COGITATIO

Politics and Governance (ISSN: 2183–2463)
2018, Volume 6, Issue 2, Pages 22–30
DOI: 10.17645/pag.v6i2.1385

Article

Cybersecurity Research Meets Science and Technology Studies

Myriam Dunn Cavelty

Center for Security Studies, ETH Zürich, 8092 Zürich, Switzerland; E-Mail: dunn@sipo.gess.ethz.ch

Submitted: 26 January 2018 | Accepted: 18 April 2018 | Published: 11 June 2018

Abstract
This article sets out to show how different understandings of technology as suggested by Science and Technology Studies (STS) help reveal different political facets of cybersecurity. Using cybersecurity research as empirical site, it is shown that two separate ways of understanding cybertechnologies are prevalent in society. The primary one sees cybertechnologies as apolitical, flawed, material objects that need to be fixed in order to create more security; the other understands them as mere political tools in the hands of social actors without considering technological (im)possibilities. This article suggests a focus on a third understanding to bridge the uneasy gap between the two others: technology defined as an embodiment of societal knowledge. The article posits that in line with that, the study of cyberpolitics would benefit from two innovations: a focus on cybersecurity as social practice—enacted and stabilized through the circulation of knowledge about vulnerabilities—and a focus on the practices employed in the discovery, exploitation and removal of those vulnerabilities.

Keywords
actor-network theory; cybersecurity; cyberwar; science and technology studies; sociology of knowledge

Issue
This article is part of the issue "Global Cybersecurity: New Directions in Theory and Methods", edited by Tim Stevens (King's College London, UK).

1. Introduction

Cybersecurity is an important matter in (inter)national politics. But what makes it a *political* issue? Is it not the case that cybersecurity sensitivities arise primarily due to the continued proliferation of digital *technologies* in many aspects of human life? More specifically, if we were to take away the technologies, would the issues not be solved?

Of course, to claim that cybersecurity is predominantly about technology does not do the issue justice, not least because there is ample research both recognizing and focusing upon the human aspect of the security equation (Furnell & Clarke, 2012; Lebek, Uffen, Neumann, Hohler, & Breiter, 2014). Despite this human aspect, this article will proceed from the claim: cybersecurity is about technology. To clarify, as science and technology studies (STS) purport, "technology" means more than is implied by the common usage of the term (Bijker, Hughes, & Pinch, 1987). To make the statement less provocative and more analytically meaningful, this article sets out to show how *three different conceptualisations* of technology can help reveal different facets of cybersecurity as a technopolitical issue. Though there are attempts to bridge the gap between STS and international relations literature more generally (McCarthy, 2016), the STS perspective has not as yet been fruitfully applied to the study of cybersecurity politics.

Following Bijker (2006) the first of the three understandings is *material*: it frames technologies as static artefacts, i.e., "things". The second of Bijker's understandings links technology to social activities: it refers to the interactive relationship between technological objects and humans. The third—and perhaps least familiar—perspective understands technology according to its etymological roots in Ancient Greek, as *techne* and *logos*. *Techne* means art, skill, craft, or the way, manner, or means by which a thing is gained. *Logos* means word, the utterance by which inward thought is expressed, a saying, or an expression. This third perspective thus refers to the discourse around "what people know as well as about what they do with" technology (Bijker, 2006, p. 682).

Technologies in this view are embodiments of societal knowledge, sites where power relations can be seen in operation as they shape and coordinate the behaviour of social actors (Behrent, 2013, p. 57; also Foucault, 1981).

Broadly speaking, STS focusses on the simultaneous shaping of scientific knowledge, technological artefacts and societal matters (cf. Jasanoff, 2005). For cybersecurity, science is an interesting empirical field from which to learn more about the dominant and less dominant ways of thinking about the issue. Empirically, this article uses biometric data to show how the different perspectives of technology play out more concretely. To help understand dominant views of technology *across* disciplines without falling prey to a disciplinary bias, the article turns to scientific output as documented in two prominent scientific databases—World of Science (WoS) and Scopus.[1] In contrast to disciplinary literature reviews (for example, Ebert & Maurer, 2017), the quantitative nature of bibliometrics "provides a certain sense of objectivity for descriptive purposes" (Martinez-Gomez, 2015, p. 209), which of course does not absolve us from interpreting the results carefully in the appropriate context.[2]

The article has three main sections, one for each of Bijker's ways of understanding technology matched to cybersecurity research. What the bibliometric analysis shows is that the first perspective is by far the most dominant. In this "techno-objectivist" view, cybertechnologies are seen as broken "objects" that need to be fixed to produce more security. Political forces are not considered, even though they clearly pre-shape the research environment. The second view, which is marginalized in comparison, is "politico-subjectivist". Cybersecurity is read within pre-existing frameworks of political theories and assumptions. By focusing on cybertechnologies as tools of power in the hands of social actors, analyses often lose sight of technological materiality and idiosyncrasies, which leads to unsatisfactory conclusions.

