribution of WoS categories, suggesting that domain-related (e.g. business, management), technical, social, humanistic, and interdisciplinary research cultures contribute in roughly equal parts to the debate in this domain.

Let us, finally, turn to the National Security domain. In this domain, publications in "international relations" and "political science" together account for 12% of the debate. We find that the ethics of cybersecurity is most strongly discussed in "Information Systems Sciences" (25%) and "Computer Science General" (39%). For unknown reasons, this is the domain in which the weight of technical disciplines is greater. The debate in "other Social Sciences" and "Ethics and Humanities" only accounts for 16% of the debate, presumably because most social and normative issues are already discussed within the specialized fields of international relations and political science.

[16] It may also be in part a result of our scoring methodology, which puts a premium on journals with a more interdisciplinary orientation (as judged by WoS). The suspicion is well-founded, considering that 1) ethics, medical ethics, philosophy, and humanities multidisciplinary contribute with respectively 9, 5, 4, 1 publications, adding up to 19 out of 20 scored by the category "Ethics and Humanities", and 2) that a single article in a bioethics journals may be counted as a distinct contribution to each of these WoS Categories, *each of which* adds to the total "score" of our "Ethics and Humanities" macro-category. By contrast, an (apparently) narrower medical journal, like the *European Respiratory Journal* is only classified as contributing to the WoS Category "respiratory systems", so it brings only one score to our macro-category of "other Medical journals". Similarly, *Plos Medicine*, being classified only as a journal in "biology", adds only one score to our macro-category of "Life Sciences". And yet, the two most highly cited contributions to the literature for this domain (both concerning research *ethics*) were published in these two journals.

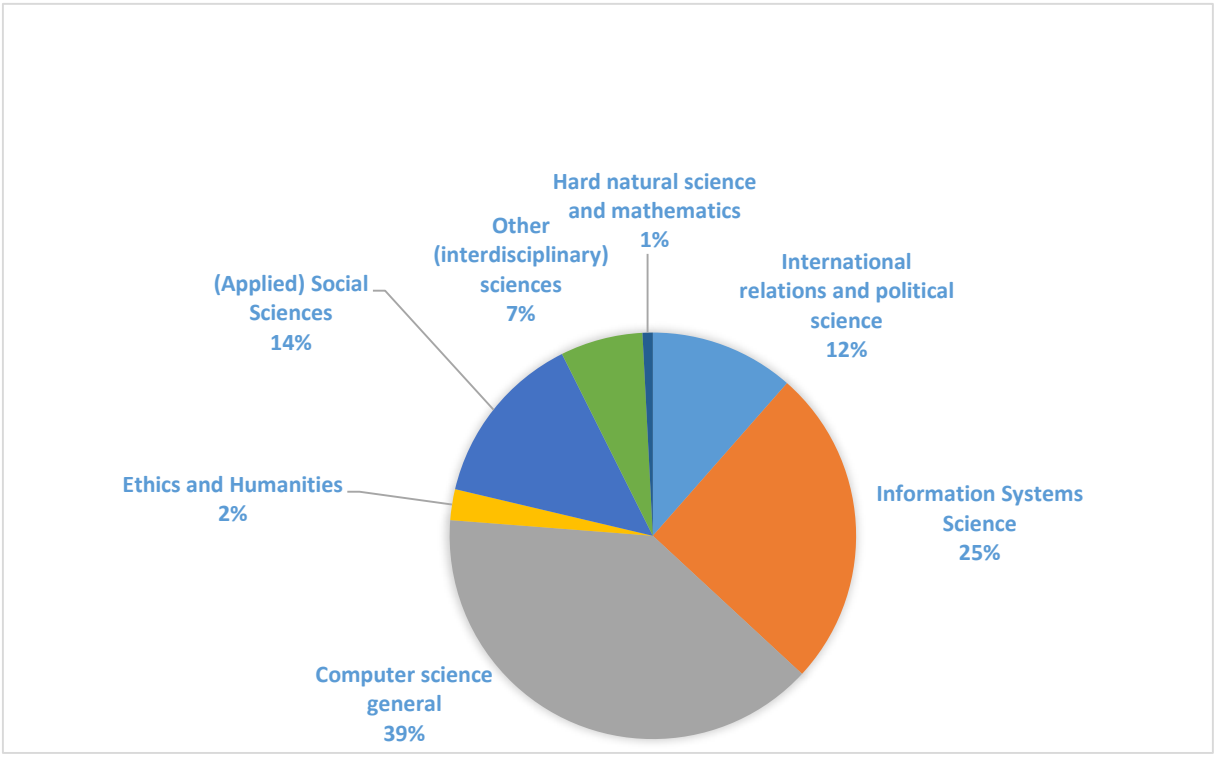

Figure 14: Subject category distributions for the national security domain.

Let us now turn to the analysis of the disciplinary fields of citations, across the three different domains. To do this, we introduce the same schema of macro-categories for all fields:[17]

1. Information Systems Science
2. Computer science general
3. Ethics and Humanities
4. (Applied) Social/Health Sciences
5. Medical disciplines, Life Sciences, Natural Sciences and Mathematics
6. Other (interdisciplinary) sciences

The differences between the citation profile of three domains are as follows (Fig. 15): in Health, the large majority of citations appear in Medical Disciplines and Life Sciences, followed by Social/Health Sciences, with a significant percentage of impact in ethics and the humanities (not found in other domains); in Business, the largest macro-area is Information Systems Science, followed by Applied Social/Health Sciences; in National Security the most relevant macro-area is Social/Health Sciences (including Political Science and International Relations). Notice also that the dominance of technical disciplines in the cybersecurity debate concerning National Security (outlier in this respect, compared to the other two domains) does not apply to the citing literature. Clearly, the comparison between the citations of different WoS categories is difficult in so far as they belong to different "citation cultures". It is not surprising, for example, to see that most citations of the health domain, the only one including publications in Medical Disciplines and Life Sciences, are produced by citing literature in Medical Disciplines and Life Science, as these disciplines have a comparatively more generous citation culture.

[17] Some arbitrary choices had to be made, such as including medical informatics in the group of "Information Systems Science" rather than of "Other Medical Disciplines and Life Sciences"; moreover, natural sciences and medical/life sciences have been grouped together (there are only few scores in natural science anyway.

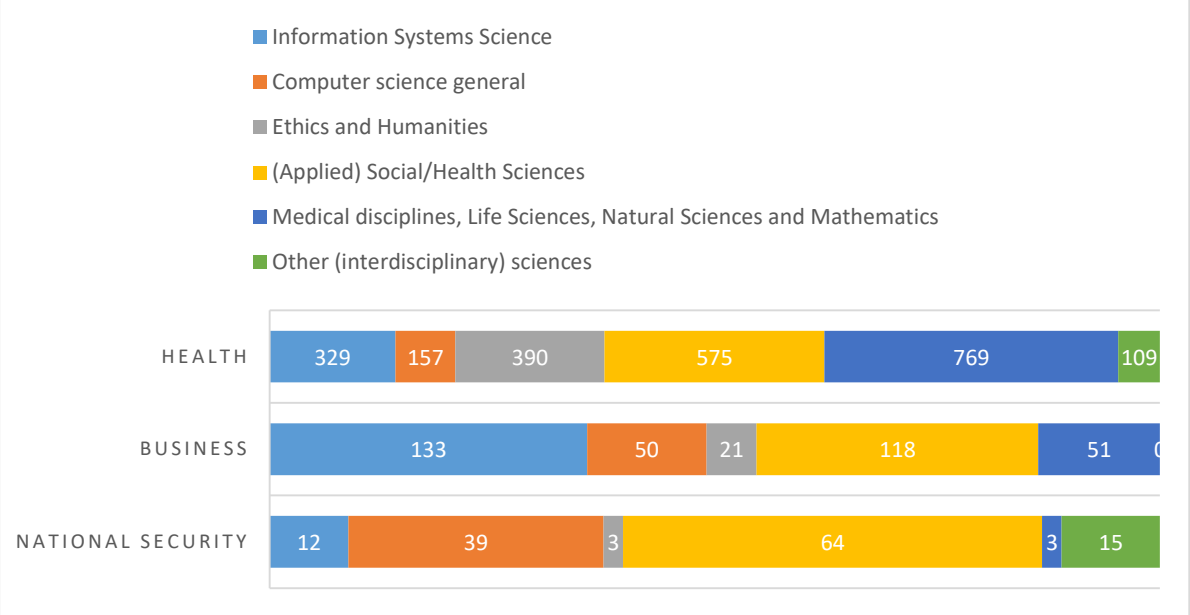

Figure 15: Subject category distributions of citing publications for all three domains.

3.2 Differences between domains

The main differences between the domains appear to be as follows:

1) The health domain has a clearer "value profile", codified also by the historically influential "principlist" ethics involving beneficence, non-malevolence, autonomy and justice. Each of these values can be positively or negatively related to cybersecurity depending on the context. By contrast, "moral character" of the other domains is not characterized by an equally well-codified theory. The "ethics" of the business or national security fields is "up for grabs" to a much greater extent than the ethics of medicine (the very idea that these two fields ought to be regulated by ethical considerations may be considered controversial).

2) Hacker ethics appears to be discussed in relation to businesses, not in relation to heath, and, oddly, not in the literature on national security, where hacking is conceptualized as crime, terrorism or warfare.

3) Surveillance appears in all three domains, but it is more negatively connotated in business (especially when applied by businesses to control employees). Surveillance in the medical domain is discussed for the possibility of "punishing" for unhealthy choices (e.g. by imposing higher costs in access to health care to individuals who are careless about their health). In the national security domain, surveillance is not framed as as a risk for individual privacy, but rather as a goal to be achieved.

4) The framing idea that health is a good of supreme importance, which is not mirrored by analogous claims concerning the value of profit in business (understandably). In the literature of the national security domain, the issue of privacy is , or (surprisingly!) that of national security in the national security domain.

5) The idea that there is a conflict between individual and public interest: it is prominent in the debate on health, where public health militates for more data sharing, that has a trade off with individual security and data protection, and in national security where instead of a concern to protect individuals from surveillance, the literature emphasizes the unwillingness of companies to exchange information about attacks as a source of vulnerability for the entire system.

3.3 Common Themes

Common themes are more evident than differences between the three domains. Two important common themes are the following:

1. That the overall justification for the use of ICT it broadly instrumental and utilitarian: it is a means to increase efficiency, reduce cost, and improve the quality of services (both private and public).
2. That the more secure you make something, the less usable it become (prominent in both health and business, not contradicted by national security).
3. That there are many trade-offs between desirable values. Trade off emerge even considering the different goals that are valuable from the same perspective, e.g. the individual perspective, or the perspective of the state. In addition to this, there are further trade-offs or conflicts when the interests of the individual are set against those of the community). One example of this is the usability/security trade off (see point 2, above) but also the fact that users may be forced to trade their privacy in exchange for some other valued good (this idea is prominent in both the health and business domain).
4. The problem of digital divide, seen as a problem of justice – while ICT makes life easier for some (perhaps most), it makes it more difficult for others, often whose who are already socially, mentally, or physically disadvantaged.
5. The problem of trust – the necessity of building the conditions for trust and the damage produced when these are compromised.
6. The threat of loss of control over data – in this respect cybersecurity is valued as part and parcel of informational self-determination and data protection.
7. The unpredictability of future uses of data.

