Cybersecurity as a Politikum

Implications of Security Discourses for Infrastructures

Fichtner, Laura; Pieters, Wolter; Herdeiro Teixeira, André

DOI
10.1145/3011883.3011887

Publication date
2016

Document Version
Accepted author manuscript

Published in
Proceedings of the 2016 New Security Paradigms Workshop

Post print version of https://doi.org/10.1145/3011883.3011887 (ACM)

Cybersecurity as a *Politikum*: Implications of Security Discourses for Infrastructures

Laura Fichtner
TU Delft
Delft, Netherlands
l.v.e.fichtner@tudelft.nl

Wolter Pieters
TU Delft
Delft, Netherlands
w.pieters@tudelft.nl

André Teixeira
TU Delft
Delft, Netherlands
andre.teixeira@tudelft.nl

ABSTRACT

In the cybersecurity community it is common to think of security as a design feature for systems and infrastructures that may be difficult to balance with other requirements. What is less studied is how security requirements come about, for which reasons, and what their influence is on the actions the system facilitates. Security is for example often used as an argument for or against granting access rights that are of importance to stakeholders, such as in the discussion on counterterrorism and privacy. This paper argues that the ongoing politicization of security issues calls for a paradigm to study cybersecurity as a *Politikum*: a matter of political concern, embedded in existing and future infrastructures. We summarize literature which inspired this paper and explain the role of security arguments for infrastructure governance. Then we outline the new paradigm and its core concepts and contribution, including the notion of framing. Finally, we present discourse analysis and infrastructure ethnography as research methods and discuss cases in which discourses (may) shape infrastructures, in particular smart cities.

CCS Concepts

•**Security and privacy** → **Social aspects of security and privacy;** *Economics of security and privacy;*

Keywords

discourse analysis, framing, infrastructure ethnography, security arguments, security politics, securitization, threat models

1. INTRODUCTION

In the cybersecurity community it is common to think of security as a design feature for systems and infrastructures that may be difficult to balance with other requirements. This however assumes there is agreement on what security is. In practice, there are different views on what the purpose of cybersecurity should be, for example in the context of the protection of (personal) information. Computer scientists often see privacy as equivalent to data confidentiality and hence as an instance of (information) security. In law and political science on the other hand, privacy and security are many times put in opposition to each other. This view has support where security is understood to require surveillance and the collection of (personal) information in order to identify and mitigate potential threats.

Such ambiguity of what security means or implies may already be familiar to many readers. Based on the recognition of this ambiguity we take one step further in this paper and propose an analysis of how this ambiguity plays out within the political sphere of infrastructure decision making and governance. This idea is in line with the Dutch Council for Government Policy [41] which sees security problems not only as *uncertain* in terms of insufficient knowledge about the consequences of threats or the effectiveness of controls, but also as inherently *ambiguous*. This means there can be controversies about what ought to be defined as desirable and undesirable effects in the first place. Focusing on information and communication technologies, in this paper we argue that security is a contested concept rather than a fixed goal. The way it is conveyed and understood (i.e. in terms of threat models and trusted parties) shapes how technologies and technological infrastructures are designed and operated. From any particular interpretation of security, *security arguments* can be deduced. These arguments can then act as *tools* for shaping the infrastructure and facilitating access to and within it. They can be used to safeguard goals, values and interests, also non-security related ones. This is what we call the political dimension of security or *security politics*.

In the paper we outline a research paradigm for unraveling and understanding this political dimension of security, focusing primarily on information and communication technology (ICT) infrastructures and on cybersecurity. With the term 'ICT infrastructures' we refer to large scale digital infrastructures built of information and communication technologies (ICTs). One prominent example for such an infrastructure would be the Internet but there are also smaller scale ICT networks such as smart city data infrastructures, university networks or infrastructure for electronic voting systems. Following Susan Leigh Star[35], we conceive of the term 'infrastructure' in a broad sense, taking it to describe underlying structures which enable interactions and activities: information and communication infrastructures enable information exchange and communication. In this

This is a preprint of an article accepted for publication in the 'Proceedings of the 2016 New Security Paradigms Workshop', ACM Digital Library under DOI http://dx.doi.org/10.1145/3011883.3011887

way, when we talk of infrastructure, we do not only refer to the purely technical network, but include for example maintenance and coordination practices and the protocols which regulate operation.

We use the Latin/German term *Politikum* to denote that security as a meaningful concept is of political importance and interest. Studying cybersecurity as a *Politikum* creates an understanding of the political and value- or interest-laden use of security concerns, arguments and solutions. Making underlying assumptions and possible implications of security arguments explicit and visible makes security practices more transparent and facilitates better communication and interaction between different actors.

The outline of this paper is as follows. In Section 2, we summarize relevant work on the political dimension of security. In Section 3 we present our paradigm's framework and its core concepts and assumptions and we discuss its contributions. In Section 4 we put forward a research agenda to study cybersecurity politics and its mechanisms; we also outline several application areas where our new paradigm fits well. We give conclusions and final remarks in Section 5.

2. INSPIRATION FROM LITERATURE

While the systematic study of cybersecurity within the framework presented here is novel, authors have addressed the political dimensions of security before, especially in the context of national security. In this section we review existing work which analyzes the ambiguity, conceptualization and politicization of security.

2.1 The meanings of security

In this subsection we discuss security as an ambiguous concept that can have different meanings and imply different activities or measures. We draw from Helen Nissenbaum's work on security and David A. Baldwin's conceptual analysis. Further we present framing as a useful lens for investigating and articulating how this ambiguity works out within communication. This subsection provides the basis for understanding how security arguments function within governance processes and as a call for action.