In contrast to the first two, the third understanding of technology is not visible in the research output. Given that this thematic issue is looking for "innovative approaches to the study of global cybersecurity governance" within the broad field of political science, the article suggests how it could be used to bridge the gap between technical and social inquiries. It is suggested that political scientists can study cybersecurity in innovative ways by looking at how knowledge around the core of cybersecurity—(computer) "vulnerabilities" and their exploitation—is gained within social relations and how such knowledge is related to social and political processes of sense-making and power.

2. Dominant View: Cybersecurity as "Fixing Broken Objects"

WoS and Scopus differ in the way they classify documents into research areas. However, in both databases the field of computer science tops the lists of research areas (WoS: 72%/Scopus: 61%), followed by engineering (WoS: 36%/Scopus: 40%).[3] Though disciplinary categorization comes with its own challenges, this trend is still indicative of the background of the professionals who produce the most cybersecurity research and where the intellectual home of cybersecurity sits.

Though the absolute number of citations varies between the two databases, which leads to different overall rankings, eight of the top ten most cited articles are the same in WoS and Scopus (see Table 1 for top three, matched across both databases).[4] A fact which leaves little doubt as to the area of highest interest, *all* of the Top 10 cited articles in both databases focus on smart grids and/or SCADA (Supervisory Control and Data Acquisition) systems, a category of software application used in many industrial processes to better control equipment and conditions. The majority of these Top 10 articles were published in journals run by the *Institute of Electrical and Electronics Engineers* (IEEE), the largest existing professional association for technical professionals. All the articles are relatively recent, focus on conceptual clarifications, define the new challenges of "cyber-physical systems", offer some classification for different

Table 1. The three most cited cybersecurity publications in both databases (in October 2017).

Title	Journal	Published in
A Reliability Perspective of the Smart Grid (Moslehi & Kumar, 2010)	IEEE Transaction on Smart Grid	2010
A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges (Yan, Qian, Sharif, & Tipper, 2013)	IEEE Communications Surveys And Tutorials	2013
Cyber-Physical System Security for the Electric Power Grid (Sridhar, Hahn, & Govindarasu, 2012)	Proceedings of the IEEE	2012

[1] Google Scholar does not offer the same services of analysis and data extraction at the moment and was therefore not used due to the impossibility to compare the data. On the differences between the databases, see Mongeon and Hus (2016).
[2] Data was considered up to the end of 2016.
[3] Multiple categories per entry are allowed.
[4] The usual method to identify publications with the most influence is to look at their number of citations. There are plenty of well-known issues with such an approach (Archambault, Vignola-Gagné, Côté, Larivière, & Gingras, 2006; Leydesdorff, 1989), but it can suffice here as an indicator of importance in the larger field.

aspects of smart grid security, and describe some of the solutions, with emphasis on risk management methodologies and future research needs.

A qualitative reading of the top 10 cited articles reveals that the reason for studying cybersecurity issues stems from a set of larger, uncontested technological trends including autonomous systems as well as cloud and high performance computing. The level of risk is considered to be on the rise because of progressive digitalization. Through the connection of the virtual realm with the real world in "cyber-physical systems", scenarios involving more severe damage are possible, the most serious being a sustained and large-scale power outage with potentially catastrophic consequences. These scenarios are not new. On the contrary, they have always been very strong fear mobilizers in the related policy debate (Conway, 2008). However, recent technological developments (*opportunity*) coupled with reports of rising skills of malicious actors (*capabilities*) make these scenarios seem more likely now than they ever were.

"Vulnerabilities", exploitable flaws in code or design of hardware or software, are the focal point of this type of research. In the field of IT-Security, vulnerabilities are defined as weaknesses or flaws in hardware or software products that allow an attacker with sufficient capabilities to compromise the integrity, availability, or confidentiality of a resource (cf. Bowen, Hash, & Wilson, 2006). The type of security that is sought is a combination of these three IT-security goals—if only one is compromised, the system's overall security is compromised. Integrity refers to the trustworthiness of a resource: it is compromised if silent modification without authorization occurs. Availability is compromised if an appropriate user is denied access to a resource. Confidentiality is compromised if somebody gains access to information that she should not have had access to. The main aim of research is to develop better cyberincident prevention, protection and detection capabilities on the one hand and more "resilient" systems and infrastructures, signifying timely recovery of functionality if under duress due to an attack, on the other. The causes of the insecurity are of little interest—fixing them is the priority.

