Veale, Michael; Brown, Ian

Article

Cybersecurity

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Veale, Michael; Brown, Ian (2020) : Cybersecurity, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 4, pp. 1-22, https://doi.org/10.14763/2020.4.1533

This Version is available at:
https://hdl.handle.net/10419/233106

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

CONCEPT

OPEN ACCESS

PEER REVIEWED

Cybersecurity

Michael Veale *University College London* m.veale@ucl.ac.uk
Ian Brown *Fundação Getulio Vargas*

DOI: https://doi.org/10.14763/2020.4.1533

Published: 17 December 2020
Received: 16 September 2020 **Accepted:** 6 November 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Veale, M. & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1533

Keywords: Cyber, Governance, Hacking, Securitisation, Surveillance

Abstract: Cybersecurity covers the broad range of technical and social issues that must be considered to protect networked information systems. The importance of the concept has increased as so many government, business, and day-to-day activities globally have moved online. It has been increasingly referred to in both academic and mainstream publications since 2003, in fields including software engineering, international relations, crisis management and public safety, slowly overtaking more technical terms such as computer/system/data security (popular in the 1970s/1980s) and information security (popular from the mid 1990s). But its strong association with national security and defence agencies, and disconnection from social science notions such as place, have led to concerns of inappropriate cyber securitisation of government programmes.

This article belongs to **Concepts of the digital society**, a special section of *Internet Policy Review* guest-edited by Christian Katzenbach and Thomas Christian Bächle.

Introduction

Cybersecurity [1] covers the broad range of technical, organisational and governance issues that must be considered to protect networked information systems against accidental and deliberate threats. It goes well beyond the details of encryption, firewalls, anti-virus software, and similar technical security tools. This breadth is captured in the widely used International Telecommunication Union (ITU) definition (ITU-T, 2008, p. 2):

> Cybersecurity is 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 and 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 importance of cybersecurity has increased as so many government, business, and day-to-day activities around the world have moved online. But especially in emerging economies, "[m]any organizations digitizing their activities lack organizational, technological and human resources, and other fundamental ingredients needed to secure their system, which is the key for the long-term success" (Kshetri, 2016, p. 3).

The more technically-focused *information security* is still in widespread use in computer science. But as these issues have become of much greater societal concern as "software is eating the world" (Andreessen, 2011), cybersecurity has become more frequently used, not only in the rhetorics of democratic governments as in the 2000s, but also in general academic literature (shown in Figure 1):

1. The authors use cybersecurity, not cyber security, throughout this text, as it is the one most in use in computer science, even in Britain.

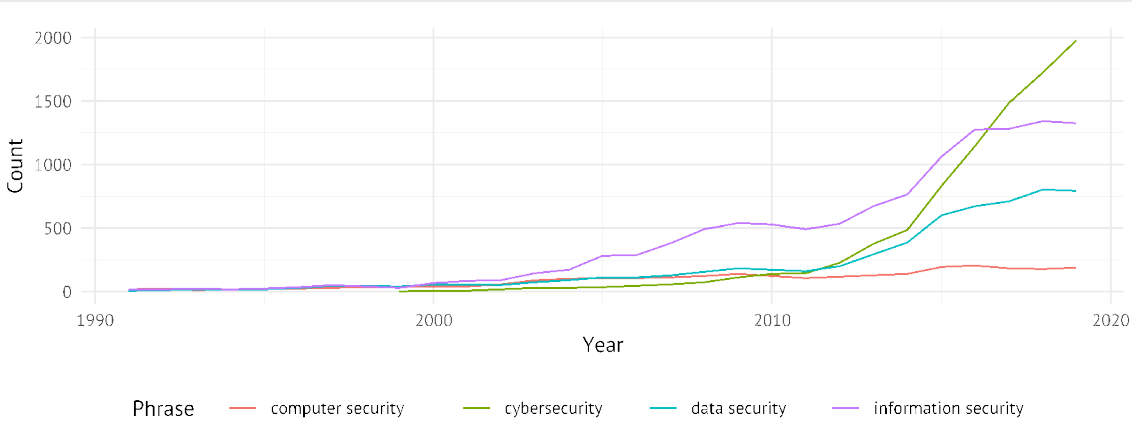

FIGURE 1: Academic articles with *cybersecurity/cyber-security/cyber security* versus *information security*, *data security* and *computer security* in title, keywords or abstract of Web of Science indexed publications over time. Small numbers of records exist for both *information security* and *computer security* in the database since 1969. Data from Web of Science.

Barely used in academic literature before 1990 (except in relation to the Cray CYBER 205 supercomputer from the late 1970s), *cyber* became ubiquitous as a prefix, adjective and even noun by the mid-1990s, with Google Scholar returning results across a broad range of disciplines with titles such as 'Love, sex, & power on the cyber frontier' (1995), 'Surfing in Seattle: What cyber-patrons want' (1995), 'The cyber-road not taken' (1994) and even the 'Cyber Dada Manifesto" (1991).

It evolved from Wiener's *cybernetics*, a "field of control and communication theory, whether in machine or in the animal" (1948)—derived from the Greek word for 'steersman'—with an important intermediate point being the popular usage of *cyborg*, a contraction of cybernetic organism, alongside the Czech-derived *robot* (Clarke, 2005, section 2.4). The notion of a 'governor' of a machine goes back to the mid-19th century, with J. C. Maxwell (discoverer of the electron) noting in 1868 it is "a part of a machine by means of which the velocity of the machine is kept nearly uniform, notwithstanding variations in the driving-power or the resistance" (Maxwell, 1868, p. 270)—what Wiener called *homeostasis*.