2.1.1 Security as an ambiguous concept

One important example of differing conceptualizations of security can be found in the divide between national and computer security which Nissenbaum for instance has distinguished as a difference between "cyber-security" and "technical computer security" [28]. Technical computer security describes security concerns closely aligned to the cybersecurity framework of confidentiality, integrity and availability (CIA). In contrast, 'cyber-security', in the way Nissenbaum uses it, describes security concerns closely related to national security. It is mainly concerned with attacks on critical infrastructures or with the use of ICT systems to facilitate behavior potentially dangerous to the stability of nation states. Technical computer security aims at securing "individual nodes" like people or companies; cyber-security focuses on collective goods or networks [28, p. 69].

These different understandings of security can have possibly contradicting implications for ICTs and the implementation of technical security measures. 'Cyber-security' and national security might call for the weakening of encryption standards in order to enable surveillance or the opening of backdoors which law enforcement and intelligence can use. 'Technical computer security' on the other hand might call for stronger encryption or systems that prevent eavesdropping and system compromise. National security concerns may call for surveillance that infringes on privacy; computer security concerns may call for ensuring privacy and access control to information (confidentiality).

Focusing on security as national security, David A. Baldwin [4] already started a discussion on the conceptual foundations of security in 1997. Dissatisfied with the existing depth of conceptual analysis of the term, he identified a number of questions that seemed to him at the core of defining security and the cause of disparity with regard to its meaning. These questions are: security (1) for whom; (2) for which values; (3) how much; (4) from what threats; (5) by what means; (6) at what cost; and (7) in which time period [4, pp. 13-17]. The last three are aspects also well-known to the domains of risk management and economics of security, where for instance the question of 'how much' is related to quantifying the amount of security [32].

Applying these conceptual questions to the example of 'technical computer security vs cyber-security' can help us understand the difference between the two. Technical computer security is often aimed at the protection of personal computers or communications (1–for whom) from for example intrusions and eavesdropping (4–from which threats) and by implementing technical measures such as encryption and authorization procedures (5–by what means); its goal can be to preserve privacy or freedom of speech (2–for which values). Cyber-security is often oriented at the protection of a nation state, its public and infrastructure (1–for whom) from for instance (cyber)attacks, organized crime and violence or anti-social behavior (4–from what threats), and often does so by means of surveillance and intelligence or military work (5–by what means); it does so to ensure nation state stability, military strength or public safety (2–for which values). If we engaged in a discussion on how to address these two 'types' of security and deal with their contradictions, we would have to answer Baldwin's other questions of 'how much' of the specific type of security we want (possibly making a trade-off) and at what costs.

2.1.2 Framing

The different notions of security presented above utilize different frames for talking about security: they pick out certain issues or events (i.e. surveillance or crime) and present them in a certain way and with certain solutions, and in their argument, they appeal to certain values. This process of presenting an issue in a certain way and embedding it within a broader normative context can be described by the notion of *framing*, first introduced by Gregory Bateson in the 80's [6]. Traditionally, the notion is used by political and media scholars in relation to how mass media function and produce (media) images situated within frames [17]. Literally, like a frame presenting a picture, media frames determine how something is presented.

Framing describes a process "by which people develop a particular conceptualization of an issue or reorient their thinking about an issue" [12, p. 104]. In this process, "some aspects of a perceived reality [are selected] and [...made] more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation" [16]. When a frame is constructed, certain aspects of an is-

sue are highlighted and others are left out, and certain values or worries are appealed to. For example, war-induced large-scale migrations of groups of people or populations (which in popular media are often framed as 'refugee crises') can be framed in different ways: as a question of international stability (political terms), as an economic threat or challenge (in terms of nation state economics), as a chance for cultural exchange or a threat to some sort of cultural preservation (cultural terms) or as a matter of human rights and solidarity (in terms of humanitarian support and human rights).

In any case of framing – by which a frame is established – a problem is defined, a cause is diagnosed, a moral judgment is made and a remedy suggested [16, p. 52]. In the case of the dichotomy presented above, 'technical computer security vs cyber-security', cybersecurity is framed in two different ways. On the one side, the problem of cybersecurity is framed as a question of protecting the data and private communications of individuals and companies against surveillance, malicious software and hacking, which are presented as the cause of the problem. Technical solutions such as encryption and laws for privacy and data protection could be potential remedies then suggested within this frame. Values appealed to and used to justify its suggestions are values like privacy and confidentiality. Within the other frame, cybersecurity is framed as a question of collecting, processing and analyzing data in order to identify threats; the problem is presented as a problem of malicious agents using computer and information networks in order to communicate, organize and carry out attacks. Surveillance and data analytics are presented as remedies, and values appealed to are for instance national stability and public safety.

In "What we talk about when we talk about cybersecurity", Josephine Wolff analyzes security arguments within internet governance debates and identifies different frames which sometimes even contradict each other [44]. One case study Wolff presents is the debate around the WHOIS database which lists personal details about the people (or organizations) who run domain names on the Internet. The debate is about whether these details, such as name and address, should be publicly displayed on the Internet. Some argue that at least for websites which run a business or offer (paid) services, consumers should be able to retrieve information about the website owners. The reason they name is the protection of consumer safety and protecting costumers from fraud. Those against such a practice on the other hand argue that keeping the data private and not displaying personal information is required as a security measure to protect individuals who run a website from for example harassment. In the debate, both sides frame their approach as a security issue but they differ in who they want to protect and why. They focus on different aspects and problems related to the issue and on different values. As Wolff concludes, "both sides would claim that their position promotes a more secure internet and a more secure society – and in a sense, both would be right, except that each promotes a differently secure internet and society, protecting different classes of people and behaviour from different threats" [44].