From this perspective, data is like a raw material, the "blood" of cyberspace, that which circulates through the arteries (the information infrastructure). Security here is security *of* cyberspace—the protection of the body and the blood. Cybertechnologies are mere objects to be acted upon. Ultimately, we are looking at the practice of fixing flawed, inanimate "things" to the greater benefit of all. This way of thinking is instrumental for sustaining a specific kind of a-political materiality, which is an underlying condition for security and protection practices, but is also reproduced through them (Aradau, 2010). Political practices or borders are secondary: all things share the same vulnerabilities and everybody will profit equally from fixing them. Consequently, cybersecurity is entirely positive in its overall connotation. The focus is on developing usable "tools and techniques" to improve the overall level of IT-security. Future research is geared towards developing marketable solutions that will create a larger benefit for society through a) ensuring trust in cybertechnologies and b) economic growth through innovation in the IT (security) market.

This dominant understanding of cybertechnologies manages to sidestep politics almost completely, and yet is quite obviously very much in its grip. Two data-driven observations support this claim (see Figure 1). First, cybersecurity research output sees an almost exponential

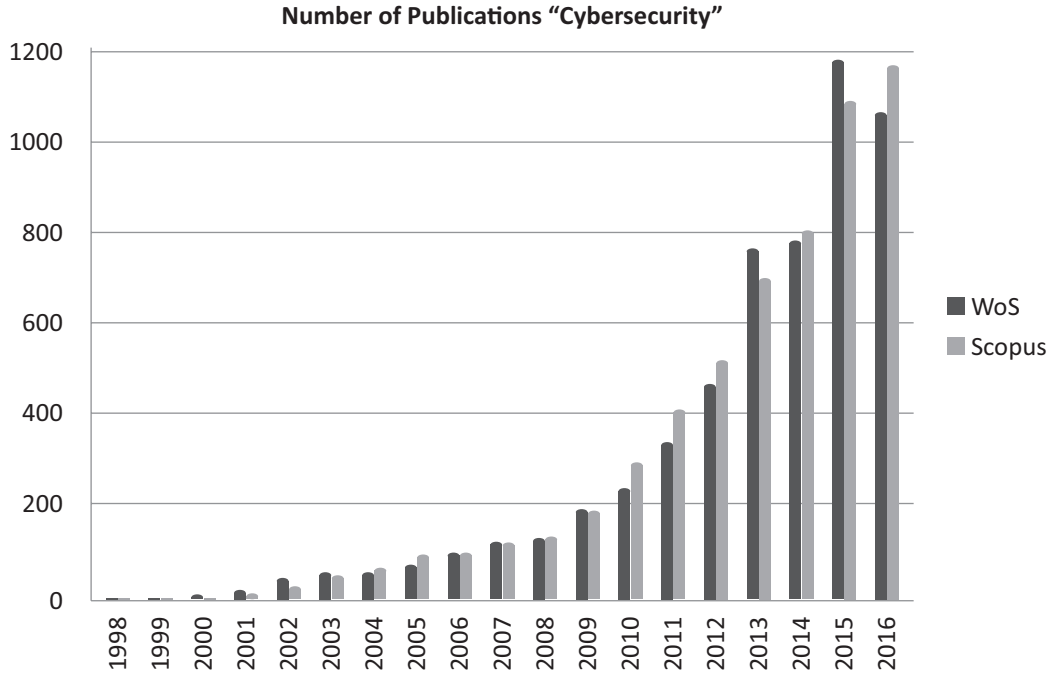

Figure 1. Number of published items per year with Topic "Cybersecurity" (WoS and Scopus).

growth rate. From 2012 to 2014, the number of scientific products almost doubled, with another steep increase in 2015. Even if we can only speculate about why 2012 is the watershed year, we can observe that the steep increase in cybersecurity-related publications around 2012 mirrors the time political attention shifted to highly sophisticated and targeted attacks (epitomized by Stuxnet). They were regarded as indicators for the rising capabilities and political willingness of state actors to use cyberspace for strategic goals (Farwell & Rohozinski, 2011; Langner, 2011). Beyond the question whether there is an *objective* increase in willingness and skill for cyberattacks among political actors, the focus of research on SCADA-systems (as targeted by Stuxnet) and on the infrastructure considered the most "critical" for society (electricity) is intertwined with political interests and sensibilities.