The use of *cyberspace* to refer to the electronic communications environment was coined in William Gibson's 1982 short story *Burning Chrome* ("widespread, interconnected digital technology") and popularised by his 1984 science fiction novel *Neuromancer* ("a graphic representation of data abstracted from the banks of every computer in the human system [...] lines of light ranged in the nonspace of mind, clusters and constellations of data [...] a consensual hallucination experienced by millions"). Cyberspace's arrival in legal and policy discussions was spearheaded by John Perry Barlow's *Declaration of the Independence of Cyberspace* (1996). But by

2000, Gibson declared cyberspace was "evocative and essentially meaningless … suggestive … but with no real meaning" (Neale, 2000).

Despite its ubiquity in present-day national security and defence-related discussions, Wagner and Vieth found: "Cyber and cyberspace, however, are not synonymous words and have developed different meanings […] Cyber is increasingly becoming a metaphor for threat scenarios and the necessary militarisation" (2016). Matwyshyn suggested the term is "the consequence of a cultural divide between the two [US] coasts: 'cybersecurity' is the Washington, D.C. legal rebranding for what Silicon Valley veterans have historically usually called 'infosec' or simply 'security'" (2017, p. 1158). Cybersecurity issues have, to many whose interests are served by the interpretation, become *national security* issues (Clarke, 2016; Kemmerer, 2003; Nissenbaum, 2005).

A review by Craigen et al. (2014) found *cybersecurity* used in a range of literature and fields from 2003 onwards, including software engineering, international relations, crisis management and public safety. Social scientists interacting with policymakers, and academics generally applying for research and translation funding from government sources and interacting with the defence and signals intelligence/information security agencies that are the cybersecurity centres of expertise in many larger governments, have further popularised the term, [2] which appears in similar form in many languages, as shown in Appendix 1.

Looking beyond academia to literature more widely, Figure 2 shows computer security was most prevalent in the Google Books corpus from 1974, overtaken by information security in 1997, and cybersecurity in 2015 (with cyber security increasingly popular since 1996, but cyber-security negligible the entire period). *Computer* (Ware, 1970), *system*, and *data* (Denning, 1982) *security* were all frequently used as closely-related terms in the 1970s (Saltzer & Schroeder, 1975). [3]

2. The second author must admit he has not been immune to this.

3. Ware's 1970 report begins: "Although this report contains no information not available in a well stocked technical library or not known to computer experts, and although there is little or nothing in it directly attributable to classified sources…"

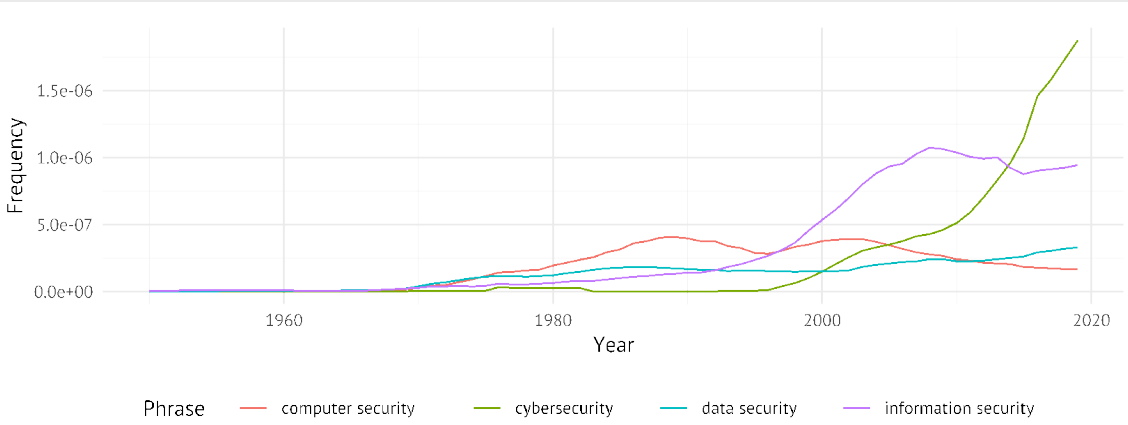

FIGURE 2: Google n-gram analysis (Lin et al., 2012) of the usage of variants of *information security* over time. Cybersecurity encompasses *cybersecurity*, *cyber security* and *cyber-security*. Retrieved using *ngramr* (Carmody, 2020).

This trend is unfortunate, since "using the term 'cybersecurity' seems to imply that information security issues are limited to code connected to the Internet [but] physical security of machines and human manipulability through social engineering are always key aspects of information security in both the private and public sector" (Matwyshyn, 2017, p. 1156).

Cybersecurity in early context

In computer science, attacks on the security of information systems are usually concerned with:

- Breaching the **confidentiality** of systems, with data exposed to unauthorised actors;
- Undermining the **integrity** of systems, and disruption of the accuracy, consistency or trustworthiness of information being processed;
- Affecting the **availability** of systems, and rendering them offline, unusable or non-functional.

Together, confidentiality, integrity and availability are called the CIA triad, and have been the basis of information security since the late 1970s (Neumann et al., 1977, pp. 11–14). Echoing this history decades later, the Council of Europe's 2001 Budapest Convention on Cybercrime set out in its first substantive section "Offences against the confidentiality, integrity and availability of computer data and systems".

Cybersecurity across disciplines

The study and practice of cybersecurity spans a range of disciplines and fields. In this article, we consider three of the main angles important to cybersecurity practice: technical aspects; human factors; and legal dimensions. This is necessarily an incomplete list—notably, the topic is also the subject of study by those who are interested in, for example, how it reconfigures organisational structures (information systems), or relationships between actors such as states (international relations), and significant non-state actors such as organised crime gangs (criminology).