Hence, framing describes a meaning-making process where individual circumstances are embedded within a broader logical or moral framework. Frames define what cybersecurity is about and which kinds of problems it ought to address, as well as how and why it ought to do so; by doing this, cybersecurity is embedded within a broader context and meaning.

Concluding, any frame can be understood as a "central organizing principle that holds together and gives coherence and meaning to a diverse array of symbols" [17, p. 384]. Frames can justify and warrant certain circumstances or actions or mobilize people and groups for a certain cause. Different frames have the potential to address and mobilize different audiences, because they care about or respond to different issues and values and to different kinds of language. Frames (co)determine how perceived problems are understood; how such problems are perceived in turn justifies certain reactions. In the case of security, framing an issue does not only define the terms in which security is understood but also which solutions are perceived as viable.

2.1.3 Securitization

In the past, framing has proven to be a useful tool for investigating and articulating the political potential inherent to security and mediated by its ambiguity [24, 26, 27]. When we look at the different ways in which security is presented, we are concerned with the content of security as a concept – 'security' is the content that is framed. In the above example, in one frame security is defined as being about technical computer security, and in the other it is defined within the terms of national security.

Another security-related aspect of framing is the framing *of* a circumstance *as* a security issue. Looking at this aspect means to look at a process where a circumstance is framed *as* a security issue, and security itself provides the frame. Such processes have been described by the field of securitization studies, where researchers look at how a circumstance is constructed as a security issue in order to mobilize and justify certain actions [10], [5]. They found that framing something as a security issue has a performative function because it warrants certain actions which might be deemed unacceptable in other circumstances. An example for this would be the proclamation of a state of emergency which governments can proclaim following a security incidents such as an attack or shooting [8]. During a state of emergency, legal safeguards are partly abrogated and more rights or freedoms are granted to the executive as well as security and military forces. For this reason a state of emergency can be used to warrant certain activities as long as they are situated within the frame of attending to an acute security issue.

Securitization now also increasingly happens within the context of the Internet and other information and communication technologies. Framing decisions as security issues can, for example, warrant the implementation of surveillance backdoors. Within the securitization of 'cyberspace', there are different coexisting frames as well. Myriam Dunn Cavelty has transferred the approach of securitization studies to the 'cyberspace' in order to look at "who shapes threat representations, who (re-)uses them in what ways, and with what constitutive effects" [15, p. 118]. She examined the cybersecurity discourse and its metaphors and analyzed different stakeholders' conceptualizations of cyberspace and its threats. She identifies two paradigms or ways of framing security within the cyber-realm: one that links cyberspace to state power, control and order, and another that links it to organisms, networks and interconnectedness [15].

2.2 Security arguments as a call for action

The ambiguity of security and its contested conceptual meaning make security susceptible to being employed and possibly exploited for framing processes. When a specific conceptualization and framing is chosen, security arguments are formed which advocate certain actions or measures. These influence how the infrastructure is operated and thus play a role in infrastructure governance. In this subsection we discuss *security arguments* and their potential within infrastructure governance.

2.2.1 Security arguments

The diversity of security definitions and the controversies around security's meaning and value are interesting when we look at how the term is used to justify or motivate specific actions. When something is presented as a security issue and in a certain way, this is often coupled with some notion of how we ought to attend to this issue and which kind of solutions we should find. In this way, different security approaches motivate certain activities or actions; these have 'real world' impacts. Security utterances can be understood as calls for action that entail certain (technological) activities. These depend on the framing of the security issue and its solutions. Different security issues and approaches can be presented as *security arguments* that motivate certain activities. Such a security argument takes the form of "security requires us to do XYZ". One way to communicate a security argument and its threat model is the use of incident scenarios – bad things that could happen [21]. Each such security argument either explicitly or implicitly includes definitions (what (cyber)security is) and arguments (what we should do about it), it includes reference to a threat model and certain system presupposition, assumptions and boundaries.

The political role of framing becomes clearer when we look at the function of security arguments within (infrastructure) governance. On the one hand, framing a security issue in a certain way is a feasible tool to justify certain activities. On the other hand, framing something *as* a security issue can justify extraordinary measures that would otherwise be deemed undesirable. What partly constitutes the power of security arguments is the fact that they are often posed as counterfactuals [21]. Incident scenarios often show possible attacks that *could* happen, not attacks that *have* happened, and they show how these could be mitigated. In order to test the scenario, an attack and a security breach would actually need to happen which is in some sense contradictory to (functioning) security. Herley and Pieters [21] discuss the use of counterfactuals or what-if statements as security arguments as well as conditions under which this is or isn't appropriate. The point they make is that what-ifs are typically easily used to argue that something should not happen and therefore that security (of a certain type) is needed, with associated access rights.

2.2.2 Infrastructure governance

The political dimension of cybersecurity is connected to the field of Internet governance, which is concerned with shaping the structural norms and conventions of the Internet infrastructure's implementation, operation and interfaces [22], [39]. Internet governance expands beyond the work of official bodies such as the Internet Cooperation for Assigned Names and Numbers (ICANN) and includes the practices of for instance companies and users which shape the infrastructure. Standards and (technological) practices embed values in technologies/technological infrastructures. When designing what would emerge to become the world wide web, Tim Berners-Lee had in mind to create a non-hierarchical, egalitarian way for people to share, access and add to information [7]. Anybody should be able to participate without being controlled or authorized by a central authority. This vision was translated to the technological structure of the Internet's Hypertext Markup Language (HTML) and its distributive protocol structure.

Within the field of Internet governance, cybersecurity is often considered as one area of governance amongst others [13]. Our approach however looks at how cybersecurity can function as a *leverage point* for effectuating broader structural interests within governance processes.