Second, cybersecurity was non-existent as a research topic before 2002, which mirrors observations elsewhere that the term came into existence and gained widespread traction in the policy field only around the year 2000 (Dunn Cavelty & Suter, 2012). Though the details of this dynamic remain unclear, one observer convincingly calls it "attributable to a combination of military influence, marketing hype and societal acceptance" (Rout, 2015). The choice of researchers to use the label "cybersecurity" for their research (rather than Internet security or information security) also occurs against a specific political background. Literature that focuses on the diplomatic difficulties of coming to any international agreements about "cybersecurity" has pointed out that the term is favoured primarily by Western states. In a clear move to disassociate from the Western understanding, Russia and China in particular like to use the term "Information Security" (Giles & Hagestad, 2013). Indeed, in both databases, the US tops the list of the Top 10 countries where cybersecurity research originates by a large margin (WoS: 63%/Scopus: 75%). However, for the search term "Information Security", China leads the ranking before the US (WoS: China 25%, US 11%/ Scopus: China 23%, US 18%).

3. Secondary View: Social Interactions with and through Cybertechnologies

The second conceptualization of technology is focused on the interactions between technology and social actors. As the empirical research reveals, this view is predominantly found in the category "social sciences".[5] Scopus has "social sciences" as a lump category on third place, with 18%. WoS lists 31% of its cybersecurity records in "social sciences", which is the third largest category after "science and technology" and "technology". Overall, this type of research is far less prevalent than the first type (cybersecurity as fixing broken things). Even though there was also a quantitative increase of research around 2010, there is a growing gap between computer sciences and engineering approaches and social sciences research (Figure 2).

Top cited research in the social sciences[6] is much more diverse than the dominant (computer science) view. A reading of the articles reveals two main focal points. The first is an interest in organizational and managerial aspects of cybersecurity, such as "information

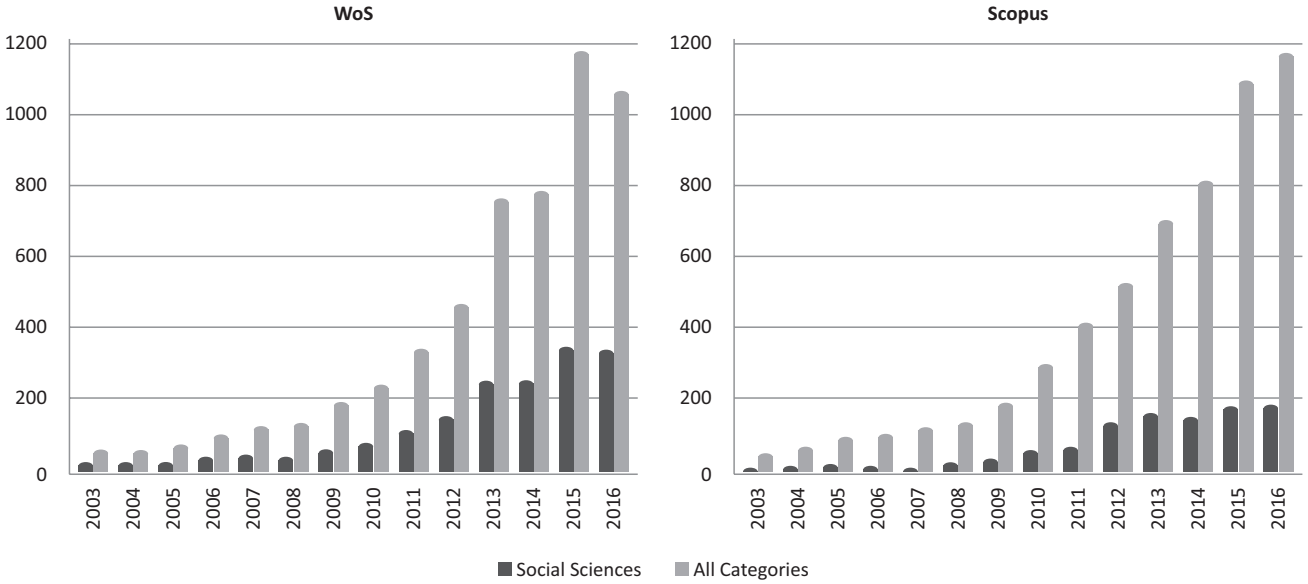

Figure 2. Output of Social Science Research vs. General Cybersecurity Research, both WoS (left) and Scopus (right).

[5] Importantly: this is a database category and does not mean to say that only social scientists work on these issues. In fact, most publications are classified into several different such categories.

[6] For each publication, multiple research areas can be chosen. Therefore, some of the top 10 papers in the social sciences category overlap with the general top 10 papers. After reducing the sample to "pure" social science, 1,220 entries remain in WoS and 497 documents in Scopus.

sharing" between state and private actors (the top cited article in both databases is Gal-Or & Chose, 2005) or the combination of technology with human and organizational factors (cf. Arce, 2003). The second focal point is on cyberwar and related political violence phenomena, which is closer to the core interest of this article. After filtering the results for publications in the "international relations" category, cyberwar and other threat forms dominate in the top cited publications (see Table 2).