Technical aspects

Many technical domains are of direct relevance to cybersecurity, but the field designed to synthesise technical knowledge in practical contexts has become known as *security engineering*: "building systems to remain dependable in the face of malice, error, or mischance" (Anderson, 2008, p. 3). It concerns the confluence of four aspects—*policy* (the security aim), *mechanisms* (technologies to implement the policy), *assurance* (the reliability of each mechanism) and *incentives* (of both attackers and defenders). Security engineers may be intellectually grounded in a specialised technical domain, but they require a range of bridging and boundary skills between other disciplines of research and practice.

A daunting (and worsening) challenge for security engineers is posed by the complexities of the sociotechnical environments in which they operate. Technological systems have always evolved and displayed interdependencies, but today infrastructures and individual devices are networked and co-dependent in ways which challenge any ability to unilaterally "engineer" a situation. Systems are increasingly *servitised*, (e.g., through external APIs) with information flows not under the control of the system engineer, and code subject to constant 'agile' evolution and change which may undermine desired system properties (Kostova et al., 2020).

Human factors and social sciences

The field of human factors in cybersecurity grew from the observation that much of the time "hackers pay more attention to the human link in the security chain than security designers" (Adams & Sasse, 1999, p. 41), leaving many sensitive systems wide open to penetration by "social engineering" (Mitnick & Simon, 2002).

It is now very problematic to draw cybersecurity's conceptual boundaries around an organisation's IT department, software vendors and employer-managed hardware, as in practice networked technologies have permeated and reconfigured so-

cial interactions in all aspects of life. Users often adapt technologies in unexpected ways (Silverstone & Hirsch, 1992) and create their own new networked spaces (Cohen, 2012; Zittrain, 2006), reliant on often-incomprehensible security tools (Whitten & Tygar, 1999) that merely obstruct individuals in carrying out their intended tasks (Sasse et al., 2001). Networked spaces to be secured—the office, the university, the city, the electoral system—cannot be boxed-off and separated from technology in society more broadly. Communities often run their networked services, such as a website, messaging group, or social media pages, without dedicated cybersecurity support. Even in companies, or governments, individuals or groups with cybersecurity functions differ widely in location, autonomy, capabilities, and authority. The complexity of securing such a global assemblage, made up of billions of users as well as hundreds of millions of connected devices, has encouraged a wider cross-disciplinary focus on improving the security of these planetary-scale systems, with social sciences as an important component (Chang, 2012).

Research focussed on the interaction between cybersecurity and society has also expanded the relevant set of risks and actors involved. While the term cybersecurity is often used interchangeably with information security (and thus in terms of the CIA triad), this only represents a subset of cybersecurity risks.

Insofar as all security concerns the protection of certain assets from threats posed by attackers exploiting vulnerabilities, the assets at stake in a digital context need not just be information, but could, for example, be people (through cyberbullying, manipulation or intimate partner abuse) or critical infrastructures (von Solms & van Niekerk, 2013). Moreover, traditional threat models in both information and cybersecurity can be limited. For example, domestic abusers are rarely considered as a threat actor (Levy & Schneier, 2020) and systems are rarely designed to protect their intended users from the authenticated but adversarial users typical in intimate partner abuse (Freed et al., 2018).

The domain of cyber-physical security further captures the way in which cybersecurity threats interact with physically located sensors and actuators. A broader flavour of definition than has been previously typical is used in the recent EU Cybersecurity Act (Regulation 2019/881), which in Article 2(1) defines cybersecurity as “the activities necessary to protect network and information systems, *the users of such systems, and other persons* affected by cyber threats” [emphasis added]. The difficult interaction between information systems, societies and environments is rapidly gaining traction in the research literature.

Research at the intersection of human–computer interaction and cybersecurity has also pointed to challenges of usability and acceptability in deploying approaches developed in fields such as security engineering. Consider the encryption of information flowing across the internet using Transport Layer Security (TLS), a protocol which is able to cryptographically authenticate the endpoints and protect the confidentiality and integrity of transmitted data. TLS raises usability challenges in relation to developers' and administrators' understanding of how it works and thus how to correctly implement it (Krombholz et al., 2017, 2019) as well as challenges with communicating its properties—and what to do in its absence—to end users in their web browsers (Felt et al., 2015; Reeder et al., 2018). Focusing on the user experience of the web browser, Camp (2013) suggests principles of *translucent security*: high security defaults, single-click override, context-specific settings, personalised settings, and use-based settings.

Related challenges faced by both users and developers or other specialists are found widely across the cybersecurity field, including passwords (e.g., Naiakshina et al., 2019) and encrypted email (Whitten & Tygar, 1999). The field of *usable security* seeks a fit between the security task and the humans expected to interact with it (Sasse et al., 2001). Without an understanding of issues such as these, the techniques used can bring at best a false sense of security, and at worst, entirely new threat vectors.

Legal dimensions

While few laws explicitly state they are governing cybersecurity, cybersecurity–related provisions are found in an extremely wide array of instruments. Law might incentivise or require certain cybersecurity practices or standards; apply civil or criminal sanctions, or apportion liability, for persons experiencing or taking action which leads to cybersecurity breaches; mandate practices (such as information sharing or interoperability) that themselves have cybersecurity implications; or create public advisory or enforcement bodies with cybersecurity responsibilities.

Data protection and privacy laws generally contain varied provisions with cybersecurity implications. They are, at the time of writing, present in 142 countries around the world (Greenleaf & Cottier, 2020) as well as promoted by the Council of Europe's Convention 108+ and model laws from several international organisations, such as the Commonwealth (Brown et al., 2020). They often, although not always, span both the public and private sectors, with common stipulations including the creation of an independent supervisory authority; overarching obligations to secure 'personal' data or information, often defined by reference to its potential

identifiability; data breach notification requirements; obligations to *design in* enforcement of data protection principles and appoint a data protection officer; and rights that can be triggered by individuals to access, manage and if they wish, erase identifiable data that relates to them.