3.4. What is missing?

The analysis provided in this White Paper points to three aspects that can be considered "blind spots" in the ethics of cybersecurity discussion:

1. First, it is generally surprising that – despite an extensive search methodology described in the appendix – the number of identified papers that deal to a considerable amount with the ethics of cybersecurity is rather low – particularly in the Business domain. Although we certainly cannot exclude the possibility that our search methodology may miss important papers, we take this as a strong indication that the academic literature just has started to deal in a more profound way with the ethics of cybersecurity. Our search methodology did not cover grey sources such as blogs, newspaper articles and the like – and it indeed could be that a livelier discussion on ethical issues of cybersecurity is present on such sources. We expect that this will change in the near future, as cybersecurity has become a top-priority of several policy makers.
2. Second, we find that the domain-specific ethicists that deal with the ethics of cybersecurity do this by taking the common topics of their discipline as starting position. For example in health, the focus in most cases was on protection of sensitive (patient) data; and the source of the argumentation were common topics such as the genetic information discussion. What is almost completely missing are discussions of the ethical dilemmas that the technology specialists are

facing, whose job is to ensure day-to-day cybersecurity. White Paper 4 lists a considerable number of such dilemmas. This we consider to be a problematic gap in the current academic discussion on the ethics of cybersecurity.

3. Finally, the analysis reveals that the number of real cases that are discussed is rather low. As an ethical analysis strongly relies on case studies, we consider this as another important gap in the current discussion; i.e. we need to create repositories of cybersecurity incidences that are related to ethical dilemmas. The problem here is that the culture of those who actually deal with such problems is a culture of secrecy; i.e. sharing incidences that are often described in a technical language may happen among the specialists themselves, but not in a wider community.

4. Conclusions

We close this White Paper on the ethics of cybersecurity with four main observations. A first observation is that the ethics of cybersecurity **not an established subject**, academically or in any other domain of operation. It is actually a rather under-developed topic within ICT ethics, where the majority of published work discusses issues such as "big data" and privacy or ethical issues of surveillance. In those cases, cybersecurity is usually only instrumentally discussed as a tool to protect (or undermine) privacy.

A second observation is that there are both common theme and differences across the three domains examined. In all domains, cybersecurity is recognized as being an **instrumental value**, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is perhaps the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data. The most prominent difference across the three domains regards the value of privacy, that is emphasized in business and health (together with confidentiality), but not in the national security domain, which appears concerned, above all, with the protecting the security and connectivity of infrastructure.

A third observation is that the ethical issues and dilemmas that the technological experts face in their daily life are to an insufficient degree represented in the literature, which may have several reasons, among which may be a lack of technical expertise of technology ethicists and a culture of secrecy among cybersecurity experts.

Finally, it is noteworthy that cybersecurity has different connotations in different social domains and these connotations affect the framing of problems and value assumptions in each domain. It is therefore plausible to think that thematic cross-pollution across different disciplines could be particularly fruitful. The health-related discussion could benefit from a little more emphasis on the need to protect vulnerable infrastructure. The discussion in national security could benefit from taking privacy more seriously. The discussion in business could also benefit from considering cybersecurity as a public good, to which businesses ought to contribute, rather than as (very important) factor in the relationship with its customer.

Appendix

A.1 Methodology

This section explains in detail how the papers have been selected that provided the basis for this White Paper. The aim of our search was to identify all relevant papers that explicitly deal with ethical issues related to cybersecurity, whereas the general theme of the paper was related to one of our three reference domains (health, business/finance and national security). The search was performed in two literature databases: Web of Science Core Collection (WoS) and Scopus. Scopus turned out to be a more comprehensive database, as it has a broader coverage of conference proceedings, which is an important publication channel for technical papers. However, the WoS data allows for more refined bibliometric studies, so that we used both databases. Some analysis steps have only been performed in one database; this will be indicated below.

Conceptually, the analysis consisted of the following four steps:

1) Step 1 – Characterize the field-specific Boolean search expressions. The aim of this step is to identify the Boolean search expressions that allows for a comprehensive, but distinctive identification of papers that likely deal with the following main fields of relevance: First, papers related to cybersecurity issues in general (=CYBER); second, papers associated to one of the three reference domains (=HEALTH, BUSINESS, NATIONAL); third, papers that include ethics-related keywords (=ETHICS). The keyword set for Step 1 has been identified solely in the Scopus database, as this offers a broader coverage of the technical literature. Step 1 has been performed by UZH.
2) Step 2 – Identify potentially relevant papers for each reference domain. Based on Step 1, potential papers of interest are then identified using the intersection sets of the searches (e.g. CYBER AND HEALTH AND ETHICS). However, this approach needed several refinement procedures such that the analysis and selection of the results is feasible. This step has been performed by UZH in both databases; duplicates have been identified and eliminated.
3) Step 3 – Complement the search result through snowballing and own expertise. One cannot expect that a purely quantitative search strategy will identify all relevant papers, e.g., because relevant papers may not contain the keywords used in the searches and because the lists generated are likely to contain irrelevant papers. Thus, the lists generated in step 2 have been screened for each reference domain by a team of two researchers. By reading relevant papers, the lists have been complemented by snowballing (i.e., we checked whether the found papers cite important papers that were not yet contained in the lists) and by domain-specific expertise of the team (i.e., based on their expertise, persons already knew about important papers; if they have not been identified beforehand, the papers have been added to the list).
4) Step 4 – Bibliometric analysis of the final sets. The final lists generated in step 3 were used for an in-depth bibliometric analysis in order to identify trends, important authors, financing sources and knowledge-transfer patterns (from publication subject categories to citation subject categories).

In the following, we outline in detail the procedure for each step.

A.1.1 Methodology of Step 1

We explain in the following the methodology for generating the Boolean search expression for CYBER. The procedure for the other Boolean search expressions was similar and we will only present the result for the other expressions. Step 1 has mainly been performed from October 2016 to January 2017. The search has been performed in Scopus (title, abstract, keywords).

In a first iteration, all members of the CANVAS consortium provided keyword candidates for characterizing the cybersecurity domain. Those candidates were grouped in three main classes; each main class consisted of sub-classes of 3-27 keywords each (the keywords took issues like word-stem variation, singular/plural etc. into account.). Those main classes were:

- General topic, with the sub-classes: keywords directly characterizing cybersecurity; authentication; crime; critical infrastructure; cryptography; cyber conflict; forensics; surveillance.
- Malware unspecific, with the sub-classes: keywords directly characterizing malware; malware defense; malware types; malware behaviour types; web security.
- Malware specific, with the sub-classes: Bots; digital vandalism; Distributed Denial of Service; hacking; identity theft; phishing; spam.

Out of those keywords, the group first identified unambiguous keywords combined with OR. Then, sequentially new keywords have been added and their influence on the set of results has been checked. The goal was to identify keywords that increase the set of hits considerably without losing specificity. We eliminated unspecific keywords (i.e., keywords where more than 20% of the additional hits did not fall into the domain; we checked the first 100 hits to make this decision) and keywords that did not contribute considerably to the previous list of hits (less than 0.1% additional hits). By using this methodology, the final Boolean search string for CYBER was as follows:

CYBER	*"Computer Security" OR "Cyber Security" OR "Cybersecurity" OR "Cyber-security" OR "Data Security" OR "Hardware Security" OR "Information Security" OR "Internet Security" OR "IT Security" OR "Mobile Security" OR "Network Security" OR "Security Breaches" OR "Security Of Data" OR "Security Requirement*" OR "Security Software" OR "Security System*" OR "Security Threat*" OR "Security Vulnerabilit*" OR "System Security" OR "Web Security" OR "data leak*" OR "non-repudiation" OR sigint OR "voting system" OR cryptography OR cyberattack OR "cyber attack" OR cyberconflict OR "cyber conflict" OR cyberdefense OR "cyber defense" OR cyberterrorism OR "cyber terrorism" OR "cyber threat*" OR cyberthread* OR cyberwar* OR "cyber war*" OR "computer crim*" OR "cyber crim*" OR malware OR firewall OR botnet* OR "denial of service" OR DDoS*

This search generated 266 343 documents in Scopus, ranging from 1978 to 2017 (search performed on January 23, 2017).

Using a similar methodology (the number of consortium members that contributed to the initial set was smaller, depending on their expertise in the domain), the Boolean search expressions were as follows:

HEALTH	*health OR healthcare OR medical OR medicine OR patient*
BUSINESS	*banking OR business OR commerce OR company OR consumer OR finance OR payment OR sales OR shopping*
NATIONAL	*"national security" OR "law enforcement" OR police*

Those sets are smaller, because we searched for domain-specific keywords already within the set CYBER, thus the search expressions were less complex. For the refinement procedure (see step 2), some additional search terms were used.

Using an adapted methodology, a search string for identifying papers that include an ethics terminology was generated. In this case we run a consultation within the group to determine which ethical and normative terms were salient and, from the list thus obtained, we deleted only those that, when combined with the CYBER search string and with the HEALTH and BUSINESS domain strings, provided a large numbers (>90%) of irrelevant results (as judged based on a summary reading of the first 50 titles). The resulting search string was:

ETHICS *autonomy OR privacy OR value-driven OR "value driven" OR "European Value*" OR value-profile OR ethic* OR responsibilit* OR accountability OR right* OR value-sensitive OR "value sensitive" OR moral* OR "informed consent" OR philosoph* OR equality OR freedom OR ethic* OR "contextual integrity" OR politic* OR dignity OR democracy OR discrimination OR unfair* OR fair* OR non-discrimination OR utilitarian OR "diversity issue*" OR trustworthiness OR transparency OR confidentiality OR accountability OR voluntariness OR accessibility OR justice OR diversity*

A.1.2 Methodology of Step 2

Step 2 was performed in April to June 2017 in Scopus and WoS, cut-off-date for the search was December 31, 2016.