Again, the 10 top ranked publications were read for a more thorough understanding of how cybersecurity is viewed. The focus shifts from the inbuilt insecurity of cybertechnologies to their intentional (mis)use by different social actors (and the political processes or concepts this challenges or triggers). The research questions vary depending on the meta-theoretical stance of the authors, leading to a treatment of cybersecurity either as an "objective" problem that calls for different (political) solutions (this is the dominant view) or as a "subjective" construction where different threat perceptions are linked to political outcomes that are critically reflected (this is the less dominant view).

Cybertechnologies become abstract tools of power ("black boxes" in STS jargon) with which to threaten objects and services of value to the state and society in peacetime and during conflict. If threats are considered, there is also an inward-looking focus on vulnerabilities, yet these vulnerabilities are no longer (just) the vulnerabilities in machines, but higher-level, abstract vulnerabilities of the entire society. In a dominant part of the literature, cybertechnologies shape the familiar "realist" conception of inter-state security in an anarchical system. Since these technologies create vulnerabilities that can have detrimental effects on society, more or less traditional "threat" actors and their willingness to do harm come into focus. This way, cybertechnologies gain traction as tools or even "weapons" for disruption and insecurity in the hands of political actors, often states.

Because a link is established to the abstract notion of "national security", states are frequently the actors called upon to re-establish control over the misuse of cybertechnologies through international norms, often by looking to lessons from previous security issues and solutions, like nuclear deterrence. This strong disciplinary "pull" is also visible in the way established approaches to studying political violence are "imposed" on cybersecurity topics. For example, the framing of cyberincidents as cyber*attacks* helps to study cybersecurity through the discipline's core concepts like political violence. Traditional conflict researchers aim to look at the effect of cybertechnologies as part of the toolset in foreign policy and conflict using quantitative methods (exemplary: Valeriano & Maness, 2014). The uncertainties surrounding cyberincidents or the question of what even qualifies as a cyberincident and for what reasons become secondary.

From this perspective, cybertechnologies are treated like any other tool of power projection and coercion and their effects are read in pre-established and familiar categories of political interaction. Technological knowledge has little value for such analyses. In fact, *homo homini lupus* (man is wolf to man) is one of the most important reasons for why cybersecurity has become an issue to study—though, arguably, of marginalized importance in the larger field when considering the minimal coverage in the top ranked political science journals.[7] However, the separation between technical and political knowledge has repercussions for this type of research. For example, the means of achieving security in the anarchical international system are international norms (DeNardis, 2014; Finnmore & Hollis, 2016), one of the core issues the discipline of international relations is interested in. When looking at (the lack of) clear norms for state behaviour in cyberspace solely through the political lens, two important details are missed. First, norms formation in this field is currently happening through explorative "cyberattacks", whereby political actors are using techni-

Table 2. The three most cited cybersecurity publications, filtered for "international relations".

Title	WOS Rank	Scopus Rank	Journal	Published in
Cyber War Will Not Take Place (Rid, 2012)	1	1	*Journal of Strategic Studies 35*(1), 5–32	2012
Digital Disaster, Cyber Security, and The Copenhagen School (Hansen & Nissenbaum, 2009)	2	2	*International Studies Quarterly 53*(4), 1155–1175	2009
Cybersecurity and Threat Politics (Dunn Cavelty, 2008)	3		Book, Routledge	2008
Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War (Liff, 2012)		3	*Journal of Strategic Studies 35*(3), 401–428	2012

[7] As an indication that cybersecurity is a fringe topic in the larger discipline, only one of the top three political science/international relations journals has published articles on cybersecurity (*International Organization*, 0 articles; *World Politics*, 0 articles; *International Security*, 8 articles). Overall, the observation that cybersecurity research in political science is a marginalized topic that communicates relatively little with more general international relations theory and research still hold true today (Eriksson & Giacomello, 2006).

cal means to elicit political reactions and to try out where the "red lines" are. Without a close reading of the technological (im)possibilities shaping these activities, understanding them properly in connection with norms formation processes is difficult. Second, the different communities involved in cybersecurity research and practices have very different understandings of what "security" means and implies. In the second (politico-subjective) perspective, it concerns not only security *of* cyberspace, but also a more abstract form of security that is influenced by activities *in* cyberspace (cf. DeNardis, 2012). Whereas the first is a limited notion of security closely related to technical logics, the second is not. Furthermore, the security *of* cyberspace and security *by* (*or through*) cyberspace are often diametrically opposed. That becomes apparent when we bring computer vulnerabilities back into the analysis: a strategically exploitable cyberspace wants to have vulnerabilities through which to achieve one's goals. A stable and secure cyberspace should have as little as possible. Without understanding the interactions between the two images, finding good solutions will remain elusive.