Ongoing conflicts between cybersecurity and surveillance efforts show how security arguments and frames play out in structuring decisions. At the end of the 1990's for example, the Internet Engineering Task Force deliberated over whether or not it would include wiretapping loopholes for intelligence purposes in its technological standards [14]. It decided that it would not do so, as such loopholes presented too great a threat to information security. In the corresponding Requests For Comments, the organization justified its decision based on what they saw as their area of responsibility, namely providing information security. They stated they would not take a moral position on whether or not wiretapping was evil or necessary in society [14, p. 79].

This is interesting for our paradigm, because it shows how framing something as a security issue (i.e. 'our responsibility to provide information security requires to refrain from implementing possibilities for surveillance') justifies technological practices and decisions. Security arguments can replace (obvious) value judgments by making decisions appear as logical consequences of straight forward security requirements. Nevertheless, the IETF *had* to make a certain decision that incorporated at least a politically relevant value judgment. By not adhering to requests to design wiretapping features into Internet protocols, they decided to prioritize information security in the sense of data protection over the interests of intelligence agencies and potential merits met by governmental surveillance efforts.

A more general conflict of this kind are the crypto wars which describe conflicts between a public's right to encrypt data and law enforcement and intelligence agencies' proclaimed need to access all communications and outlaw (unbreakable) encryption. Crypto wars are an example of how value conflicts and different stakeholder interests play out with regard to ICTs [19, 30] and of how different definitions of cybersecurity are mobilized to motivate the legitimacy of different positions.

2.3 Summary

In this section we presented relevant ideas from literature on the ambiguity and political dimension of security, which we summarize as follows:

1. Stakeholders can frame security problems in different ways, including what to secure against whom;

2. Security arguments support frames in a discourse, for example by referring to incident scenarios;

3. Security arguments are translated to infrastructures by motivating or justifying practices, standards and regulations;

4. Infrastructure designs have associated access possibilities and impossibilities;

5. Access possibilities influence the possible actions of stakeholders, as well as future security discourses;

6. The design, organization and practices of infrastructures incorporate normative dimensions.

Based on the literature and the concepts presented in this section, we propose a novel paradigm which systematically studies cybersecurity as a *Politikum*. In the next section, we outline our vision for this paradigm.

3. THE NEW PARADIGM

The starting point for developing the new paradigm of *security as a Politikum* is the hypothesis that security, rather than being a well-defined term, is an (essentially) ambiguous and at times contested concept. Depending on how it is used, by whom and in which context, security may mean very different things and imply very different activities or practices. Beneath every use of the term security and the practices or activities related to or implied by it, there are a number of assumptions or decisions which need to be made. Many of these assumptions can be described within the threat model that characterizes a particular security approach. This contingency and ambiguity of security opens it up to political debate, as security measures do not follow from straightforward security challenges but are the result of contestable decisions with potentially impactful consequences for how the network or infrastructure is governed and operated.

In this section, we present the core concepts and main arguments upon which our new paradigm is built and we discuss its main contributions to cybersecurity research, policy and practice.

3.1 Foundations for a new paradigm

In this subsection we discuss the is-ought divide and its importance for security arguments and discourses, the role the framing of security plays in our paradigm, and the significance of the threat models which underlie security approaches. These assumptions and core concepts build the foundations for the new paradigm.

3.1.1 Separating the 'is' from the 'ought'

A distinction important for understanding the political dimension of cybersecurity is the distinction between the 'is' and the 'ought'. 'Is' statements refer to descriptive statements about *present* state of affairs or circumstances; 'ought' statements refer to prescriptive statements about how things *should* be (in the future). Sometimes it can be challenging to unambiguously articulate whether one will be studying the 'is', so for example how security stakeholders actually make decisions, or the 'ought', so how they for example *should* make these decisions. When researching the effectiveness of security controls for instance, does one want to study effectiveness of measures and decisions based on the actually applied risk metrics (the 'is')? Or is one interested in how security controls should be set up and in how a possibly 'better' risk metrics could be created (the 'ought')?

Many security arguments are about *future* events we would like to *prevent* from happening. Most descriptive statements in the field of security are then about existing threats or about past security failures; at times, they might also be about unsuccessful or mitigated 'attacks'. Apart from these clearly descriptive statements, so these statements which describe what can be or has actually been observed, there are also those statements which describe *potential* threats. These statements are especially intriguing for our paradigm, because they are presented as hypotheticals [21]. This means they describe the potential behavior that *could* be carried out by a conceived adversary. In reaction to such a potential threat, security measures aim to create architectures and practices which *prevent* the potential adversary from (successfully) carrying out its anticipated behavior.

Testing the validity of the threat model which is proposed in a hypothetical security statement is empirically easy only where the security measure fails and a proposed adversary succeeds in its behavior. But where security measures appear as 'successful', nothing can be observed and hence it can be difficult to validate the threat model against empirical data. When in case of success we cannot empirically or factually test the (threat) assumptions upon which security decisions rest, we are required to have a special kind of trust in decision makers.

Our paradigm focuses on studying the *is*, so how security is actually being discussed and by whom, and how security decisions are (presently) made. While we do not provide answers for how this *should* be done, the insights generated by the paradigm provide a knowledge basis for making more informed and transparent security decisions in the future.

3.1.2 Framing of security

In our approach to studying discussions and decisions, framing plays a central role. For security as a *Politikum*, framing is relevant in two intertwined ways. On the one hand, there is the question of *how* security is framed: there, security is the content that is situated within a certain frame. On the other hand, there is the question of framing something *as* a security issue: here, different content is positioned within a security frame. Our paradigm studies both aspects: how security is being discussed and put forward and how security decisions are structured as a consequence of framing. We investigate the effects of how security concerns are presented and how certain actions or issues are framed as matters of security.