The first iterations were performed by the UZH team. Using the combinations of the Boolean expressions identified in step 1, the following results were found:

CYBER AND HEALTH AND ETHICS	WoS:	1539 records
	Scopus:	2183 records
CYBER AND BUSINESS AND ETHICS	WoS:	2386 records
	Scopus:	4098 records
CYBER AND NATIONAL AND ETHICS	WoS:	405 records
	Scopus:	1742 records

This initial search yielded too large numbers for a search by hand, whereas the numbers for the national security domain were considerably lower. The goal was to identify candidate sets in the order of ~1000 publications each (for the domains health and business). Therefore, the following orthogonal refinement strategies were used for the two domains health and business:

- First, only the sets CYBER AND HEALTH/BUSINESS were determined (without the additional condition ETHICS). Within those sets, only papers that were attributed to non-technical subject categories[18] were determined. The number of entries per category was checked. If the number was <70, all entries were taken. If the numbers were >70, only the 50 most cited papers were taken. The reason for this strategy was to identify candidates potentially relevant for the ethics of cybersecurity without imposing a preconceived idea of ethical salience defined by the ETHICS Boolean expression. Only non-technical papers were chosen, because the likelihood of finding papers that explicitly deal with ethical issues is likely to be higher.
- Second, within the sets defined above (CYBER AND HEALTH AND ETHICS, CYBER AND BUSINESS AND ETHICS), a cutoff of value for a minimal number of citations per paper was chosen such that the resulting sets have the size of approximately 500 publications.[19] Furthermore, as the citation criterion includes a bias for older papers (where more time was available to generate citations), also the first 500 papers (in terms of publication date) were chosen.

[18] For HEALTH, the following WoS subject categories were used: ethics, medical ethics, social issues, philosophy, humanities multidisciplinary, social sciences interdisciplinary, computer science interdisciplinary applications, social sciences biomedical, medicine legal, women's studies, sociology, law. In Scopus, the following subject categories were used: ADD. For BUSINESS, the following WoS subject categories were used: management, business, operations research, management science, ethics, social issues, humanities multidisciplinary, history philosophy of science, social sciences interdisciplinary, women's studies, sociology, law. In Scopus, the following subject categories were used: business, decision sciences, art and humanities, social sciences, economics, econometrics and finance, undefined. Remind that the WoS category scheme is much more fine-grained than the Scopus category scheme.

[19] The cutoff value had to be adapted per domain (due to different citation cultures per domain) and database in order to yield similar set sizes. For health, the cutoff values were 4 citations for WoS and Scopus; for business, the cutoff-value was 6 citations for WoS and 9 citations for Scopus.

The sets generated in this way were merged for each domain separately and duplications were identified and eliminated using a variety of tools.[20] All titles in the resulting list (1738 for health, 1533 for business, 1543 for national security) were manually reviewed and those records that, based on their title, immediately appeared to be irrelevant, were deleted. The resulting lists included 1360 records for health, 1451 for business, and 1213 for the national security domain. Those lists were then sent to three teams of two persons each (health: OTH, business: DCU, national security: TUD) for further processing.

A.1.3 Methodology of Step 3

The third step mainly was based on a qualitative analysis of the results of step 2. For each domain, a team of two researchers performed the following analysis:

- The papers of the lists were evaluated with respect to their relevance based on the abstract and (if needed) based on a full-text review. This analysis classified the papers into three categories:
    a) Papers that explicitly discuss ethical issues of cybersecurity.
    b) Papers that mention ethical issues (mainly) as a motivation to present a new technical cybersecurity solution (or the like)
    c) Papers that do not fall into categories a) and b) and that are considered irrelevant.
- References of papers of category a) were checked for additional relevant papers based on their citation in the text and/or their title. If they also explicitly discuss ethical issues of cybersecurity, they were added to the list.
- Finally, if the expertise of the team yielded relevant papers that were not found so far (e.g., through conference visits or professional exchange with colleagues), they were also added to the list.

The result of this process yielded the following papers that were taken for the final analysis:

Health domain:	74
Business domain:	35
National Security domain:	125

A.1.4 Methodology of Step 4

In step 4, we start from the final set of step 3 and we use the "result analysis" tool of Web of Science (https://apps.webofknowledge.com) in order to run bibliographic analytics on the literature results. To do so, we search all items from the three domains in the Web Of Science (WoS) Database and run analytics on the results for each domain, excluding a few records obtained from snowballing that are referred in the literature on the ethics of cybersecurity but are not specific to the ethics of cybersecurity. For the domain Health, the WoS search led to 57 results (out of 74 of the final list), for the domain Business, it led to x results (out of x of the final list), and for the domain National Security, it led to x results (out of x of the final list). In addition to this, we queried WoS for all articles (and other scientific publications) citing the records in our final lists. For the domain Health, we obtained x citing records, for the domain Business, x citing records, and for the domain National Security, x citing records.

For the record set of each domain, both the original sources and the citing material, we queried WoS for meta-data about the publications, in particular:

1) Authors
2) Conferences
3) Countries
4) The type of record (article, conference proceeding, review, other)

[20] First, the "find duplicates and merge" tool of Mendeley was used. Then Python Code was used to rapidly detect the errors generated by using the Mendeley tool. For the national security domain, only the Python script was used. Moreover, files had to be converted and exported into different formats, thus creating further sources of error, which had to be controlled and corrected both with Python code and manually.

5) Funding agencies
6) Affiliations
7) Records per year
8) Sources (journals etc)
9) Research areas
10) Web of Science categories

We provide a selection of this data with rankings and graphs, as relevant.

A.2 List of Papers

Papers we would recommend for readers to get an introduction are marked with a *.

Papers in the top 10th decile for citations (for each domain) are marked with (two) **.

Papers which were not used for the bibliographic analysis are marked with a "×".

We have used colors to indicate relevance to specific domains. The colour codes are as follows:

Health domain

Business domain

National Security domain

Abbas, Assad, and Samee U. Khan. "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds." *IEEE Journal of Biomedical and Health Informatics* 18, no. 4 (July 2014): 1431–41. doi:10.1109/JBHI.2014.2300846.

Abdul Ghani Azmi, I.M., S. Zulhuda, and S.P. Wigati Jarot. "Data Breach on the Critical Information Infrastructures: Lessons from the Wikileaks." In *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, 306–11. Kuala Lumpur, Malaysia: IEEE, 2012. doi:10.1109/CyberSec.2012.6246173.

Abreu, Rute, Liliane Segura, Fatima David, Henrique Formigoni, Jelena Legcevic, and Flavio Mantovani. "Ethics and Fraud in E-Banking Services." In *2015 10th Iberian Conference on Information Systems and Technologies (Cisti)*, edited by A. Rocha, G. P. Dias, A. Martins, L. P. Reis, and M. P. Cota. New York: Ieee, 2015.

Abreu R, David F, Segura L. E-banking services: Why fraud is important? Journal of Information Systems Engineering & management. 2016;1(2):120 ×

Adeel, M., A.A. Chaudhry, R.A. Shaikh, and S.I. Shah. "Taxonomy of Cyber Crimes and Legislation in Pakistan." In *Proceedings of 1st International Conference on Information and Communication Technology, ICICT 2005*, 2005:350. Karachi, Pakistan: IEEE, 2005. doi:10.1109/ICICT.2005.1598625.

Ahmad, Nehaluddin. "Privacy and the Indian Constitution: A Case Study of Encryption." *Communications of the IBIMA* 2009 (2009): Article ID 455684.

Ali, Azman, David Hutchison, Plamen Angelov, and Paul Smith. "Adaptive Resilience for Computer Networks: Using Online Fuzzy Learning." In *RNDM 2012 - 4th International Workshop on Reliable Networks Design and Modeling*, 791–97. St. Petersburg, Russia: IEEE, 2012.

Alouane, Meryeme, and Hanan El Bakkali. "Security, Privacy and Trust in Cloud Computing: A Comparative Study." *2015 International Conference on Cloud Technologies and Applications (Cloudtech 15)*, 2015, 1-8.

Alqahtani, A. "Towards a Framework for the Potential Cyber-Terrorist Threat to Critical National Infrastructure." *Information and Computer Security* 23, no. 5 (2015): 532–69. doi:10.1108/ICS-09-2014-0060.

Alqahtani, Abdulrahman. "The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia." In *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, edited by D. Hart, 231–39. Reading (UK): Academic Conferences and Publishing International Limited, 2013.

Altawy, Riham, and Amr M. Youssef. "Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices." *IEEE Access* 4 (2016): 959–79. doi:10.1109/ACCESS.2016.2521727.

Árnason, Vilhálmur "Coding and Consent: Moral Challenges of the Database Project in Iceland." *Bioethics* 18, no. 1 (February 2004): 27–49. doi:10.1111/j.1467-8519.2004.00377.x.**

Arquilla, John, and David Ronfeldt, eds. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 239–88. Santa Monica (CA): Rand Corporation, 2001.

Asllani, A., C.S. White, and L. Ettkin. "Viewing Cybersecurity as a Public Good: The Role of Governments, Businesses, and Individuals." *Journal of Legal, Ethical and Regulatory Issues* 16, no. 1 (2013): 7–14.

Ayatollahi, Haleh, Peter A. Bath, and Steve Goodacre. "Accessibility versus Confidentiality of Information in the Emergency Department." *Emergency Medicine Journal* 26, no. 12 (December 2009): 857–60. doi:10.1136/emj.2008.070557.

Bahsi, Hayretdin, and Olaf Manuel Maennel. "A Conceptual Nationwide Cyber Situational Awareness Framework for Critical Infrastructures." In *Secure It Systems, Nordsec 2015*, edited by S. Buchegger and M. Dam. Stockholm, Sweden, 2015. https://link.springer.com/chapter/10.1007/978-3-319-26502-5_1.

Barnard-Wills, David, and Debi Ashenden. "Securing Virtual Space: Cyber War, Cyber Terror,and Risk." *Space and Culture* 15, no. 2 (May 2012): 110–23. doi:10.1177/1206331211430016.**

Barrett, Edward T. "Warfare in a New Domain: The Ethics of Military Cyber-Operations." *Journal of Military Ethics* 12, no. 1 (2013): 4–17.

Barros-Bailey, Mary, and Jodi L. Saunders. "Ethics and the Use of Technology in Rehabilitation Counseling." *Rehabilitation Counseling Bulletin* 53, no. 4 (July 2010): 255–59. doi:10.1177/0034355210368867.

Barrows, Randolph C., and Paul D. Clayton. "Privacy, Confidentiality, and Electronic Medical Records." *Journal of the American Medical Informatics Association* 3, no. 2 (April 1996): 139–48.**

Batchelor, Rachel, Ania Bobrowicz, Robin Mackenzie, and Alisoun Milne. "Challenges of Ethical and Legal Responsibilities When Technologies' Uses and Users Change: Social Networking Sites, Decision-Making Capacity and Dementia." *Ethics and Information Technology* 14, no. 2 (June 2012): 99–108. doi:10.1007/s10676-012-9286-x.

Bendrath, Ralf. "From Cyberterrorism to Cyberwar, Back and Forth : How the United States Securitized Cyberspace." In *International Relations and Security in the Digital Age*, edited by Johan Eriksson and Giampiero Giacomello, 57–82. London: Routledge, 2007. http://www.diva-portal.org/smash/record.jsf?pid=diva2:404792.