4. Cybersecurity as "Knowledge about Vulnerabilities"

Even though both the view of cybersecurity based on material vulnerabilities and the socio-political view are interconnected at the very least through their common interest in what both call "cybersecurity", the overlap between the two spheres of research is small. While the first focuses on improving technologies and governing processes without considering the larger context that shapes research questions, the second loses sight of cybertechnologies as a material underpinning of political action. The third perspective—that which sees technology as embodiment of societal knowledge—can help to bridge this gap by analytically combining technical knowledge with political knowledge. Furthermore, it comes with an interesting focus on social practices, much in line with and speaking to the practice turn in critical security studies (Bueger & Gadinger, 2014).

Importantly, neither the technical nor the political lens should be given precedence over the other, at least analytically speaking. Rather, the socio-political determines the technical, and the technical determines the socio-political and both spheres should always be considered as closely intertwined. As an example, consider the limits to the "interpretative flexibility" of cybertechnologies. "Interpretative flexibility" is a term from STS used to highlight that the interpretations and uses of any technology vary across time and between different groups (Woolgar, 1991, p. 30). However, the underlying material insecurity of cybertechnologies is not open to social interpretation. There *are* vulnerabilities that can be exploited by malicious software (malware) or through social engineering (the manipulation of human psychology). On the other hand, knowledge of these vulnerabilities combined with the right capabilities allows certain actions in specific contexts, but are restricted by the characteristic of the vulnerability and its technical environment.

Vulnerabilities (broadly understood) offer themselves as interesting concept around which cybersecurity practices converge.[8] More concretely, the third perspective invites us to focus on cybersecurity as social practice, enacted and stabilized through the circulation of knowledge about vulnerabilities. An approach from STS well suited to study these practices is *Actor Network Theory* (ANT) (Balzacq & Dunn Cavelty, 2016). ANT, better understood as "a way of thinking" instead of a coherent theory, prominently develops a generalized ontological symmetry between human and non-human entities. Both are equally involved in relational productive activities without giving one precedence over the other (Latour, 1994; Preda, 1999). Of interest is the circulation of different "objects"[9] and the structures of relations ("networks" in ANT jargon) that these objects activate. Among other things, ANT scholars are interested in understanding how social practices emerge, how they spread and how they become normalized. They are also interested in the moments such routines break down. These moments are called *depunctualization* because they interrupt the normalized and unproblematic workings of stable networks (Latour, 1999), thereby revealing their inner working to the interested analyst (cf. Best & Walters, 2013, p. 346).

Characteristically, vulnerabilities become visible once their exploitation creates an effect in a machine (the depunctualization). In a first instance, such effects affect the machine that runs the software, and potentially various other processes supported by that machine. However, depending on the type and context of these technical effects, they may be translated into political consequences. In this process, the following questions—among others—are of interest: what kind of incidents become visible and why? Why do some make it into the news, while others remain obscure or potentially invisible? Who has the authority to make claims about cyberincidents and why? In what form is this knowledge made available? Are there conflicting accounts? Do they endure or does one set of interpretations become "the truth"? How does knowledge about vulnerabilities travel between and across different boundaries and with what effects? In what ways is knowledge about vulnerabilities and their exploitation used to make political attributions? In what ways is this knowledge mobilized for political action?

Since space is scarce, a brief example must suffice here. The blockbuster malware "Stuxnet" is chosen;

[8] As a side-note, the concept could also serve for a study on "boundary objects". In STS literature, "boundary objects" operate as mediators in the coordination process between different communities of practice (originally: Star & Griesemer, 1989).

[9] Importantly, an object is not a material thing, but simply something people or other objects "act toward and with. Its materiality derives from action" (Star, 2010, p. 603).

since there is already a large amount of common knowledge about this worm, the added benefit of the proposed approach should become more easily apparent. In the phase immediately after depunctualization, a lot can be learned about power and authority and different practices of knowledge gathering specific to the tech community from observing knowledge claims about vulnerabilities and the incident. In Stuxnet's case, there were several instances of depunctualization, visible to different communities at different times (for more details, see Balzacq & Dunn Cavelty, 2016, p. 17–19). In July 2010 security blogger Brian Krebs broke the news about Stuxnet, causing a very high interest among tech-oriented news media (Krebs, 2010). Several other security researchers added facets of knowledge afterwards. The pieces were finally assembled by Ralph Langner, a German security researcher, who first claimed that Stuxnet was a precision weapon targeting specific facilities and that significant insider knowledge was required for the creation of this worm (Langner, 2010). That made the classification of this malware as "weapon" possible and gave this program particular weight in the discourse.