Our paradigm accepts that there is no one clear definition of security, or right approach to security, or a unique feature that makes something a security issue. Rather the term security can refer to "a set of family resemblances" in the same way that it has been argued to be the case with privacy [34, p. 756]. This means what gets conceptualized or framed as a security issue relates to other security issues through a myriad of complicated relationships. A security issue may share some features with certain other security issues, but not necessarily all. Security issues resemble each other in their structure as they are about systems, threats and prevention. But they can differ in their underlying assumptions and threat models as well as their implications for technological or infrastructural practices. Such a dif-

ference can be seen in the case of national security versus information security.

The ambiguity of security enables the strategic use of security arguments within political discourses. When we think about the case of voting for instance, the electoral advantage lies in facilitating the electorate that supports one's own party. So if there would be a reason to support extra security measures in districts that support a different party, which in turn would require from the voters more effort, security could be an interesting argument to try and tilt the vote. In the US there has been a vivid discussion on which type of identification voters are required to provide. It has been argued that requiring a photo ID discriminates against minorities and poor people, since many lack adequate identification [42]. In North Dakota, a stricter law for voter identification-cards has reportedly been barred on the grounds that it would exclude many Native Americans, traditionally Democratic voters, from exercising their right to vote [43].

The debate over the voter ID issue presents one example of how security can be one of several alternative frames for talking about an issue [11]. The proponents of stricter voter ID laws, which would require voters to identify themselves with an ID that includes a photograph and address, frame the issue within security terms and claim these laws are needed in order to prevent voter's fraud. The opponents of these laws on the other hand do not buy into this frame – to them, imposing stricter voting laws is a way to keep certain people – traditionally Democratic voters – from exercising their right to vote. Hence, the opponents do not frame the voter ID issue as a security issue but as an issue of fairness and constitutional rights. The voting example illustrates how, within the context of cybersecurity as a *Politikum*, the question of *who* puts forward a security argument can appear of interest. This also introduces an element of trust relevant to any security decision: when security measures are proposed and appear successful, this requires us to trust these were really necessary and proposed out of genuine security interest.

3.1.3 Threat models

The assumption that there is no one definition or feature of security opens up a reading of security issues as being proposed within certain frames. Frames describe a particular conception of reality which is accompanied by underlying system assumptions and threat models. Different actors or stakeholders can mean different things when referring to security, because they view issues through their own frame that is shaped by their expertise, concerns and interests.

The questions Baldwin identified can be transferred to cybersecurity. They present an interesting conceptual foundation for further specifying framing in the security *Politikum*. It is significant to look at who is interested in the protection of something, what it is they want to protect and against whom. For example, who should (not) have access to which data or systems and for what reasons? Within the field of cybersecurity we understand the process of answering such questions as threat modeling (in conjunction with other processes such as modeling attack scenarios). For any security issue we aim to tackle, we need to, either implicitly or explicitly, decide on a number of questions, namely who is going to attack which system, for what reasons and how. The way we devise our threat models has implications for *how we respond to a perceived security threat.*

The defined way of responding to a perceived security threat has implications for how an ICT infrastructure is governed and operated. Therefore, looking at the underlying threat models of different security approaches is a good starting point for studying cybersecurity as a *Politikum.* To illustrate we can once again consider the dichotomy between computer security and national security. A major difference between the two approaches can be found in their different threat models. Computer and network security aim to protect an ICT network and its devices from cyber-intrusions from the outside; national security aims to exploit weakness of computer and network security in order to surveil and infiltrate target devices for its mission to protect a state or its public. The two securities have different meanings, protect against different threats and their means require opposing features of technology.

3.2 Security shapes infrastructures

In this subsection we discuss how our paradigm handles the role of specific cybersecurity frames and arguments in infrastructure governance. The key idea is that frames and arguments can shape the way the infrastructure is operated. Proposed security arguments and solutions can define a specific infrastructure and its operational practices. In many cases, these practices impact on other non-security related aspects of the infrastructure. Because security arguments are connected to other values and aspects, they can be used strategically. For example, they can offer reasons for accessing data and performing surveillance or for advocating both open and closed source software.

3.2.1 Security and the operation of infrastructures

When something is framed as a security issue, it can motivate actions which have structural impacts on an ICT infrastructure. Within governance processes, cybersecurity arguments can justify certain actions and practices which have effects on the overall infrastructure and can further or counter other, non-security related aspects. Because the *exact way* in which security issues and responses are framed shapes what happens and which measures are put into place, and because these measures in turn shape the infrastructure and its standards of implementation and operation, security arguments can further or restrain interests and values within infrastructure governance processes. Consequently, when we consider the infrastructural implications of different security arguments and the activities they warrant, we can develop an understanding of how security arguments can interfere with or impact on other values and infrastructural aspects and how they could even be used to achieve other non-security related interests. Understanding the structural function of cybersecurity arguments for shaping an infrastructure and its operation offers us insights into the political dimension of cybersecurity and supports us in navigating a politicized field.

Since there are many different approaches to security and many different kinds of solutions, any actual infrastructure put in place and any specific measures that address cybersecurity appear as the outcome of negotiations between different stakeholders and points of view. This negotiation can be carried out through discourse but also through technological means. In any case, an emerging agreement on or

dominant understanding of cybersecurity and the practices it requires appears as the outcome of a decision making or negotiation process between different actors involved. This is unlikely to happen in a vacuum, but in interplay with existing power relations, values and interests. Potentially, negotiation processes could be used for shaping an infrastructure by putting forward specific arguments or framing security in a specific way. Therefore, the security discourse can play an important role in creating, governing and maintaining ICT infrastructures.