----------"The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection." *ISIJ Information & Security: An International Journal* 7 (2001): 80–103.

Bennasar, Hanane, Mohammad Essaaidi, Ahmed Bendahmane, and Jalel Ben-othman. "State-of-The-Art of Cloud Computing Cyber-Security." In *Proceedings of 2015 Third Ieee World Conference on Complex Systems (Wccs)*, edited by M. Essaaidi and M. Nemiche. Marrakech, Morocco: IEEE, 2015. doi:10.1109/ICoCS.2015.7483283.

Betz, David J, and Tim Stevens. *Cyberspace and the State toward a Strategy for Cyber-Power*. Abingdon: Routledge, 2011. http://www.tandfonline.com/toc/tadl20/51/424.

Bodle, Robert. "Regimes Of Sharing: Open APIs, Interoperability, and Facebook." *Information Communication & Society* 14, no. 3 (2011): 320–37. doi:10.1080/1369118X.2010.542825.

Bonner, Steven, and Eleanor O'Higgins. "Music Piracy: Ethical Perspectives." *Management Decision* 48, no. 9 (2010): 1341–54. doi:10.1108/00251741011082099.

Bourret, Christian, and Olivia Pestana. "Information Systems and Patients' Empowerment around Patients' Pathways: The French and the Portuguese Scenarios." *Qualitative & Quantitative Methods in Libraries* 4 (December 2015): 767–73.

Brey, Philip. "Ethical Aspects of Information Security and Privacy." In *Security, Privacy, and Trust in Modern Data Management*, 21–36. Data-Centric Systems and Applications. Berlin/Heidelberg: Springer, 2007. http://link.springer.com/content/pdf/10.1007/978-3-540-69861-6.pdf#page=36.

Brumnik, Robert, and Iztok Podbregar. "How Terrorists Use the Internet." In *Policing in Central and Eastern Europe–Social Control of Unconventional Deviance*, edited by G. Mesko, A. Sotlar, and J. Winterdyk, 157–74. Maribor: University of Maribor, Faculty of Criminal Justice and Security, 2011.

Bucci, Steven. "Joining Cybercrime and Cyberterrorism: A Likely Scenario." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, edited by Derek S Reveron. Washington, DC: Georgetown University Press, 2012. http://www.jstor.org/stable/j.ctt2tt6rz. ×

Buckovich, Suzy A., Helga E. Rippen, and Michael J. Rozen. "Driving Toward Guiding Principles: A Goal for confidentiality, and Security of Health Information." *Journal of the American Medical Informatics Association* 6, no. 2 (April 1999): 122–33.

Bunnik, Eline M., Maartje H. N. Schermer, and A. Cecile J. W. Janssens. "Personal Genome Testing: Test Characteristics to Clarify the Discourse on Ethical, Legal and Societal Issues." *BMC Medical Ethics* 12 (June 2011): 11. doi:10.1186/1472-6939-12-11.

Caldicott, Dame F., Kingsley Manning: "A Guide to Confidentiality in Health and Social Care: Treating Confidential Information with Respect." Health & Social Care Information Center (September 2013). Accessed August 4, 2017. http://content.digital.nhs.uk/media/12822/Guide-to-confidentialityin-health-and-socialcare/pdf/HSCIC-guide-to-confidentiality.pdf.

Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey." *Journal of Biomedical Informatics* 55 (June 2015): 272–89. doi:10.1016/j.jbi.2015.04.007.

Cambon-Thomsen, Anne, Emmanuelle Rial-Sebbag, and Bartha M. Knoppers. "Trends in Ethical and Legal Frameworks for the Use of Human Biobanks." *European Respiratory Journal* 30, no. 2 (August 2007): 373–82. doi:10.1183/09031936.00165006.**

Capek, Jan, and Jana Hola. “Cybersecurity Within Cyberspace.” In *Idimt-2016- Information Technology, Society and Economy Strategic Cross-Influences*, edited by D. Petr, C. Gerhard, and O. Vaclav, 325–32. Linz: Trauner Verlag, 2016.

Carr, Madeline. “Public-Private Partnerships in National Cyber-Security Strategies.” *International Affairs* 92, no. 1 (January 2016): 43–62. doi:10.1111/1468-2346.12504.**

Caudle, Daryl. “Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context into Poliheuristic Decision Theory.” In *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, edited by D. Hart, 240–47. Reading (UK): Academic Conferences Ltd., 2013.

Caulfield, Timothy, Amy L. McGuire, Mildred Cho, Janet A. Buchanan, Michael M. Burgess, Ursula Danilczyk, Christina M. Diaz, et al. “Research Ethics Recommendations for Whole-Genome Research: Consensus Statement.” *PLoS Biology* 6, no. 3 (March 2008): 430–35. doi:10.1371/journal.pbio.0060073.**

Caulfield, Timothy, Ross EG Upshur, and Abdallah Daar. “DNA Databanks and Consent: A Suggested Policy Option Involving an Authorization Model.” *BMC Medical Ethics* 4 (January 2003): 1. doi:10.1186/1472-6939-4-1.

Cavelty, Myriam Dunn. “Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate.” *Journal of Information Technology and Politics* 4, no. 1 (2008): 19–36. doi:10.1300/J516v04n01_03.

---------- “The Militarisation of Cyberspace: Why Less May Be Better.” In *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings*. Tallinn, Estonia: IEEE, 2012. http://ieeexplore.ieee.org/document/6243971/.

---------- “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse.” *International Studies Review* 15, no. 1 (March 2013): 105–22. doi:10.1111/misr.12023.**

--------- “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.” *Science and Engineering Ethics* 20, no. 3 (September 2014): 701–15. doi:10.1007/s11948-014-9551-y.**

Dunn Cavelty, M., V. Mauer, and S. Krishna-Hensel, eds. “Concluding Remarks: The Role of the State in Securing the Information Age–challenges and Prospects.” In *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace.*, 130–51. Aldershot, England: Ashgate, 2007.

Chang, Betty L., Suzanne Bakken, S. Scott Brown, Thomas K. Houston, Gary L. Kreps, Rita Kukafka, Charles Safran, and P. Zoe Stavri. “Bridging the Digital Divide: Reaching Vulnerable Populations.” *Journal of the American Medical Informatics Association* 11, no. 6 (December 2004): 448–57. doi:10.1197/jamia.M1535.**

Chaturvedi, Manmohan, Aynur Unal, Preeti Aggarwal, Shilpa Bahl, and Sapna Malik. “International Cooperation in Cyber Space to Combat Cyber Crime and Terrorism.” In *2014 Ieee Conference on Norbert Wiener in the 21st Century (21cw)*, edited by M. Gibbs. Boston (MA): IEEE, 2014. http://ieeexplore.ieee.org/document/6893915/.

Chen, Yasha, Xinjie Zhao, Wen Li, and Jianpeng Zhao. “A New Architecture for Cloud Computing System Protection.” In *2013 International Conference on Advanced Cloud and Big Data (Cbd)*, 46–50. Nanjing, China: IEEE, 2013. doi:10.1109/CBD.2013.6.

Chow-White, Peter A., Maggie MacAulay, Anita Charters, and Paulina Chow. "From the Bench to the Bedside in the Big Data Age: Ethics and Practices of Consent and Privacy for Clinical Genomics and Personalized Medicine." *Ethics and Information Technology* 17, no. 3 (September 2015): 189–200. doi:10.1007/s10676-015-9373-x.

Christen M, Fischer J, Huppenbauer M, Tanner C, van Schaik C (eds.) (2014): Empirically Informed Ethics. Morality between Facts and Norms. Library of Ethics and Applied Philosophy. Springer, Berlin (349 pp.) x

Christen M, Ineichen C, Tanner C (2014b): How moral are the principles of biomedical ethics? BMC Medical Ethics 15: 47 x

Christen M, Narvaez D, Tanner C, Ott T (2016): Mapping Values: Using Thesauruses to Reveal Semantic Structures of Cultural Moral Differences. Cognitive Systems Research 40: 59-74 x

Christensen, S., W.J. Caelli, W.D. Duncan, and E. Georgiades. "An Achilles Heel: Denial of Service Attacks on Australian Critical Information Infrastructures." *Information and Communications Technology Law* 19, no. 1 (2010): 61–85. doi:10.1080/13600831003708059.

Conger, Sue, Joanne H. Pratt, and Karen D. Loch. "Personal Information Privacy and Emerging Technologies." *Information Systems Journal* 23, no. 5 (September 2013): 401–17. doi:10.1111/j.1365-2575.2012.00402.x.

Creasey, J.C. "Protecting Critical National Infrastructure through Collaborative Cyber Situational Awareness." In *8th IET International System Safety Conference Incorporating the Cyber Security Conference 2013*, Vol. 2013. IET Conference Publications, 2013. doi:10.1049/cp.2013.1708.

Cutts, Andrew. "Warfare and the Continuum of Cyber Risks: A Policy Perspective." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, edited by C. Czosseck and K. Geers, 66–76. Amsterdam: IOS Press, 2009.

Czosseck, Christian, Rain Ottis, and Anna-Maria Talihaerm. "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security." In *Proceedings of the 10th European Conference on Information Warfare and Security*, edited by R. Ottis, 57–64. Estonia 7-8 July 2011.

D'Arcy, John, and Anat Hovav. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures." *Journal of Business Ethics* 89 (2009): 59–71.

Da Veiga, Adele. "A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument." In *Proceedings of the 2016 SAI Computing Conference (SAI)*, 1006–15. London, UK: IEEE, 2016.

Davis, Gaye. "State Security in Charge of Cybercrime Plans | Dailynews." *Independent Media Online*. February 20, 2012, Daily News edition. https://www.iol.co.za/dailynews/news/state-security-in-charge-of-cybercrime-plans-1238243.

Dawson, M. "A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism." In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*, edited by M. Dawson and O. Marvan, 1–7. Hershey PA, USA: Igi Global, 2015. doi:10.4018/978-1-4666-8345-7.ch001.

De Abajo, Francisco J., Lydia F. Grande, Javier J. Gutiérrez, Mara C. M. Arribas, Benedetto Terracini, Teresa P. Ros, Jaime C. Castelló, Amelia M. Uranga, Moisés A. Alonso, Joaquin H. Carranza and Maria J. S. Martinez. "Ethical Guidelines Governing the Creation and Use of Registries for Biomedical Research Puposes." Ethics Committee of the Rare Disease Research Institute, 2007.

De Vries, Jantina, Muminatou Jallow, Thomas N. Williams, Dominic Kwiatkowski, Michael Parker, and Raymond Fitzpatrick. "Investigating the Potential for Ethnic Group Harm in Collaborative Genomics Research in Africa: Is Ethnic Stigmatisation Likely?" *Social Science & Medicine* 75, no. 8 (October 2012): 1400–1407. doi:10.1016/j.socscimed.2012.05.020.