Other specific laws also contain cybersecurity breach notification (to users and/or regulators) and incident requirements scoped beyond personal data, such as the European eIDAS Regulation (Regulation 910/2014, concerning identity and trust providers) and Network and Information Security Directive (Directive 2016/1148, concerning essential infrastructure, including national infrastructure such as electricity and water as well as 'relevant digital service providers', meaning search engines, online marketplaces and cloud computing). While lacking an omnibus federal data protection law, all 50 US states have some form of data breach law, although their precise requirements vary (Kosseff, 2020, Appendix B).

In the EU, the law that would seem the most likely candidate for a horizontal regime is the 2019 Cybersecurity Act (Regulation 2019/881).It however provides little of real substantive interest, mainly increasing the coordination and advisory mandates of ENISA, the EU's cybersecurity agency, and laying the foundation for a state-supported but voluntary certification scheme.

A grab-bag of highly specific cybersecurity laws also exists, such as the California Internet of Things Cybersecurity Law, aimed mostly at forbidding devices from using generic passwords (Cal. Civ. Code § 1798.91.04). These reactive, ad-hoc instruments are often not technologically neutral: they may have clarity and legal certainty in the current situation, but may not be sustainable as technologies change, for example, away from passwords (Koops, 2006). On the other hand, generic laws have also, over time, morphed into cybersecurity laws. The Federal Trade Commission in the US penalises companies for exceptionally poor data security practices under the prohibition of "unfair or deceptive practices" in the FTC Act (15 U.S.C. § 45).

There are, however, limits to the ability of generic laws to morph into cybersecurity laws. Computer misuse laws emerged in legal regimes in part due to the limitations of existing frameworks in capturing digital crime. Before the mid-1980s, the main avenue to prosecuting computer misuse in the US was theft (Kerr, 2003), a rationale which proved strained and unpredictable. The UK saw unsuccessful attempts to repurpose the law of forgery against unauthorised password use (*R v Gold* [1988] AC 1063), leading to the passing of the Computer Misuse Act 1990.

The US has struggled with the concept of 'unauthorised' access in its law. Offences in the Computer Fraud and Abuse Act (CFAA) of 1984 typically occur when individuals enter systems without authorisation, or where they exceed authorised access, mimicking laws of trespass (Kerr, 2016). But the notion of authorisation in digital systems quickly becomes tricky. If a website is designed such that sensitive information is discoverable by typing in a long URL (a problematic "security through obscurity" approach), without any authentication mechanism, is there implicit authorisation? Is an address bar more like a password box—guessing someone else's being telling about your motive to access unauthorised material; or a telephone keypad or map—and the user is simply exploring?

The CFAA has also created tensions based on its interaction with a site's terms of service (ToS). This tension centres on whether authorisation is revoked based on statements in these long, legalistic documents that only few read. For example, such documents often preclude web scraping in broad, vague language (Fiesler et al., 2020), and despite over sixty legal opinions over the last two decades, the legal status of scraping remains "characterized as something just shy of unknowable, or a matter entirely left to the whims of courts" (Sellars, 2018, p. 377). This becomes highly problematic for firms, researchers or journalists, as computer misuse law may effectively turn potential civil liability for breach of contract into criminal liability under the CFAA.

As a consequence, scholars such as Orin Kerr have argued that only the bypassing of authentication requirements, such as stealing credentials, or spoofing a log-in cookie, should be seen as creating a lack of authorisation under CFAA (Kerr, 2016). This contrasts with messy existing case law, which includes prosecution on the basis that an IP address was changed (as it often does by design) to avoid a simple numeric IP block. Contingent and subjective social aspects of cybersecurity law will remain, both in computer misuse and in other areas, even if this argument was accepted.

Legal instruments around cybercrime and cybersecurity more generally continue to develop—the Council of Europe's Budapest Convention on Cybercrime was concluded in 2001, seeking to harmonise cybercrime legislation and facilitate international cooperation, and drawing on experiences and challenges of earlier cybersecurity and cybercrime law. It has been ratified/acceded to by 65 countries including the US, which has only ever ratified three Council of Europe treaties. However, the further development of legal certainty in areas of cybersecurity will require yet clearer shared norms of how computing systems, and in particular, the internet, should be used.

Cybersecurity's broader impact

Here, we select and outline just two broader impacts of cybersecurity—its link to security-thinking in other domains of computing and society, and its effect on institutional structures.

(Cyber)securitisation

While *computer security* narrowly focussed on the CIA triad, the *cybersecurity* concept expanded towards both national security and the use of computers for societally harmful activities (e.g., hatred and incitement to violence; terrorism; child sexual abuse) and attacks on critical infrastructures, including the internet itself (Nissenbaum, 2005). The privileged role of technical experts and discourse inside computer security has given technical blessing to this trend of securitisation (Hansen & Nissenbaum, 2009, p. 1167).

Security is not new to technification, as 'Cold War rationality' showed (Erickson et al., 2013). Yet not only have technical approaches arguably been able to take a more privileged position in cybersecurity than any other security sector (Hansen & Nissenbaum, 2009, p. 1168), their success in raising salience through securitisation has resonated widely across computing issues.

For example, privacy engineering has a dominant strand focussing on quantitative approaches to confidentiality, such as minimising theoretical *information leakage* (Gürses, 2014); while algorithmic fairness and anti-discrimination engineering has also emerged as a similar (and controversial) industry-favoured approach to issues of injustice (Friedler et al., 2019; see Gangadharan & Niklas, 2019). Gürses connects the engineering of security, privacy, dependability and usability—an ideal she claims "misleadingly suggests we can engineer social and legal concepts" (Gürses, 2014, p. 23).