As soon as several unusual aspects about the malware became public knowledge, attempts to "attribute" the malware began to dominate the discussion. This is a second phase after depunctualization that reveals the interplay between the technical and the political. In November 2010, Langner claimed that the culprit was most likely Israel, the US, Germany or Russia (Zeiter, 2011)—using the *cui bono* logic (to whose benefit) as a basis for this statement. Alternative interpretations existed at the time, but they did not manage to convince a larger audience. Not long after, it became accepted knowledge that Stuxnet was launched by the US and Israel. Debates about this attribution continued among security experts for a time, until a detailed report in the New York Times in June 2012 took an authoritative stance on the attribution question. In this article, David E. Sanger, claiming access to government sources, explained how Stuxnet was programmed and released as a collaborative effect between American and Israeli intelligence services (Sanger, 2012). This explanation has since established itself as the "truth" because the technical expertise was aligned with and influenced by political reasoning.

Of course, we cannot expect access to the inner workings of intelligence agencies and the knowledge creation processes happening there. Nevertheless, public statements by political actors about vulnerabilities and cyberincidents are available and can be studied as part of the larger picture. In the case of Stuxnet, because the US was accepted as the likely culprit, the reaction of its "allies" were twofold. On the one hand, many states updated their cybersecurity strategies. On the other hand, they started investing in cybercapabilities for both their military and their intelligence agencies, in turn creating new possibilities for security-relevant practices. While such reactions can be explained by pointing to the "security dilemma", the actual practices of security actors in cyberspace can only be understood when we take into account the technical possibilities. Finally, returning to the point made above about emerging "norms" of behaviour in cyberspace, rules are shaped by practices and practices are guided by political interests. In cyberspace, practices always have a link to technologies. Ultimately, understanding the behaviour of involved actors means understanding social practices as shaped and restrained by technological (im)possibilities.

5. Conclusion

Though it is true that without (insecure) technology we would not have a cybersecurity issue, these issues also cannot be solved through technical means alone. In addition, though it is impossible to understand the evolution of cybersecurity as a policy issue without telling it as a history shaped by digital technologies and their (mis)use, we cannot understand why it is considered one of the top security political challenges of our time without also understanding why and how digital technologies have been used in social and political contexts. Indeed, technological realities and social practices are closely intertwined.

This article used scientific research as an empirical basis to gain an understanding of how cybersecurity is viewed and then matched it to three views of technology discussed in STS. Two dominant perspectives were identified. The first sees cybersecurity as the practice of fixing broken objects and the second sees cybertechnologies as tools to further political goals. With relatively little overlap between them, the first view neglects social construction and meaning-making processes whereas the second focuses too much on preconceived notions of politics and security, with too little knowledge of how the materiality of the artefacts constrains their use. What we therefore need for innovative cybersecurity research is to combine both perspectives at the intersection between the technical and the social to the greater benefit of both communities. At this intersection, as argued in this article, lies knowledge (and non-knowledge) about vulnerabilities. Therefore, to bridge the two spheres of research, we need to study how knowledge about vulnerabilities is created, disseminated and transformed into political (and other) effects.

Acknowledgements

I would like to thank the three anonymous reviewers and the academic editor for their very helpful comments and my Cybersecurity Team at the Center for Security Studies, ETH Zürich for the many fruitful discussions over coffee and lunch and in the corridors. Special thanks to Robert Dewar for proofreading and editing.

Conflict of Interests

The author declares no conflict of interests.

References

Aradau, C. (2010). Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, *43*(2), 491–514.

Arce, I. (2003). The weakest link revisited. *IEEE Security & Privacy*, *1*(2), 172–176.

Archambault, É., Vignola-Gagné, É., Côté, G., Larivière, V., & Gingras, Y. (2006). Benchmarking scientific output in the social sciences and humanities: The limits of existing databases. *Scientometrics*, *68*(3), 329–342.

Balzacq, T., & Dunn Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176–198.

Behrent, M. C. (2013). Foucault and technology. *History and Technology*, *29*(1), 54–104.

Best, J., & Walters, W. (2013). Translating the sociology of translation. *International Political Sociology*, *7*(3), 345–349.

Bijker, W. E. (2006). Why and how technology matters. In R. E. Goodin & C. Tilly (Eds.), *The Oxford handbook of contextual political analysis* (pp. 681–706). Oxford: Oxford University Press.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (1987). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

Bowen, P., Hash, J., & Wilson, M. (2006). *Information security handbook: A guide for managers*. Gaithersburg: National Institute of Standards and Technology (NIST).

Bueger, C., & Gadinger, F. (2014). *International practice theory: New perspectives*. Basingstoke: Palgrave Macmillan.

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In M. Dunn Cavelty & K. S. Kristensen (Eds). *Securing 'the homeland': Critical infrastructure, risk and (in)security* (pp. 109–129). London: Routledge.