Dean, Matthew D., Dinah M. Payne, and Brett J. L. Landry. "Data Mining: An Ethical Baseline for Online Privacy Policies." *Journal of Enterprise Information Management* 29, no. 4 (2016): 482–504. doi:10.1108/JEIM-04-2014-0040.

Deibert, Ronald J. "Cyber-Security and Threat Politics: US Efforts to Secure the Information Age." *International Studies Review* 11, no. 2 (June 2009): 373–75.

Deibert, Ronald. Tracking the Emerging Arms Race in Cyberspace." *Bulletin of the Atomic Scientists* 67, no. 1 (February 2011): 1–8. doi:10.1177/0096340210393703.

Demchak, C.C. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens and London: The University of Georgia Press, 2011.

Dennis, A., R. Jones, D. Kildare, and C. Barclay. "Design Science Approach to Developing and Evaluating a National Cybersecurity Framework for Jamaica." *Electronic Journal of Information Systems in Developing Countries* 62, no. 1 (2014).

Devillier, Nathalie. "Ageing, Well-Being and Technology: From Quality of Life Improvement to Digital Rights Management: A French Perspective." *Proceedings of the 2016 ITU Kaleidoscope Academic Conference - ICTs for a Sustainable World (ITU WT)*, 2016, 41–47.

Dillon, Gurpreet, Tiago Oliveira, Santa Susarapu, and Mario Caldeira. "Deciding between Information Security and Usability: Developing Value Based Objectives." *Computers in Human Behavior* 61 (August 2016): 656–66. doi:10.1016/j.chb.2016.03.068.

Docherty, Annemarie B., and Nazir I. Lone. "Exploiting Big Data for Critical Care Research." *Current Opinion in Critical Care* 21, no. 5 (October 2015): 467–72. doi:10.1097/MCC.0000000000000228.

Dodig-Crnkovic, Gordana. "On the Importance of Teaching Professional Ethics to Computer Science Students." In *Computing and Philosophy Conference, E-CAP*. London: College Publications, 2004. http://www.idt.mdh.se/personal/gdc/work/TeachingProfEthics.pdf.

Dong, L.N. *Design of Computer Information Network Security System*. Vol. 539. Applied Mechanics and Materials. Zurich: Trans Tech Publications Inc., 2014. doi:10.4028/www.scientific.net/AMM.539.305.

Dong, Naipeng, Hugo Jonker, and Jun Pang. "Challenges in eHealth: From Enabling to Enforcing Privacy." In Foundations of Health Informatics Engineering and System, 195–206. Springer, 2011. Accessed August 4, 2017. http://link.springer.com/content/pdf/10.1007/978-3-642-32355-3.pdf#page=205.

Dunn Cavelty, M. (2014). "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", Science and Engineering Ethics, Volume 20, Issue 3, September 2014, Pages 701-715, DOI: 10.1007/s11948-014-9551-y.

Elkhannoubi, H., and M. Belaissaoui. "A Framework for an Effective Cybersecurity Strategy Implementation: Fundamental Pillars Identification." In *International Conference on Intelligent Systems Design and Applications, ISDA 2015*. Marrakech, Morocco, 2016. doi:10.1109/ISDA.2015.7489156.

Eun, Yong-Soo, and Judith Sita Amann. "Cyberwar: Taking Stock of Security and Warfare in the Digital Age." *International Studies Perspectives* 17, no. 3 (August 2016): 343–60. doi:10.1111/insp.12073.

Faqir, R.S.A. "Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010." *International Journal of Cyber Criminology* 7, no. 1 (2013): 81–90.

Fayomi, Oluyemi, Oly Nelson Ndubisi, Charles Ayo, Felix Chidozie, Lady Ajayi, and Uchechukwu Okorie. "Cyber-Attack as a Menace to Effective Governance in Nigeria." Edited by C. Adams. *Proceedings of the 15th European Conference on Egovernment*, 2015, 107–16.

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US Legislative Efforts to Address Cybercrime." *Journal of Homeland Security and Emergency Management* 10, no. 1 (2013). doi:10.1515/jhsem-2012-0007.

France, Francis H. Roger. "Ethics and Biomedical Information." *International Journal of Medical Informatics* 49, no. 1 (March 1998): 111–15. doi:10.1016/S1386-5056(98)00018-5.

Garvie C., Bedoya A. M., and Frankle J. 2016. The perpetual line-up. Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology. ×

Gattiker, U. E., and H. Kelley. "Morality and Computers: Attitudes and Differences in Moral Judgments." *Information Systems Research* 10, no. 3 (September 1999): 233–54. doi:10.1287/isre.10.3.233.**

Geers, K. "The Challenge of Cyber Attack Deterrence." *Computer Law and Security Review* 26, no. 3 (2010): 298–303. doi:10.1016/j.clsr.2010.03.003.

------ "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Journal of Digital Forensic Practice* 3, no. 2–4 (2010): 124–30. doi:10.1080/15567281.2010.536735.

Ghernouti-Helie, Solange. "A National Strategy for an Effective Cybersecurity Approach and Culture." *Fifth International Conference on Availability, Reliability, and Security: Ares 2010, Proceedings*, 2010, 370–73. doi:10.1109/ARES.2010.119.

Ghioni, F. "National Security and Threat Awareness." In *Data Mining VI: Data Mining, Text Mining and Their Business Applications*, edited by A. Zanasi, C. A. Brebbia, and N. F. F. Ebecken, 381–87, 2005.

Godard, Béatrice, Sandy Raeburn, Marcus Pembrey, Martin Bobrow, Peter Farndon and Ségolène Aymé. "Genetic Information and Testing in Insurance and Employment: Technical, Social and Ethical Issues. *European Journal of Human Genetics* 11, no. 2 (December 2003): 123-42. doi: 10.1038/sj.ejhg.5201117.

Goldman, H., R. McQuaid, and J. Picciotto. "Cyber Resilience for Mission Assurance." In *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 236–41. Waltham, MA, USA: IEEE, 2011. doi:10.1109/THS.2011.6107877.

Grabosky, P. "Organised Crime and the Internet: Implications for National Security." *RUSI Journal* 158, no. 5 (2013): 18–25. doi:10.1080/03071847.2013.847707.

Granado, N., and G. White. "Cyber Security and Government Fusion Centers." Waikoloa, HI, USA: IEEE, 2008. doi:10.1109/HICSS.2008.111.

Grant, Jeremy A. "The National Strategy for Trusted Identities in Cyberspace Enhancing Online Choice, Efficiency, Security, and Privacy through Standards." *Ieee Internet Computing* 15, no. 6 (December 2011): 80–84.

Greenbaum, Dov, Andrea Sboner, Xinmeng Jasmine Mu, and Mark Gerstein. "Genomics and Privacy: Implications of the New Reality of Closed Data for the Field." *PLoS Computational Biology* 7, no. 12 (December 2011): e1002278. doi:10.1371/journal.pcbi.1002278.

Greiman, Virginia. "To Catch a Thief in the Cloud: A Paradigm for Law Enforcement." In *Proceedings of the 9th International Conference on Cyber Warfare and Security (Iccws-2014)*, edited by S. Liles, 77–83. London: Academic Conferences and Publishing International Limited, 2014.

Grobler, M., J.J. Van Vuuren, and L. Leenen. "Implementation of a Cyber Security Policy in South Africa: Reflection on Progress and the Way Forward." In *ICT Critical Infrastructures and Society. Proceedings.*, Vol. 386 AICT. IFIP Advances in Information and Communication Technology. Berlin: Springer, 2012. doi:10.1007/978-3-642-33332-3_20.

Gunarto, Harry. "Ethical Issues in Cyberspace and IT Society." Paper given at the Symposium on Whither The Age of Uncertainty, Ritsumeika Asia Pacific University, 2003/01/23. http://www.apu.ac.jp/~gunarto/it1.pdf

Gutmann, A. W., J. W. Wagner, Y. Ali, A. L. Allen, J. D. Arras, B. F. Atkinson, N. A. Farahany, et al. "Privacy and Progress in Whole Genome Sequencing." Washington, D.C.: Presidential Commission for the Study of Bioethical Issues, October 2012.

Harrington, S. J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions." *Mis Quarterly* 20, no. 3 (September 1996): 257–78. doi:10.2307/249656.**

Harrop, W., and A. Matteson. "Cyber Resilience: A Review of Critical National Infrastructure and Cyber Security Protection Measures Applied in the UK and USA." *Journal of Business Continuity & Emergency Planning* 7, no. 2 (2013): 149–62.

Hashim, M.S., M.N. Masrek, and Z. Yunos. "Elements in the Cyber Security Framework for Protecting the Critical Information Infrastructure against Cyber Threats." *Information (Japan)* 19, no. 7B (2016): 2989–94.

Hens, Kristien, Emmanuelle Lévesque, and Kris Dierickx. "Children and Biobanks: A Review of the Ethical and Legal Discussion." *Human Genetics* 130, no. 3 (September 2011): 403–13. doi:10.1007/s00439-011-1031-8.

Hiller, Janine S., and Roberta S. Russell. "The Challenge and Imperative of Private Sector Cybersecurity: An International Comparison." *Computer Law & Security Review* 29, no. 3 (June 2013): 236–45. doi:10.1016/j.clsr.2013.03.003.**

Hoedemaekers, Rogeer, Bert Gordijn, and Martien Pijnenburg. "Solidarity and Justice as Guiding Principles in Genomic Research." *Bioethics* 21, no. 6 (July 2007): 342–50. doi:10.1111/j.1467-8519.2007.00562.x.

Hui, Lucas C. K., K. P. Chow, and S. M. Yiu. "Tools and Technology for Computer Forensics: Research and Development in Hong Kong (Invited Paper)." In *Information Security Practice and Experience, Proceedings*, edited by E. Dawson and D. S. Wong, 11–19. LNCS 4464. Berlin/Heidelberg: Springer, 2007.

Hunton, Paul. "A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment." *Digital Investigation* 7, no. 3–4 (April 2011): 105–13. doi:10.1016/j.diin.2011.01.002.

Ienca, Marcello, and Pim Haselager. "Hacking the Brain: Brain-Computer Interfacing Technology and the Ethics of Neurosecurity." *Ethics and Information Technology* 18, no. 2 (June 2016): 117–29. doi:10.1007/s10676-016-9398-9.

Ikonen, Veikko, and Eija Kaasinen. "Ethical Assessment in the Design of Ambient Assisted Living." In *Assisted Living Systems - Models, Architectures and Engineering Approaches*, edited by Arthur I. Karshmer, Jürgen Nehmer, Hartmut Raffler, and Gerhard Tröster. Dagstuhl Seminar Proceedings. Dagstuhl, Germany: Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany, 2008. http://drops.dagstuhl.de/opus/volltexte/2008/1462.