These echoes may have their origins in the very human dimensions of these fast-changing areas, as organisations seek to apply or redeploy employees with security skill sets shaped by strong professional pressures to these recently salient problems (DiMaggio & Powell, 1983), as well as the hype-laden discourse of cybersecurity identified as fuelling a range of problems in the field (Lee & Rid, 2014). While these areas may not yet be able to be considered *securitised*, insofar as neither privacy nor discrimination is commonly politically positioned as an existential threat to an incumbent political community (Buzan et al., 1998; Cavelty, 2020; see Hansen & Nissenbaum, 2009), neither can they be said to be unaffected by the way cybersecurity and national security, and the forms of computing knowledge

and practice considered legitimate in those domains, have co-developed over recent decades.

Institutions

Requirements of cybersecurity knowledge and practice have led states to create new institutions to meet perceived needs for expertise. The location of this capacity differs. In some countries, there may be significant public sector capacity and in-house experts. Universities may have relevant training pipelines and world-leading research groups. In others, cybersecurity might not be a generic national specialism. In these cases, cybersecurity expertise might lie in sector-specific organisations, such as telecommunications or financial services companies, which may or may not be in public hands.

Some governments have set up high-level organisations to co-ordinate cybersecurity capacity-building and assurance in public functions, such as the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the National Cyber Security Centre (UK and Ghana—soon to become an Authority) and the Cyber Security Agency (Singapore). A new Cybersecurity Competence Centre for the EU is set to be based in Bucharest. Relatedly, and sometimes independently or separately, countries often have cybersecurity strategy groups sitting under the executive (Brown et al., 2020).

Cybersecurity agencies can find themselves providing more general expertise than simply security. During the COVID-19 pandemic, for example, the first version of the UK's National Health Service (NHS) contact tracing app for use in England had considerable broad technical input from the government's signals intelligence agency GCHQ and its subsidiary body the National Cyber Security Centre, which was considered a data controller under UK data protection law (Levy, 2020). Relatedly, these agencies have also been called upon to give advice in various regimes to political parties who are not currently in power—a relationship that would be challenging in countries where peaceful transitions of power cannot be easily taken for granted, particularly given many of these institutions' close links with national security agencies which may have politically-motivated intelligence operations (Brown et al., 2020).

National Computer Security Incident Response Teams (CSIRTs) are a relatively recent form of institution, which act as a coordinator and a point of contact for domestic and international stakeholders during an incident. Some of these have been established from scratch, while others have been elevated from existing areas of

cybersecurity capacity within their countries (Maurer et al., 2015). These expert communities, trusted clearing houses of security information, are found in many countries, sectors and networks, with 109 national CSIRTs worldwide as of March 2019 (International Telecommunication Union, 2019).

CSIRTs can play important international roles, although as they are infrequently enshrined in or required by law, they often occupy a somewhat unusual quasi-diplomatic status (Tanczer et al., 2018). Under the EU's Network and Information Security Directive however, all 27 member states must designate a national CSIRT, with ENISA playing a coordinating role under the NIS Directive.

Some researchers have expressed a more sceptical view of CSIRTs, with Roger Clarke telling the authors: "Regrettably, in contemporary Australia, at least, the concept has been co-opted and subverted into a spook sub-agency seeking ever more power to intrude into the architecture and infrastructure of telecommunications companies, and whatever other 'critical infrastructure' organisations take their fancy. Would you like a real-time feed of the number-plates going under toll-road gantries? Easily done!" (personal communication, September 2020).

Conclusion

Understanding cybersecurity is a moving target, just like understanding computing and society. Exactly what is being threatened, how, and by whom are all in flux.

While many may still look on with despair at the insecurities in modern systems, few computing concepts excite politicians more. It is hardly surprising to see the language of security permeate other computing policy concepts as a frame. Politicians talk of keeping the internet *safe*; dealing with privacy *breaches*, and defending democracies against information *warfare*. This makes cybersecurity an important concept for scholars to study and understand, and its legal and institutional adventures instructive for the development of neighbouring domains (although perhaps not always as the best template to follow). Its tools and methodological approach are also a useful training ground for interdisciplinary scholars to gain the skills required to connect and work across social, legal and technical domains.

In a 2014 review, three Canadian Communications Security Establishment science and learning advisers (Craigen et al., 2014) concluded cybersecurity is "used broadly and its definitions are highly variable, context-bound, often subjective, and, at times, uninformative". In 2017, Matwyshyn noted "'cyberized' information security legal discourse makes the incommensurability problems of security worse. It exac-

erbates communication difficulty and social distance between the language of technical information security experts on the one hand, and legislators, policymakers and legal practitioners on the other" (Matwyshyn, 2017, p. 1150).

It is not clear the situation has since improved in this regard. Cybersecurity has become a catch-all term, attached to the prevention of a very wide range of societal harms seen to be related to computing and communications tools now omnipresent in advanced economies, and increasingly prevalent in emerging economies. There are concerns this has led to a *militarisation* (Wagner & Vieth, 2016) or *securitisation* of the concept and hence measures taken by states as a result. (The UK Ministry of Defence trumpeted the launch of its "first cyber regiment" in 2020.) And the large-scale monitoring capabilities of many cybersecurity tools have led to serious concerns about their impact on human rights (Korff, 2019).