3.2.2 Security and the regulation of access

Security frames provide *arguments* for structuring technological practices in a specific way; these practices can then also have an impact on other non-security related aspects or interests. In explicating this thought, we build on one particular facet of security: that security is about "regulating access to assets" [23]. Security involves views on who or what a threat is and how it might operate; it also involves (implicit) views on which actions are sanctioned, allowed or tolerated and on which kind of access needs to be provided to certain authorized parties. While security is about preventing or regulating access, as the other side of the same coin, it is also about *enabling* access. Distributions of advantage and disadvantage or of cost and benefit – in a non-security related sense as well – can often crucially depend on how access is mediated.

Gaining or restricting access can be interesting for different parties or actors, also for non-security related reasons. For example, if one has access to network data, one can mine it for potentially interesting patterns and make decisions based on those. Security arguments can promote technological practices that enable or restrict access in a way that coincides with non-security related aspects or interests. For example, once a centralized infrastructural design has been chosen due to security considerations, its architecture enables authorized parties to easily obtain full access to data and collect information through a central point. This interaction between security and other interests is another element central to the *Politikum*.

Two illustrating examples of how such security arguments can connect to enabling or prohibiting access potentially useful for non-security related reasons are the debates about security & privacy and open & closed source (software). When security is framed within the field of national security, intelligence agencies are assigned the responsibility to identify and mitigate threats through mass surveillance. They are then granted unrestricted access to information that can be of advantage in non-security related contexts, such as for instance climate change conferences [40].

By making a case for security by design, security can present an argument for advocating open source software. When we have the possibility to analyze, test and debug the software code, we can evaluate the effectiveness of security measures and collectively find eventual backdoors or vulnerabilities. We can check whether promises or statements made actually hold true. However, as the Heartbleed example shows [25], there is no guarantee that even the most motivated open source community will necessarily find all vulnerabilities or potential exploits. The limited possibilities for making revenue pose a major obstacle for open source; much of the work of the open source community is voluntary. Companies which profit from closed source products on the other hand have the financial means and interests to employ full-time security professionals. Depending on the way they are framed, security arguments can potentially advocate both for open and for closed source while there are other financial or political interests involved.

3.3 Contributions

Based on the core concepts discussed above, the paradigm of cybersecurity as a *Politikum* can contribute to better governance of security and infrastructures. In particular, increasing the knowledge of the politics that is conducted in the context of cybersecurity, the associated practices could be improved for instance by increasing the possibilities for democratic control. By shedding light on the political use of security, the paradigm can help in devising security practices with awareness of how security framing impacts on infrastructure and interacts with other values.

3.3.1 Refining the security discourse

Our first contribution is to broaden and refine the security discourse. Firstly, we raise awareness for security professionals and others about how their approach to security and their understanding of it are situated within a particular frame. This frame is mediated by a conception of reality that has underlying assumptions about the system and potential adversaries and it adheres to a particular threat model. Our paradigm helps security stakeholders, researchers and practitioners to carefully examine how they articulate their approach and what its underlying assumptions and threat model are. To an extent, it also requires the justification of security choices. Explicit articulation helps to reflect upon our views and decisions concerning security. Consequently we can refine those, especially when encountering difficulties or possible problems that had been formerly hidden.

Articulating frames and assumptions encourages reflection upon decisions and point of views taken. It also enables better *communication* between researchers and/or practitioners and policy makers from different disciplinary fields and backgrounds and with different interests or opinions. When misunderstandings or dispute occur, their cause can be traced back to differing assumptions, threat models and interests. In the best case, this resolves controversies. As one can get a clearer picture of what is at the core of each security argument, a solution might be found that can satisfy everyone's concerns or at least present an acceptable compromise.

Further, raising awareness of the contingency of security and different security frames helps to get a clearer picture of what is at stake when making security decisions. Doing security is not a straightforward matter that needs to be balanced with other values, but involves itself a number of inherently normative and political decisions. How do we allocate resources, who do we make them available to and to whose protection? And how do we allocate trust? Choosing one of many different security frames is also a question of deciding who we trust and what we trust them with, so who gets access to information for example and who is responsible for our security. The proposed paradigm helps to make explicit the relevance these questions have when talking about security and making security decisions that impact on infrastructural practices.

3.3.2 Increased transparency

A refined and better articulated security discourse can increase transparency and precision of security decision making. It allows us to a) reflect on our threat model and the underlying assumptions, b) to examine on other non-security related implications and c) to confront and make sense of other (opposing) opinions. This makes it more difficult to make decisions 'under the table' and present decided-upon measures as necessary consequences of a straightforward account of security (remember the is-ought divide here). Instead it is now possible to analyze how a security argument is framed and to trace back (implemented) security measures and their consequences to conceptual and political decisions made.

Transparency and traceability of security decisions also enhances public debate and supports democratization of decision making on security matters. By being conscious and articulate about security and its framing, more nuanced views on security issues and arguments can be developed and strongly biased frames can be identified and counterbalanced. The assumptions made and the threat models promoted are checked upon and debated and citizens get the chance to figure out whether they agree to or support them. Finally, possible consequences of security decisions are better explicated and evaluated, especially in terms of their effects on non-security related aspects and interests.

3.3.3 Responsibility & traceability

Our paradigm allows us to better understand how security decisions relate to or impact on other values or responsibilities, such as privacy, openness or decentralization. By looking at the assumptions and implications of different security approaches, we can identify potential conflicts or negative interference and trace them back to their point of origin. For instance, issues of cybersecurity might conflict with values such as interchangeability, openness and efficiency. In our paradigm this conflict can be traced back to the assumptions that underlie a security concern or solution. We can then discover new ways to think about security or open up choices to deal with conflicts in a constructive manner. Considering the broader infrastructural context and the non-security related implications of security concerns and solutions provides a basis for figuring out early on where things could 'go wrong' or have undesired consequences.