Introna L., Wood D. 2004. "Picturing algorithmic surveillance: the politics of facial recognition systems." In: Surveillance & Society 2 (2/3): 177-198. URN: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-200675 ×

Jain, N., D.R. Kalbande, and P. Sharma. "Empirical Relationship between Victim's Occupation and Their Knowledge of Digital Forensic," 21-22-March-2016:61–65, 2016. doi:10.1145/2909067.2909077.

Jakobson, G., and M.N. Schmitt. "Proceedings: Foreword." In *2012 4th International Conference on Cyber Conflict, CYCON 2012 - Proceedings*. Tallinn, Estonia: IEEE, 2012. http://ieeexplore.ieee.org/document/6243959/

Jica, H. "Cyber Security and National Security Awareness Initiatives in Albania: A Synergy Approach." *Mediterranean Journal of Social Sciences* 4, no. 10 (2013): 614–22. doi:10.5901/mjss.2013.v4n10p614.

Kaminski, Ryan T. "Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions." In *Conference on Cyber Conflict. Proceedings 2010*, edited by C. Czosseck and K. Podins, 2010. https://ccdcoe.org/multimedia/conference-cyber-conflict-proceedings-2010.html.

Kaplan, Bonnie, and Sergio Litewka. "Ethical Challenges of Telemedicine and Telehealth." *Cambridge Quarterly of Healthcare Ethics* 17, no. 4 (Fall 2008): 401–16. doi:10.1017/S0963180108080535.

Karabacak, Bilge, and Unal Tatar. "Strategies to Counter Cyberattacks: Cyberthreats and Critical Infrastructure Protection." In *Critical Infrastructure Protection*, edited by M. Edwards, 116:63–73, 2014.

--------- "Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey." *Computer Law & Security Review* 32, no. 3 (June 2016): 526–39. doi:10.1016/j.clsr.2016.02.005.

Karabacak, Bilge, Sevgi Ozkan Yildirim, and Nazife Baykal. "A Vulnerability-Driven Cyber Security Maturity Model for Measuring National Critical Infrastructure Protection Preparedness." *International Journal of Critical Infrastructure Protection* 15 (December 2016): 47–59. doi:10.1016/j.licip.2016.10.001.

Kask, R.J. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." In *Strategies for Trusted Identities and Infrastructure in Cyberspace*, by R. J. Kask, 49–127. New York: Nova Science Publishers, 2011.

Kasper, A. "The Fragmented Securitization of Cyber Threats." In *Regulating Etechnologies in the European Union: Normative Realities and Trends*, edited by Tanel Kerikmäe, 157–88. Cham: Springer International Publishing, 2014. doi:10.1007/978-3-319-08117-5_9.

Kiggins, R.D. "Us Leadership in Cyberspace: Transnational Cyber Security and Global Governance." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller, 161–80. Berlin: Springer, 2014. doi:10.1007/978-3-642-37481-4_10.

Kim, J., S. Park, and T. Hyun. "An Inquiry into International Countermeasures against Cyberterrorism." In *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005.* Phoenix Park, South Korea: IEEE, 2005. doi:10.1109/ICACT.2005.245895.

Kittinger, R., L. Kittinger, and G.E. Avina. "Job Analysis and Cognitive Task Analysis in National Security Environments." In *Foundations of Augmented Cognition: Neuroergonomics and Operational Neuroscience*, 341–47. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 9743. Berlin/Heidelberg: Springer, 2016. doi:10.1007/978-3-319-39955-3_32.

Kjaerland, M. "Profiling Coordinated Cyber Incidents towards the Critical Infrastructure in Norway." *International Journal of Critical Infrastructures* 4, no. 4 (2008): 335–52. doi:10.1504/IJCIS.2008.020155.

Klare B.F., Burge M.J., Klontz J.C., Vorder Bruegge R.W., and Jain A.K. 2012. "Face Recognition Perfor-mance: Role of Demographic Information." IEEE Transactions on Information Forensics and Security 7 (6): 1789-1801. ×

Kluge, Eike-Henner W. "E-Health Promises and Challenges: Some Ethical Considerations." In *International Perspectives in Health Informatics*, edited by E. M. Borycki, J. A. BartleClar, M. S. Househ, C. E. Kuziemsky, and E. G. Schraa, 148–53. Studies in Health Technology and Informatics 164. Amsterdam: IOS Press, 2011.

Knoppers, Bartha Maria. "Framework for Responsible Sharing of Genomic and Health-Related Data." *The HUGO Journal* 8 (2014): 3.

Kotsopoulou, Anastasia, Athanasios Melis, Violetta-Irene Koutsompou, and Christina Karasarlidou. "E-Therapy: The Ethics behind the Process." *Procedia Computer Science* 65 (2015):492–99.

Kouatli, Issam. "Managing Cloud Computing Environment: Gaining Customer Trust with Security and Ethical Management." In *Promoting Business Analytics and Quantitative Management of Technology: 4th International Conference on Information Technology and Quantitative Management (Itqm 2016)*, edited by H. Lee, Y. Shi, J. Lee, F. Cordova, I. Dzitac, G. Kou, and J. Li, 91:412–21. Amsterdam: Elsevier Science Bv, 2016.

Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by Franklin D Kramer, Stuart H Starr, and Larry K Wentz, 1–23. Lincoln NE: University of Nebraska Press, 2009.

Kugler, Richard L. "Deterrence of Cyber Attacks." In *Cyberpower and National Security*, edited by Franklin D Kramer, Stuart H Starr, and Larry K Wentz. Lincoln NE: University of Nebraska Press, 2009.

Lane, Julia, and Claudia Schur. "Balancing Access to Health Data and Privacy: A Review of the Issues and Approaches for the Future." *Health Services Research* 45, no. 5 (October 2010): 1456–67. doi:10.1111/j.1475-6773.2010.01141.x.

Laur, Audrey. "Fear of E-Health Records Implementation?" *Medico-Legal Journal* 83, no. 1 (March 2015): 34–39. doi:10.1177/0025817214540396.

Lawson S. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday* 17, no. 7 (2012). http://firstmonday.org/ojs/index.php/fm/article/view/3848

Lee, Daeseob, and Dongho Won. "A Study on Security Management Service System for Wireless Network Environment." *Applied Mathematics & Information Sciences* 6 (January 2012): 209–20.

Lee, K.-B., and J.-I. Lim. "The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-Terror Attack on the Korea Hydro & Nuclear Power Co., Ltd." *KSII Transactions on Internet and Information Systems* 10, no. 2 (2016): 857–80. doi:10.3837/tiis.2016.02.023.

Lehto, M. "The Ways, Means and Ends in Cyber Security Strategies." In *European Conference on Information Warfare and Security, ECCWS*, 182–90. London: Academic Conferences and Publishing International, 2013.

Leiwo, J., and S. Heikkuri. "An Analysis of Ethics as Foundation of Information Security in Distributed Systems." In *Proceedings of the Thirty-First Hawaii International Conference on System Sciences, Vol Vi: Organizational Systems and Technology Track*, edited by H. J. Watson, 213–22. Los Alamitos: Ieee Computer Soc, 1998.

Leukfeldt, R., S. Veenstra, and W. Stol. "High Volume Cyber Crime and the Organization of the Police: The Results of Two Empirical Studies in the Netherlands." *International Journal of Cyber Criminology* 7, no. 1 (2013): 1–17.

Li, X. "Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime." *International Journal of Cyber Criminology* 9, no. 2 (2016): 185–204. doi:10.5281/zenodo.56225.

Liu, E.C., G. Stevens, K.A. Ruane, A.M. Dolan, and R.M. Thompson. "Cybersecurity: Selected Legal Issues." In *Cybersecurity and Related Federal Laws: Revision Proposals*, 81–141. New York: Nova Science Publishers, 2012.

Lowrance, William W. "Privacy, Confidentiality, and Identifiability in Genomic Research: Discussion document for workshop convened by the National Human Genome Research Institute, Bethesda, October 3-4, 2006.". Accessed August 4, 2017. https://www.genome.gov/pages/about/od/reportspublications/identifiabilityworkshopwhitepaper.pdf.

Lowry, Paul Benjamin, Clay Posey, Tom L. Roberts, and Rebecca J. Bennett. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse." *Journal of Business Ethics* 121, no. 3 (2014): 385–401.

Lupton, Deborah. "Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps." *Culture Health & Sexuality* 17, no. 4 (April 2015): 440–53. doi:10.1080/13691058.2014.920528.

Mascalzoni, Deborah, Edward S. Dove, Yaffa Rubinstein, Hugh J. S. Dawkins, Anna Kole, Pauline McCormack, Simon Woods, et al. "International Charter of Principles for Sharing Bio-Specimens and Data." *European Journal of Human Genetics* 23, no. 6 (June 2015): 721–28. doi:10.1038/ejhg.2014.197.

Matwyshyn, Andrea M. "CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices." *Journal of Business Ethics* 88 (September 2009): 579–94. doi:10.1007/s10551-009-0312-9.

McClanahan, Kitty. "Balancing Good Intentions: Protecting the Privacy of Electronic Health Information" *Bulletin of Science, Technology & Society* 28 no. 1 (2007): 69–79. ×

McCormack, Pauline, Anna Kole, Sabina Gainotti, Deborah Mascalzoni, Caron Molster, Hanns Lochmüller, and Simon Woods. "'You Should at Least Ask'. The Expectations, Hopes and Fears of Rare Disease Patients on Large-Scale Data and Biomaterial Sharing for Genomics Research." *European Journal of Human Genetics* 24, no. 10 (October 2016): 1403–8. doi:10.1038/ejhg.2016.30.

McCormack, Pauline, Simon Woods, Annemieke Aartsma-Rus, Lynn Hagger, Agnes Herczegfalvi, Emma Heslop, Joseph Irwin, et al. "Guidance in Social and Ethical Issues Related to Clinical, Diagnostic Care and Novel Therapies for Hereditary Neuromuscular Rare Diseases: "Translating" the Translational." *PLoS Currents* 5 (January 2013). doi:10.1371/currents.md.f90b49429fa814bd26c5b22b13d773ec.

McGraw, Deven, James X. Dempsey, Leslie Harris, and Janlori Goldman. "Privacy As An Enabler, Not An Impediment: Building Trust Into Health Information Exchange." *Health Affairs* 28, no. 2 (April 2009): 416–27. doi:10.1377/hlthaff.28.2.416.**

McGraw, Gary, Richard Clarke, Silver Bullet, and Gary McGraw. "Silver Bullet Talks with Richard Clarke." *Ieee Security & Privacy* 8, no. 4 (August 2010): 5–11.

McNally, Julie. "Improving Public-Private Sector Cooperation on Cyber Event Reporting." Edited by D. Hart. *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, 2013, 147–53.

McReynolds, Phillip. "How to Think About Cyber Conflicts Involving Non-State Actors." *Philosophy & Technology* 28, no. 3 (September 1, 2015): 427–48. doi:10.1007/s13347-015-0187-x.