Meanwhile, many computer and social scientists publicly mock [4] the notion of *cyber* and *cyberspace* as a separate domain of human action (Graham, 2013). Rid (2016, chapter 9) noted even Wiener "would have disdained the idea and the jargon. The entire notion of a separate space, of cordoning off the virtual from the real, is getting a basic tenet of cybernetics wrong: the idea that information is part of reality, that input affects output and output affects input, that the line between system and environment is arbitrary". Matwyshyn concluded "[s]ecurity experts fear that in lieu of rigorously addressing the formidable security challenges our nation faces, our legal and policy discussions have instead devolved into a self-referential, technically inaccurate, and destructively amorphous "cyber-speak," a legalistic mutant called "cybersecurity"" (p. 1154).

We have described now that notions relating to the protection of information systems—and all the societal functions those systems now support—are increasingly significant in both academic literature and the broader public and policy discourse. The development of the "Internet of Things" will add billions of new devices over time to the internet, many with the potential to cause physical harm, which will further strengthen the need for security engineering for this overall system (Anderson, 2018).

There appears little likelihood of any clear distinctions developing at this late stage between information security and cybersecurity in practice. It may be that the former simply falls out of common usage in time, as computer security slowly

4. See the Twitter hashtag #cybercyber and @cybercyber account, and Google search results for "cyber cyber cyber", for hundreds of thousands of further examples, and the "cyber song" and video Unsere Cyber Cyber Regierung - Jung & Naiv: Ultra Edition.

has since 2010—although those with security capabilities (a.k.a. state *hacking*) still stick resolutely with *cyber*.

Anderson suggests the continued integration of software into safety-critical systems will require a much greater emphasis on safety engineering, and protection of the security properties of systems like medical devices (even body implants) and automotive vehicles for decades—in turn further strengthening political interest in the subject (2021, p. 2).

Martyn Thomas, a well-known expert in safety-critical system engineering, told us (personal communication, September 2020):

> Rather than attackers increasingly finding new ways to attack systems, the greater threat is that developers increasingly release software that contains well-known vulnerabilities – either by incorporating COTS (commercial off-the-shelf) components and libraries with known errors, or because they use development practices that are well known to be unsafe (weakly typed languages, failure to check and sanitise input data, etc.). So, the volume of insecure software grows, and the pollution of cyberspace seems unstoppable.

Powerful states (particularly the US) have since at least the 1970s used their influence over the design and production of computing systems to introduce deliberate weaknesses in security-critical elements such as encryption protocols and libraries (Diffie & Landau, 2010), and even hardware (Snowden, 2019). The US CIA and NSA Special Collection Service "routinely intercepts equipment such as routers being exported from the USA, adds surveillance implants, repackages them with factory seals and sends them onward to customers" (Anderson, 2020, p. 40). It would be surprising if other states did not carry out similar activities.

In the long run, as with most technologies, we will surely take the *cyber* element of everyday life for granted, and simply focus on the safety and security (including reliability) of devices and systems that will become ever more critical to our health, economies, and societies.

ACKNOWLEDGEMENTS

The authors thank Roger Clarke, Alan Cox, Graham Greenleaf, Douwe Korff, Chris Marsden, Martyn Thomas and Ben Wagner for their helpful feedback, and all the native speakers who shared their linguistic knowledge.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd ed.). Wiley.

Anderson, R. (2018). Making Security Sustainable. *Communications of the ACM*, *61*(3), 24–26. https://doi.org/10.1145/3180485

Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.

Andreessen, M. (2011, August 20). Why Software Is Eating The World. *The Wall Street Journal*. https://www.wsj.com/articles/SB10001424053111903480904576512250915629460

Baran, P. (1960). *Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes* (P-1995 Paper). The RAND Corporation. https://www.rand.org/pubs/papers/P1995.html

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. https://www.eff.org/cyberspace-independence

Bell, D. E., & LaPadula, L. J. (1973). *Secure Computer Systems: Mathematical Foundations* (Technical Report No. 2547; Issue 2547). MITRE Corporation.

Biba, K. J. (1975). *Integrity Considerations for Secure Computer Systems* (Technical Report MTR-3153). MITRE Corporation.

Brown, I., Marsden, C. T., Lee, J., & Veale, M. (2020). *Cybersecurity for elections: A Commonwealth guide on best practice*. Commonwealth Secretatiat. https://doi.org/10.31228/osf.io/tsdfb

Buzan, B., Wæver, O., & De Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner Publishers.

Camp, P. L. J. (2013). *Beyond usability: Security Interactions as Risk Perceptions* [Position paper]. https://core.ac.uk/display/23535917

Carmody, S. (2020). *ngramr: Retrieve and Plot Google n-Gram Data* (1.7.2) [Computer software]. https://CRAN.R-project.org/package=ngramr

Cavelty, M. D. (2020). Cybersecurity between hypersecuritization and technological routine. In E. Tikk & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (1st ed., pp. 11–21). Routledge. https://doi.org/10.4324/9781351038904-3

Chang, F. R. (2012). Guest Editor's Column. *The Next Wave*, *19*(4). https://www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-19-4.pdf

Clark, D. D., & Wilson, D. R. (1987). *A Comparison of Commercial and Military Computer Security Policies*. 184–194. https://doi.org/10.1109/SP.1987.10001

Clarke, R. (2005, May 9). *Human-Artefact Hybridisation: Forms and Consequences*. Ars Electronica 2005 Symposium, Linz, Austria. http://www.rogerclarke.com/SOS/HAH0505.html

Clarke, R. (2016). Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives. *Computer Law & Security Review*, *32*(3), 403–418. https://doi.org/10.1016/j.clsr.2016.01.009

Clarke, R. (2017). *Cyberspace, the Law, and our Future* [Talk]. Issue Launch of Thematic Issue Cyberspace and the Law, UNSW Law Journal, Sydney. http://www.rogerclarke.com/II/UNSWLJ-CL17.pdf

Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press. http://juliecohen.com/configuring-the-networked-self

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Denning, D. E. R. (1982). *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc.