DeNardis, L. (2012). Hidden levers of internet control. *Information, Communication & Society*, *15*(5), 720–738.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Dunn Cavelty, M., & Suter, M. (2012). The art of CIIP strategy: Taking stock of content and processes. In J. Lopez, R. Setola, & S.D. Wolthusen (Eds.), *Critical infrastructure protection: Information infrastructure models, analysis, and defense* (pp. 15–38). Berlin: Springer.

Dunn Cavelty, M. (2008). *Cyber-security and threat politics: US efforts to secure the information age*. London: Routledge.

Ebert, H., & Maurer, T. (2017). Cyber security. *Oxford Bibliographies*. Retrieved from http://oxfordbibliographiesonline.com/view/document/obo-9780199743292/obo-9780199743292-0196.xml?

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review*, *27*(3), 221–244.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of cyber war. *Survival*, *53*(1), 23–40.

Finnmore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *The American Journal of International Law*, *110*(3), 425–479.

Foucault, M. (1981). *The history of sexuality* (Vol. 1). Harmondsworth: Penguin.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988.

Gal-Or, E., & Chose, A. (2005). The Economic incentives for sharing security information. *Information Systems Research*, *16*(2), 186–208.

Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *Proceedings of the 5th international conference on cyber conflict* (pp. 1–17). Tallinn: CCD COE Publications.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175.

Jasanoff, S. (2005). *Designs on nature: Science and democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.

Krebs, B. (2010, July 10). Experts warn of new windows shortcut flaw. *Krebs on Security*. Retrieved from www.krebsonsecurity.com/2010/07/experts-warn-of-new-windows-shortcut-flaw

Langner, R. (2010, September 10). *Stuxnet logbook, Sep 16 2010, 1200 hours mesz*. Retrieved from www.langner.com/en/2010/09/16/stuxnet-logbook-sep-16-2010-1200-hours-mesz

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, *9*(3), 49–51.

Latour, B. (1994). Pragmatogonies: A mythical account of how humans and non-humans swap properties. *American Behavioral Scientist*, *37*(6), 791–808.

Latour, B. (1999). *Pandora's hope: Essays on the reality of science studies*. Cambridge, MA: Harvard University Press.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breiter, M. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092.

Leydesdorff, L. (1989). The relation between qualitative theory and scientometric methods in science and technology studies. *Scientometrics*, *15*(5/6), 333–347.

Liff, A. P. (2012). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, *35*(3), 401–428.

Martínez-Gómez, A. (2015). Bibliometrics as a tool to

map uncharted territory: A study on non-professional interpreting. *Perspectives*, *23*(2), 205–222.
McCarthy, D. R. (2016). *Technology and world politics: An introduction*. London: Routledge.
Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, *106*(1), 213–228.
Moslehi, K., & Kumar, R. (2010). A reliability perspective of the Smart Grid. *IEEE Transactions on Smart Grid*, *1*(1), 57–64.
Preda, A. (1999). The turn to things: Arguments for a sociological theory of things. *The Sociological Quarterly*, *40*(2), 347–366.
Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35*(1), 5–32.
Rout, D. (2015). Developing a common understanding of cybersecurity. *ISACA Journal*, 6. Retrieved from https://www.isaca.org/Journal/archives/2015/volume-6/Pages/developing-a-common-understanding-of-cybersecurity.aspx
Sanger, D. E. (2012, June 1). Obama order sped up wave of cyberattacks against Iran. *The New York Times*. Retrieved from www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=2
Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, *100*(1), 210–224.
Star, S. L., & Griesemer, J. R. (1989). Institutional ecology, "Translations" and boundary objects: Amateurs and professionals in Berkeley's museum of vertebrate zoology, 1907–39. *Social Studies of Science*, *19*(3), 387–420.
Star, S. L. (2010). This is not a boundary object: Reflections on the origin of a concept. *Science, Technology & Human Values*, *35*(5), 601–617.
Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists 2001–11. *Journal of Peace Research*, *51*(3), 347–360.
Woolgar, S. (1991). The turn to technology in social studies of science. *Science, Technolgy & Human Values*, *16*(1), 20–50.
Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2013). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. *IEEE Communications Surveys and Tutorials*, *15*(1), 5–20.
Zeiter, K. (2011, November 7). Stuxnet timeline shows correlation among events. *Wired*. Retrieved from www.wired.com/2011/07/stuxnet-timeline

About the Author

Myriam Dunn Cavelty is a senior lecturer for security studies and deputy for research and teaching at the Center for Security Studies (CSS), ETH Zürich. She was a visiting fellow at the Watson Institute for International Studies (Brown University) in 2007 and Fellow at the stiftung neue verantwortung in Berlin, Germany 2010–2011. Her research focuses on the politics of risk and uncertainty in security politics and changing conceptions of (inter-)national security due to cyber issues.