Meinrath, Sascha D., and Sean Vitka. "Crypto War II." *Critical Studies in Media Communication* 31, no. 2 (June 2014): 123–28. doi:10.1080/15295036.2014.921320.

Moore, T., A. Friedman, and A.D. Procaccia. "Would a 'Cyber Warrior' Protect Us? Exploring Trade-Offs between Attack and Defense of Information Systems," 85–94, 2010. doi:10.1145/1900546.1900559.

Motti, Vivian Genaro, and Kelly Caine. "Users' Privacy Concerns About Wearables: Impact of Form Factor, Sensors and Type of Data Collected." In *Financial Cryptography and Data Security (FC 2015)*, edited by M. Brenner, N. Christin, B. Johnson, and K. Rohloff, 8976:231–44. Berlin: Springer, 2015.

Mulligan, Deirdre K., and Fred B. Schneider. "Doctrine for Cybersecurity." *Daedalus* 140, no. 4 (FAL 2011): 70–92.

Mulvenon, J. "Toward a Cyberconflict Studies Research Agenda." *Ieee Security & Privacy* 3, no. 4 (August 2005): 52–55. doi:10.1109/MSP.2005.110.

Myhre, Sonja L., Jane Kaye, Lee A. Bygrave, Margunn Aanestad, Buthaina Ghanem, Patricia Mechael, and J. Frederik Frøen. "eRegistries: Governance for Electronic Maternal and Child Health Registries." *BMC Pregnancy and Childbirth* 16 (September 2016): 279. doi:10.1186/s12884-016-1063-0.

Nissenbaum, H. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7, no. 2 (2005): 61–73. doi:10.1007/s10676-005-4582-3.

O'Shea, P. "Cyber War from a Living Room." *Electronic Products (Garden City, New York)* 52, no. 10 (2010).

Olmsted, Murrey G., Barbara L. Massoudi, and Yuying Zhang. "What Consumers Want in Personal Health Applications: Findings from Project HealthDesign." *Personal and Ubiquitous Computing* 19, no. 1 (January 2015): 79–83. doi:10.1007/s00779-014-0811-2.

Olvingson, Christina, Jonas Hallberg, Toomas Timpka, and Kent Lindqvist. "Ethical Issues in Public Health Informatics: Implications for System Design When Sharing Geographic Information." *Journal of Biomedical Informatics* 35, no. 3 (June 2002): 178–85. doi:10.1016/S1532-0464(02)00527-0.

Organisation for Economic Co-operation and Development. "Cybersecurity Policy Making at a Turning Point." OECD Digital Economy Papers. Paris: OECD Publishing, 2012.

Ottis, R. "Proactive Defense Tactics against On-Line Cyber Militia," 233–37, 2010. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84873105908&partnerID=40&md5=0f7b0212912c9ccde5b71fc044ac2ef7.

Ozair, Fouzia F., Nayer Jamshed, Amit Sharma, and Praveen Aggarwal. "Ethical Issues in Electronic Health Records: A General Overview." *Perspectives in Clinical Research* 6, no. 2 (2015): 73–76. doi:10.4103/2229-3485.153997.

Pearson, Siani. "Privacy, Security and Trust in Cloud Computing." In *Privacy and Security for Cloud Computing*, by Siani Pearson and George Yee, 3–42. London: Springer, 2013.

Peddicord, Douglas, Ann B. Waldo, Marc Boutin, Tina Grande, and Luis Gutierrez. "A Proposal To Protect Privacy Of Health Information While Accelerating Comparative Effectiveness Research." *Health Affairs* 29, no. 11 (November 2010): 2082–90. doi:10.1377/hlthaff.2010.0635.

Peng, C., M. Xu, S. Xu, and T. Hu. "Modeling and Predicting Extreme Cyber Attack Rates via Marked Point Processes." Article in Press, 2016. Scopus. doi:10.1080/02664763.2016.1257590.

Phahlamohlaka, Jackie. "Globalisation and National Security Issues for the State: Implications for National ICT Policies." In *Social Dimensions of Information and Communication Technology Policy*, edited by C. Avgerou, M. L. Smith, and P. VandenBesselaar, 95–107. IFIP International Conference on Human Choice and Computers 282. Berlin: Springer, 2008.

Phahlamohlaka, L. J., J. C. Jansen van Vuuren, and A. J. Coetzee. "Cyber Security Awareness Toolkit for National Security: An Approach to South Africa's Cyber Security Policy Implementation," 2011. http://researchspace.csir.co.za/dspace/handle/10204/5162.

Pieters, Wolter. "Security and Privacy in the Clouds: A Bird's Eye View." In *Computers, Privacy and Data Protection: An Element of Choice*, 445–457. Springer, 2011. http://link.springer.com/chapter/10.1007/978-94-007-0641-5_21.

Piotrowski, Rafal, and Joanna Sliwa. "Cyberspace Situational Awarness in National Security System." *2015 International Conference on Military Communications and Information Systems (Icmcis)*, 2015.

Posey, Clay, Becky Bennett, Tom Roberts, and Paul Benjamin Lowry. "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," 2011. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1958530.

Prislan, Kaja, and Igor Bernik. "From Traditional Local to Global Cyberspace - Slovenian Perspectives on Information Warfare." Edited by V. Lysenko. *Proceedings of the 7th International Conference on Information Warfare and Security*, 2012, 237–44.

Qian, Li. "Study of Information System Security of Government Data Center Based on the Classified Protection." In *8th International Conference on Computer Science & Education (ICCSE), 2013*. Colombo, Sri Lanka: IEEE, 2013.

Rahim, Fiza Abdul, Zuraini Ismail, and Ganthan Narayana Samy. "Information Privacy Concerns in Electronic Healthcare Records: A Systematic Literature Review." In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)*, 504–9. New York: IEEE, 2013.

Read, O. "How the 2010 Attack on Google Changed the Us Government's Threat Perception of Economic Cyber Espionage." In *Cyberspace and International Relations: Theory, Prospects and Challenges*, 9783642374814:203–30, 2014. doi:10.1007/978-3-642-37481-4_12.

Reddy, D.S., and G. Dietrich. "Identifying Multiple Categories of Cybersecurity Skills That Affect User Acceptance of Protective Information Technologies." In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016. http://aisel.aisnet.org/amcis2016/ISSec/Presentations/37/.

Reddy, D.S., and S.V. Rao. "Cybersecurity Skills: The Moderating Role in the Relationship between Cybersecurity Awareness and Compliance." In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*, 2016. http://aisel.aisnet.org/amcis2016/ISSec/Presentations/23/.

Rifaut, Andre, Christophe Feltus, Slim Turki, and Djamel Khadraoui. "Analysis of the Impact of Ethical Issues on the Management of the Access Rights." In *Proceedings of the 8th International Conference on Security of Information and Networks*, 12–19. ACM, 2015. http://dl.acm.org/citation.cfm?id=2799996.

Rigoni, Andrea, and Salvatore Di Blasi. "A Proposal for Domain Name System (DNS) Security Metrics Framework." Edited by R. Ottis. *Proceedings of the 10th European Conference on Information Warfare and Security*, 2011, 333–36.

Robertson, Christopher J., Anna Lamin, and Grigorios Livanis. "Stakeholder Perceptions of Offshoring and Outsourcing: The Role of Embedded Issues." *Journal of Business Ethics* 95, no. 2 (August 2010): 167–89. doi:10.1007/s10551-009-0353-0.

Rock, Barry, and Elaine Congress. "The New Confidentiality for the 21st Century in a Managed Care Environment." *Social Work* 44, no. 3 (May 1999): 253–62.

Rodrigues, Paulo, and Henrique Santos. "Health Users' Perception of Biometric Authentication Technologies." Edited by Pedro P. Rodrigues, Mykola Pechenizkiy, João Gama, Ricardo C. Correia, Jiming Liu, Agma Traina, Peter Lucas, and Paolo Soda. *2013 IEEE 26th International Symposium on Computer-Based Medical Systems (CBMS)*, 2013, 320–25.

Rollins, J., and A.C. Henning. "Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations." In *Internet Policies and Issues*, 6:65–89, 2010.

Ross, David A. "Foreword". In *Public health informatics and information systems*, edited by Patrick W. O'Carroll, William A. Yasnoff, M. Elizabeth Ward, Laura H. Ripp and Ernest L. Martin, v-vi. New York: Springer, 2003. ×

Rothenpieler, Peter, Claudia Becker, and Stefan Fischer. "Privacy Concerns in a Remote Monitoring and Social Networking Platform for Assisted Living." In *Privacy and Identity Management for Life*, edited by Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, Giovanni Russello, 352 (2011): 219–30.

Saigí-Rubió, Francesc, Ana Jiménez-Zarco, and Joan Torrent-Sellens. "Determinants of the Intention to Use Telemedicine: Evidence from Primary Care Physicians." *International Journal of Technology Assessment in Health Care* 32, no. 1–2 (2016): 29–36. doi:10.1017/S0266462316000015.

Salman, Ali, Suhana Saad, and Mohd Nor Shahizan Ali. "Dealing with Ethical Issues among Internet Users: Do We Need Legal Enforcement?" *Asian Social Science* 9, no. 8 (2013): 3.

Sekgwathe, Virginiah, and Mohammad Talib. "Cyber Crime Detection and Protection: Third World Still to Cope-Up." In *E-Technologies and Networks for Development*, edited by J. J. Yonazi, E. Sedoyeka, E. Ariwa, and E. ElQawasmeh, 171:171–81, 2011.

Sevis, Kamile Nur, and Ensar Seker. "Cyber Warfare: Terms, Issues, Laws and Controversies." *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2016.

Shakib, Javad, and David Layton. "Interaction between Ethics and Technology." *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, 2014.

Shannon, J., and N. Thomas. "Human Security and Cyber-Security: Operationalising a Policy Framework." In *Cyber-Crime*, 327–46, 2005.

Shkëmbi, A., and D. Sina. "Cybercrime in the Perspective of the European Legal Framework." *Mediterranean Journal of Social Sciences* 4, no. 9 (2013): 327–31. doi:10.5901/mjss.2013.v4n9p327.

Simshaw, Drew, and Stephen S. Wu. "Ethics and Cybersecurity: Obligations to Protect Client Data." In *National Symposium on Technology in Labor and Employment Law*. San Francisco, CA, 2015.

Spafford, Eugene H. "Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense." In *Protecting Persons While Protecting the People*, edited by C. S. Gal, P. B. Kantor, and M. E. Lesk, 5661:20–33, 2009.

Spitalewsky, K., J. Rochon, M. Ganzinger, and P. Knaup. "Potential and Requirements of IT for Ambient Assisted Living Technologies: Results of a Delphi Study." *Methods of Information in Medicine* 52, no. 3 (2013): 231–38. doi:10.3414/ME12-01-0021.