Making assumptions, choices and implications more explicit and systematic creates a more complete understanding of the implications of security decisions, allowing us to trace the effects of such decisions. When researching the contextual function of security as a *Politikum*, it is important to look at the broader discourse, to look not only at what is said, but also by whom and how and in which context and to analyze thoroughly the technologies, technological systems and practices referred to, created and sustained. This helps us to document how different actors and their use of security arguments shape infrastructures in order to attribute responsibility.

3.3.4 Out-of-the-box security thinking

Finally, our paradigm facilitates out-of-the-box security thinking and innovative approaches to security. By thinking in frames and understanding their implications, threat models and system presuppositions, we become more fully aware of the range of possible approaches to security. To reflect on one's assumptions and enter a constructive negotiation with differing or opposing views challenges one's own perspective or paradigm and may create new security perspectives or solutions. By studying different views, we become more flexible and adaptive in our solutions, in particular when it comes to accommodating different stakeholder values. This helps to switch paradigms when encountering (unsolvable) problems in one paradigm and/or to find solutions on another system level.

This is interesting when attempting to change the security properties of existing infrastructures, for example enabling more access for intelligence agencies or when trying to reduce those instead. In such cases, an understanding of the different framings of security and the corresponding threat models, embedded both in the arguments and infrastructural practices, provides a basis for better or more inclusive solutions where the interests of more diverse stakeholders can be heard and understood.

When aiming to reconcile privacy and (national) security for example, we can contrast the different framings and threat models and observe the paradox that a commonly proposed solution to enable mass surveillance, i.e. backdoors, may also decrease security/privacy against knowledgeable adversaries. In recognizing the way the (national) security issue is framed, we can open up new possibilities of tackling these security issues that are not confined to the scope of mass surveillance. In the future, it will be exciting to find out how our paradigm and its research agenda can help uncover such new possibilities.

3.4 Summary

In this section, we outlined a research paradigm for studying cybersecurity as a *Politikum*. This paradigm focuses on tracing back the frames and arguments made within security discourses and on assessing their impact for infrastructures and access possibilities. Key aspects studied under the paradigm are:

1. security frames and their underlying threat models;
2. the construction and function of security arguments;
3. the relationship between security arguments and security discourses on the one hand, and the corresponding infrastructures and their access possibilities on the other.

Main contributions of the paradigm are to:

1. refine security discourse and improve communication;
2. increase transparency in decision making;
3. make traceability of arguments possible and enhance responsibility;
4. facilitate out-of-the-box security thinking and innovative approaches.

4. A RESEARCH AGENDA

Based on the observations discussed before, we propose a new research agenda for studying cybersecurity politics and its mechanisms. First, we discuss the kinds of topics that can be studied. Second, we outline useful research methods, and finally we suggest interesting cases.

4.1 Topics

The topics that can be studied follow from the starting points of the paradigm and the variables we identified. Aspects we propose to investigate under this paradigm are:

- how different views on cybersecurity manifest themselves in ICT infrastructures;
- how they interact with other values such as interoperability;
- what role cybersecurity plays in the broader field of infrastructure governance;
- how different stakeholders frame cybersecurity differently, possibly in accordance with their other interests.

These topics call for methods that focus on uncovering security frames both from arguments in the discourse and from the design of the infrastructures themselves.

4.2 Research methodology

In order to study the new paradigm of security as a *Politikum*, we propose to make use of the methodological variety provided by the social sciences which have been grappling with similar types of questions for a long time. In particular, we suggest the methods provided by discourse analysis and infrastructure ethnography as suitable tools for studying the socio-political dimensions of cybersecurity, for studying cybersecurity as a *Politikum*.

4.2.1 Discourse analysis

Discourse analysis is a powerful tool for looking at how which arguments are put forward and responded to within the security discourse and for identifying different actors' definitions and descriptions of cybersecurity. Generally, the methodology can be used to investigate how realities are constructed by language and communication ("in 2020, 60 billion devices will be online", or "Moore's law predicts that..."), how they are judged ("complete surveillance is dangerous"), or how notions of causality are created ("security threats require that"). It studies how "language is recruited 'on site' to enact specific social activities and social identities" [18, p. 1].

All three examples given in the first part of this section indicate certain actions in the world in a more or less direct way. Even ostensibly descriptive sentences such as "security will be a major issue" or normative sentences such as "security is an important issue to consider" indirectly entail an appeal to certain actions ("we should not adopt these systems as they are too insecure" or "we should create and exercise certain security measures", etc.). By creating realities that incite certain actions and inhibit others, such language can have a performative function [5]. This applies to security arguments which postulate what *ought* to be done based on an evaluation of what *is*. The performative function of security arguments makes it interesting to frame something as a security issue and to frame it in a specific way – framing has an influence on actions that shape worldly realities.

With discourse analysis, we develop an understanding of the meaning-making process of security arguments and frames and their performative functions. We identify how security arguments are phrased and put forward, which perspective they take and which courses of action they incite that can result in infrastructures with certain properties. Next to looking at the content of *what* is said, it is important to look at contextual factors, to look for example at *how* something is said and *by whom*. This creates insights into how different actors use security arguments within the context of infrastructure governance. Discourse analysis enables us to critically analyze security arguments which establish truths about is and ought and to make security measures traceable back to arguments and contextual decisions.