Diffie, W., & Landau, S. (2010). *Privacy on the Line: The Politics of Wiretapping and Encryption*. MIT Press. https://library.oapen.org/handle/20.500.12657/26072

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147. https://doi.org/10.2307/2095101

Erickson, P., Klein, J. L., Daston, L., Lemov, R. M., Sturm, T., & Gordin, M. D. (2013). *How Reason Almost Lost its Mind: The Strange Career of Cold War Rationality*. The University of Chicago Press. https://doi.org/10.7208/chicago/9780226046778.001.0001

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., & Grimes, J. (2015). Improving SSL Warnings: Comprehension and Adherence. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI*, *15*, 2893–2902. https://doi.org/10.1145/2702123.2702442

Fiesler, C., Beard, N., & Keegan, B. C. (2020). No Robots, Spiders, or Scrapers: Legal and Ethical Regulation of Data Collection Methods in Social Media Terms of Service. *Proceedings of the International AAAI Conference on Web and Social Media*, *14*(1), 187–196.

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., & Dell, N. (2018). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, *667*, 1–667. https://doi.org/10.1145/3173574.3174241

Friedler, S. A., Scheidegger, C., Venkatasubramanian, S., Choudhary, S., Hamilton, E. P., & Roth, D. (2019). A comparative study of fairness-enhancing interventions in machine learning. *Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT**, *19*, 329–338. https://doi.org/10.1145/3287560.3287589

Gangadharan, S. P., & Niklas, J. (2019). Decentering technology in discourse on discrimination. *Information, Communication & Society*, *22*(7), 882–899. https://doi.org/10.1080/1369118X.2019.1593484

Global Cyber Security Capacity Centre. (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition*. Global Cyber Security Capacity Centre, University of Oxford. https://doi.org/10.2139/ssrn.3657116

Graham, M. (2013). Geography/internet: Ethereal alternate dimensions of cyberspace or grounded augmented realities? *The Geographical Journal*, *179*(2), 177–182. https://doi.org/10.1111/geoj.12009

Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report*, *163*, 24–26.

Grossman, W. (2017, June). Crossing the Streams: Lizzie Coles-Kemp. *Research Institute for the Science of Cyber Security Blog*.

Gürses, S. (2014). Can you engineer privacy? *Communications of the ACM*, *57*(8), 20–23. https://doi.org/10.1145/2633029

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

International Telecommunication Union. (2019, March). *National CIRTs Worldwide* [Perma.cc record]. https://perma.cc/MSL6-MSHZ

I.T.U.-T. (2008, April 18). *X.1205: Overview of cybersecurity*. https://www.itu.int/rec/T-REC-X.1205-200804-I

Kabanov, Y. (2014). *Information (Cyber-) Security Discourses and Policies in the European Union and Russia: A Comparative Analysis (WP 2014-01*. Centre for German and European Studies (CGES. https://zdes.spbu.ru/images/working_papers/wp_2014/WP_2014_1–Kabanov.compressed.pdf

Kanwal, G. (2009). China's Emerging Cyber War Doctrine*Journal of Defence Studies, 3*(3).

Kemmerer, R. A. (2003). Cybersecurity. *25th International Conference on Software Engineering, 2003. Proceedings*, 705–715. https://doi.org/10.1109/ICSE.2003.1201257

Kerr, O. S. (2003). Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes. *New York University Law Review*, *78*(5), 1596–1668.

Kerr, O. S. (2016). Norms of Computer Trespass. *Columbia Law Review*, *116*, 1143–1184.

Koops, B.-J. (2006). Should ICT Regulation Be Technology-Neutral? In B.-J. Koops, C. Prins, M. Schellekens, & M. Lips (Eds.), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (pp. 77–108). T.M.C. Asser Press.

Korff, D. (2019). First do no harm: The potential of harm being caused to fundamental rights and freedoms by state cybersecurity interventions. In *Research Handbook on Human Rights and Digital Technology*. Elgar.

Kosseff, J. (2020). *Cybersecurity law* (Second). Wiley. https://doi.org/10.1002/9781119517436

Kostova, B., Gürses, S., & Troncoso, C. (2020). Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design. *ArXiv*. http://arxiv.org/abs/2007.08613

Krombholz, K., Busse, K., Pfeffer, K., Smith, M., & Zezschwitz, E. (2019). *'If HTTPS Were Secure, I Wouldn't Need 2FA'—End User and Administrator Mental Models of HTTPS*. 246–263. https://doi.org/10.1109/sp.2019.00060

Krombholz, K., Mayer, W., Schmiedecker, M., & Weippl, E. (2017). *I Have No Idea What I'm Doing'—On the Usability of Deploying HTTPS*. 1339–1356. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/krombholz

Kshetri, N. (2016). Cybersecurity and Development. *Markets, Globalization & Development Review*, *1*(2). https://doi.org/10.23860/MGDR-2016-01-02-03

Lee, R. M., & Rid, T. (2014). OMG Cyber! *The RUSI Journal*, *159*(5), 4–12. https://doi.org/10.1080/03071847.2014.969932

Levy, I. (2020). *High level privacy and security design for NHS COVID-19 Contact Tracing App*. National Cyber Security Centre. https://www.ncsc.gov.uk/files/NHS-app-security-paper%20V0.1.pdf

Levy, K., & Schneier, B. (2020). Privacy threats in intimate relationships. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa006

Lin, Y., Michel, J.-B., Aiden, E. L., Orwant, J., Brockman, W., & Petrov, S. (2012). Syntactic annotations for the Google Books ngram corpus. *Proceedings of the ACL 2012 System Demonstrations*, 169–174.