Spriggs, Merle, Michael V. Arnold, Christopher M. Pearce and Craig Fry. "Ethical questions must be conserved for electronic health records." *Journal of Medical Ethics* 39, no. 9 (May 2012): 635-39. doi: 10.1136/medethics-2011-100413.

Stahl, Bernd Carsten, Neil F. Doherty, Mark Shaw, and Helge Janicke. "Critical Theory as an Approach to the Ethics of Information Security." *Science and Engineering Ethics* 20, no. 3 (September 2014): 675–99. doi:10.1007/s11948-013-9496-6.

Taddeo, Mariarosaria. "Cyber Security and Individual Rights, Striking the Right Balance." *Philosophy and Technology* 26, no. 4 (2013): 353–356. doi:10.1007/s13347-013-0140-9.

------- "The Struggle Between Liberties and Authorities in the Information Age." *Science and Engineering Ethics* 21, no. 5 (October 2015): 1125–38. doi:10.1007/s11948-014-9586-0.

Tatar, Unal, Bilge Karabacak, and Adrian Gheorghe. "An Assessment Model to Improve National Cyber Security Governance." *Proceedings of the 11th International Conference on Cyber Warfare and Security (Iccws 2016)*, 2016, 312–19.

Tatar, Unal, Orhan Calik, Minhac Celik, and Bilge Karabacak. "A Comparative Analysis of the National Cyber Security Strategies of Leading Nations." In *Proceedings of the 9th International Conference on Cyber Warfare and Security (Iccws-2014)*, edited by S. Liles, 211–18, 2014.

Tatarinova, L.F., K.N. Shakirov, and D.V. Tatarinov. "Criminological Analysis of Determinants of Cybercrime Technologies." *Mathematics Education* 11, no. 5 (2016): 1127–34.

The Academy of Medical Sciences. "Personal Data for Public Good: Using Health Information in Medical Research." London: Academy of Medical Sciences, January 2006. Accessed August 4, 2017. https://acmedsci.ac.uk/policy/policy-projects/personal-data.

Thilakanathan, Danan, Rafael A. Calvo, Shiping Chen, Surya Nepal, and Nick Glozier. "Facilitating Secure Sharing of Personal Health Data in the Cloud." *JMIR Medical Informatics* 4, no. 2 (June 2016): 56–73. doi:10.2196/medinform.4756.

Thuraisingham, B. *Dependable Computing for National Security: A Position Paper*, 2003.

---------- *Data Mining for Security Applications*. Edited by M. Kantardzic, O. Nasraoui, and M. Milanova, 2004.

Tieu, Lina, Urmimala Sarkar, Dean Schillinger, James D. Ralston, Neda Ratanawongsa, Rena Pasick, and Courtney R. Lyles. "Barriers and Facilitators to Online Portal Use Among Patients and Caregivers in a Safety Net Health Care System: A Qualitative Study." *Journal of Medical Internet Research* 17, no. 12 (December 2015): e275. doi:10.2196/jmir.4847.

U. K. Biobank. "UK Biobank Ethics and Governance Framework: Version 3.0." 2007. Accessed August 4, 2017. https://www.ukbiobank.ac.uk/wp-content/uploads/2011/05/EGF20082.pdf.

Van Allen, Jason, and Michael C. Roberts. "Critical Incidents in the Marriage of Psychology and Technology: A Discussion of Potential Ethical Issues in Practice, Education, and Policy." *Professional Psychology-Research and Practice* 42, no. 6 (December 2011): 433–39. doi:10.1037/a0025278.

Van der Linden, Helma, Dipak Kalra, Arie Hasman, and Jan Talmon. "Inter-Organizational Future Proof EHR Systems: A Review of the Security and Privacy Related Issues." *International Journal of Medical Informatics* 78, no. 3 (March 2009): 141–60. doi:10.1016/j.ijmedinf.2008.06.013.

van Vuuren, Joey Jansen, Jackie Phahlamohlaka, and Louise Leenen. "Governance of CyberSecurity in South Africa." Edited by E. Filiol and R. Erra. *Proceedings of the 11th European Conference on Information Warfare and Security*, 2012, 135–44.

van Vuuren, Joey Jansen, Jackie Phahlamohlaka, and Mario Brazzoli. "The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen." Edited by E. L. Armistead. *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, 171–81.

van Vuuren, Joey Jansen, Louise Leenen, Jackie Phahlamohlaka, and Jannie Zaaiman. "Development of a South African Cybersecurity Policy Implementation Framework." Edited by D. Hart. *Proceedings of the 8th International Conference on Information Warfare and Security (Iciw-2013)*, 2013, 106–15.

van Vuuren, Joey Jansen, L. Leenen, J. Phahlamohlaka, and J. Zaaiman. "An Approach to Governance of Cybersecurity in South Africa." In *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*, 3–4:1583–97, 2014. doi:10.4018/978-1-4666-5942-1.ch082.

van Vuuren, Joey Jansen, Marthie Grobler, and Jannie Zaaiman. "Cyber Security Awareness as Critical Driver to National Security." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 2, no. 1 (2012): 27–38.

-------- "The Influence of Cyber Security Levels of South African Citizens on National Security." Edited by V. Lysenko. *Proceedings of the 7th International Conference on Information Warfare and Security*, 2012, 138–47.

van Vuuren, Joey Jansen, Marthie Grobler, Louise Leenen, and Jackie Phahlamohlaka. "Proposed Model for a Cybersecurity Centre of Innovation for South Africa." In *Ict and Society*, edited by K. Kimppa, D. Whitehouse, T. Kuusela, and J. Phahlamohlaka, 431:293–306, 2014.

Vayena, Effy, Urs Gasser, Alexandra Wood, David O'Brien, Micah Altman: "Elements of a New Ethical Framework for Big Data Research." Washington and Lee Law Review Online 72, Issue 3 (March 2016): 420-441.

Venkatraman, Sitalakshmi, and Indika Delpachitra. "Biometrics in Banking Security: A Case Study." *Information Management & Computer Security* 16, no. 4 (2008): 415–430.

Verheul, E., B.-J. Koops, and H. Van Tilborg. "Binding Cryptography - A Fraud-Detectible Alternative to Key-Escrow Proposals." *Computer Law and Security Report* 13, no. 1 (1997): 3–14. doi:10.1016/S0267-3649(97)81186-7.

Visvanathan, Akila, Alan P. Gibb, and Richard R. W. Brady. "Increasing Clinical Presence of Mobile Communication Technology: Avoiding the Pitfalls." *Telemedicine and E-Health* 17, no. 8 (October 2011): 656–61. doi:10.1089/tmj.2011.0018.

Wallace, Ilse M. "Is Patient Confidentiality Compromised With the Electronic Health Record? A Position Paper." *CIN: Computers, Informatics, Nursing* 33, no. 2 (February 2015): 58–62. doi:10.1097/CIN.0000000000000126.

Walters, Gregory J. "Privacy and Security: An Ethical Analysis." *SIGCAS Comput. Soc.* 31, no. 2 (June 2001): 8–23. doi:10.1145/503345.503347.

Wang, Jin, Zhongqi Zhang, Kaijie Xu, Yue Yin, and Ping Guo. "A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System." *International Journal of Security and Its Applications* 7, no. 4 (2013): 287–98.

Warren, Matthew, and Shona Leitch. "Australian National Critical Infrastructure Protection: A Case Study." Edited by R. Ottis. *Proceedings of the 10th European Conference on Information Warfare and Security*, 2011, 275–80.

White, G.B., and D.J. DiCenso. "Information Sharing Needs for National Security." In *Proceedings of the Annual Hawaii International Conference on System Sciences*. Big Island, HI, USA, USA: IEEE, 2005. http://ieeexplore.ieee.org/document/1385491/.

Williams, Patricia A. H. "In a 'Trusting' Environment, Everyone Is Responsible for Information Security." *Information Security Technical Report* 13, no. 4 (2008): 207–15. doi:10.1016/j.istr.2008.10.009.

Wilson, Clay, "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." *Focus on Terrorism* 9 (2003): 1–42.

-------- "Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues." In *Electronic Warfare*, 161–80. New York: Nova Science Publishers, 2010

-------- "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." Report for Congress. Washington, D.C.: Congressional Research Service, 2005

--------- "Cyber Threats to Critical Information Infrastructure." In *Cyberterrorism: Understanding, Assessment, and Response*, 123–36. Berlin/Heidelberg: Springer, 2014. doi:10.1007/978-1-4939-0962-9_7.

Wjst, Matthias. "Caught You: Threats to Confidentiality Due to the Public Release of Large-Scale Genetic Data Sets." *BMC Medical Ethics* 11 (December 2010): 21. doi:10.1186/1472-6939-11-21.

World Medical Association. "Declaration of Helsinki: Ethical Principles for Medical Research Involving Human Subjects." *Journal of the American Medical Association* 310, no. 20 (November 2013): 2191–94. doi:10.1001/jama.2013.281053.

Wright, Galen E. B., Pieter G. J. Koornhof, Adebowale A. Adeyemo, and Nicki Tiffin. "Ethical and Legal Implications of Whole Genome and Whole Exome Sequencing in African Populations." *BMC Medical Ethics* 14 (May 2013): 21. doi:10.1186/1472-6939-14-21.

Wynia, Matthew K., Steven S. Coughlin, Sheri Alpert, Deborah S. Cummins, and Linda L. Emanuel. "Shared Expectations for Protection of Identifiable Health Care Information: Report of a

National Consensus Process." *Journal of General Internal Medicine* 16, no. 2 (February 2001): 100–111. doi:10.1046/j.1525-1497.2001.00515.x.

Xiao, Liang, Paul Lewis, and Alex Gibb. *Developing a Security Protocol for a Distributed Decision Support System in a Healthcare Environment*. New York: ACM, 2008.

Yang, Bian. "What Make You Sure That Health Informatics Is Secure." In *Inclusive Smart Cities and Digital Health*, edited by C. K. Chang, L. Chiari, Y. Cao, H. Jin, M. Mokhtari, and H. Aloulou, 9677:443–48. Cham: Springer, 2016.

Young-do, Kim, Kim Jin-sung, and Lee Kyung-ho. "Major Issues of the National Cyber Security System in South Korea, and Its Future Direction." *Korean Journal of Defense Analysis* 25, no. 4 (2013): 435–55.

Young, Rachel, Erin Willis, Glen Cameron, and Mugur Geana. "'Willing but Unwilling': Attitudinal Barriers to Adoption of Home- Based Health Information Technology among Older Adults." *Health Informatics Journal* 20, no. 2 (June 2014): 127–35. doi:10.1177/1460458213486906.

Zheng, A.-K., P. Song, B.-X. Han, and M.-J. Zheng. *Reflection of the Nation Cybersecurity's Evolution*. Vol. 347–350. Applied Mechanics and Materials, 2013. doi:10.4028/www.scientific.net/AMM.347-350.2553.