Matwyshyn, A. M. (2017). CYBER! *Brigham Young University Law Review*, *2017*(5), 1109. https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6/

Maurer, T., Hohmann, M., Skierka, I., & Morgus, R. (2015). *National CSIRTs and Their Role in Computer Security Incident Response* [Policy Paper]. New America; Global Public Policy Institute. http://newamerica.org/cybersecurity-initiative/policy-papers/national-csirts-and-their-role-in-computer-security-incident-response/

Maxwell, J. C. (1867-1868). On Governors. *Proceedings of the Royal Society of London, Vol. 16 (1867 - 1868)*, pp. 270-283

Miller, B. (2010, March 1). CIA Triad [Blog post]. *Electricfork*. http://blog.electricfork.com/2010/03/cia-triad.html

Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.

Moyle, E. (2019). *CSIRT vs. SOC: What's the difference?* In *Ultimate guide to cybersecurity incident response* [TechTarget SearchSecurity]. https://searchsecurity.techtarget.com/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

Naiakshina, A., Danilova, A., Gerlitz, E., Zezschwitz, E., & Smith, M. (2019). 'If you want, I can store the encrypted password': A Password-Storage Field Study with Freelance Developers. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, *19*, 1–12. https://doi.org/10.1145/3290605.3300370

Neale, M. (2000, October 4). *No Maps for These Territories* [Documentary]. Mark Neale Productions.

Neumann, A. J., Statland, N., & Webb, R. D. (1977). Post-processing audit tools and techniques. In Z. G. Ruthberg (Ed.), *Audit and evaluation of computer security* (pp. 2–5). National Bureau of Standards. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, *7*(2), 61–73. https://doi.org/10.1007/s10676-005-4582-3

Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018). An Experience Sampling Study of User Reactions to Browser Warnings in the Field. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, *18*, 1–13. https://doi.org/10.1145/3173574.3174086

Rid, T. (2016). *Rise of the Machines: The lost history of cybernetics*. Scribe.

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/a:1011902718709

Sellars, A. (2018). Twenty Years of Web Scraping and the Computer Fraud and Abuse Act. *Boston University Journal of Science & Technology Law*, *24*(2), 372. https://scholarship.law.bu.edu/faculty_scholarship/465/

Silverstone, R., & Hirsch, E. (1992). *Consuming Technologies: Media and Information in Domestic Spaces*. Routledge. https://doi.org/10.4324/9780203401491

Snowden, E. (2019). *Permanent Record*. Pan Macmillan.

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, *9*(S3), 60–66. https://doi.org/10.1111/1758-5899.12625

Wagner, B., & Vieth, K. (2016). Was macht Cyber? Epistemologie und Funktionslogik von Cyber. *Zeitschrift für Außen- und Sicherheitspolitik*, *9*(2), 213–222. https://doi.org/10.1007/s12399-016-0557-1

Ware, W. (1970). *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Issues R609-1)) [Report]. The RAND Corporation. https://doi.org/10.7249/R609-1

Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proceedings of the 8th Conference on USENIX Security Symposium*, *8*. https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten.ps

Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. MIT Press.

Zittrain, J. L. (2006). The Generative Internet. *Harvard Law Review*, *119*, 1974–2040. http://nrs.harvard.edu/urn-3:HUL.InstRepos:9385626

Appendix 1 – Cybersecurity in other languages [5]

TABLE 1: Terms for cybersecurity (via Google Translate on 14 September 2020, checked against by native speakers).

LANGUAGE	TERM
Afrikaans	kubersekuriteit
Arabic	الأمن الإلكتروني

5. According to Google Translate, confirmed or updated by native speakers consulted by the authors, including the top-15 most spoken languages according to Wikipedia. With thanks to Eleftherios Chelioudakis, Francis Davey, Fukami, Andreas Grammenos, Hamed Haddadi, Werner Hülsmann, Douwe Korff, Sagwadi Mabunda, Bogdan Manolea, Matthias Marx, Veni Markovski, Grace Mutung'u, Yudhistira Nugraha, Jan Penfrat, Judith Rauhofer, Kaspar Rosager, Eric Skoglund, Anri van der Spuy and Mathias Vermeulen for many of these translations!

LANGUAGE	TERM
Bengali	?????? ?????????
Bulgarian	киберсигурност
Chinese	????
Danish	computersikkerhed
Dutch	cyberbeveiliging
Finnish	Kyberturvallisuus
Farsi	امنیت شبکه (or امنیت رایانه/ امنیت سایبری)
French	la cyber-sécurité
German	Cybersicherheit (sometimes IT-sicherheit, Informationssicherheit, or Onlinesicherheit in Austria)
Greek	κυβερνασφάλεια
Hindi	????? ???????
Bahasa Indonesia	keamanan siber
Italian	sicurezza informatica
Japanese	??????????
Portuguese	cíber segurança
Marathi	????? ???????
Romanian	securitate cibernetica
Russian	кибербезопасность
Spanish	ciberseguridad or (more popularly) seguridad informática
Swahili	usalama wa mtandao
Swedish	Cybersäkerhet (or, commonly, IT-säkerhet)
Urdu	سائبر سیکورٹی
Xhosa	ukhuseleko

One important difference between European languages is that some (such as English) differentiate *security* and *safety*, while others (such as Swedish and Danish) do not. One sociologist of security noted: “it does frame how you understand the concepts, particularly structure. When you're talking about access control in Swedish it's a different logic than when you talk about it in Anglo-Saxon languages [...] In the Scandinavian view of the world there is always a much more

socio-technical bent for thinking about security" (Grossman, 2017).

Published by
Alexander von Humboldt Institute for Internet and Society
in cooperation with
CREATe
centre internet et societe
R&I IN3 Internet interdisciplinary Institute
Universitat Oberta de Catalunya