4.2.2 Infrastructure ethnography

But not all aspects important for cybersecurity (practices) might be articulated in a documented discourse. Many assumptions are implicit or invisible, materiality and technology pose practical constraints and some implications are not presented or foreseen. In order to study aspects of cybersecurity which play a role in infrastructural practices but are hidden in discourse, we propose to employ the methodological toolkit of infrastructure ethnography. This method applies ethnographic tools such as document analysis, interviews and participatory observation to technological infrastructures. It aims to uncover norms, conventions and standards which structure and guide practices.

It was first proposed by Susan Leigh Star, who applied ethnographic methods to understudied information infrastructures. Her goal was to "read the invisible layers of control and access, to understand the changes in the social orderings that are brought about by information technology" [36, p. 107] and to reveal underlying organizational practices [35].

The ethnographic perspective we propose unravels the infrastructural ordering brought about by the definition and consequent application of cybersecurity measures. It allows us to research cybersecurity perspectives and approaches in a hands-on manner. How do different assumptions of how the infrastructure ought to work, of who carries what responsibility, of who adversaries and who the in- and outsiders are, play out in the way an ICT infrastructure is governed and operated? Looking at standards and practices of operation and organization helps us to understand the broader implications of security perspectives on, for instance, values like openness, interoperability or user empowerment. The infrastructure ethnography we propose is the careful observation and analysis of infrastructural practices and norms. These include rules and norms of sharing data, operating the infrastructure and addressing cybersecurity. They can be embedded more implicitly within conventional practices and modes of conduct as well as more formally in standards and regulations.

The goal of applying infrastructure ethnography to the study of cybersecurity is to study and understand the significance of cybersecurity perspectives within the practical operation of infrastructures. For example, how are cybersecurity measures decided upon and what do they imply for how the infrastructure is operated? Different aspects to be investigated include rights of access and restrictions to access, security standards and requirements for new devices, data collection, distribution, storage and processing, control over infrastructural operation and its parts, and distributions of responsibility.

4.2.3 Challenges

Although we think the combination of these methods provides an excellent starting point for studying cybersecurity

politics, research will by no means be trivial. In particular, we see the following challenges and limits (and there are probably more):

- *Identifying discourses and security arguments & frames within them.* A first challenge is to identify the discourses which are important for studying cybersecurity as a *Politikum* and to find valuable resources for their analysis. When discourses and suitable sources are identified, a lot of the methodological work will have to be done on how to identify and define different security arguments and frames within them.
- *Gaining access to valuable information.* Especially for carrying out infrastructure ethnography, it might be difficult to gain access to the needed information, as stakeholders might not be willing to share certain things or because decisions are made behind closed doors for strategic and economic reasons.
- *Identifying and attributing interests.* When we recover arguments from the discourse in texts and interviews, this does not necessarily reveal the interests behind those arguments. It can be investigated whether arguments are in line with stated or expected interests, but this does not show whether arguments are used with any particular purpose. Therefore, strategic use of security arguments is hard to define.
- *Limits to traceability and attribution.* It may not always be possible to trace features of the infrastructure back or attribute them to security arguments. There are many reasons for infrastructural features; whether a reason contributed to a decision may not always be explicit. Additionally, some features may have emerged by chance rather than by strategy.

Tackling these challenges and defining the limits of the paradigm should be part of the maturation of the study of cybersecurity politics.

4.3 Cases

In the following we present interesting areas for exploring the potential of our new security paradigm. Apart from the contributions outlined in the previous section, studying challenging cases is useful for sharpening the paradigm in terms of topics, methods and limitations. We focus on smart cities as a main case and briefly outline others.

4.3.1 Smart cities

Smart cities aim to utilize big data, crowd-sourcing and information and communication technologies to improve processes of living together in the city or of for instance energy production, distribution and consumption. There are many initiatives which aim to use new technologies for improving coordination, sustainability and user experience in the city. These projects apply so-called "Internet of Things" technology [37] to their respective urban context. For example the Amsterdam Smart City initiative [1] is an umbrella project for a diverse range of applications within the Amsterdam area such as elderly care, transportation, energy consumption, heating, water management, innovation and more. In Chicago, the *Array of Things* initiative is setting up sensors around the city which are meant for improving sustainability and safety [2]. And in South Korea, the Songdo International Business District is the first city built 'smart' completely from scratch. Everything in the district is equipped with sensors and processed and coordinated by ICT systems; everyone's movements and activities are tracked via their phone [3, 33].

Cybersecurity challenges for smart cities.

The security issues smart city structures pose are manifold. There are issues of fraud and theft which can be directed against companies by the users manipulating data. There is also a risk of criminals being able to read data and interfere useful information for burglaries, such as whether the inhabitants of a house are on holiday. There are security issues concerning public and national security as such new systems offer a new surface for cyberwarfare and cyberattacks against critical infrastructures. Moreover, newly connected devices and technologies can pose dangers to individual people's safety. A recent smart car hack has made us conscious of the security risks smart devices pose, especially when limited security safeguards are implemented [20].

Cybersecurity arguments in smart city governance.

How issues of cybersecurity will be framed within the smart city context and which measures will be implemented depends on the specific security issues addressed and on the solutions proposed. The protection against fraud and energy theft could present an argument for more access to data (infrastructures) for companies and other third parties such as law enforcement and for a centralized data infrastructure. On the other hand, the protection against privacy invasions, surveillance and other hacks could present an argument for encrypting and protecting data from third parties or for installing a decentralized/distributed data infrastructure.

When studying smart cities from the *Politikum* paradigm, the framing of cybersecurity within the smart city context and the different security arguments used can be investigated via an analysis of the discourse. An example of how a security discourse may shape an infrastructure, in this case a smart grid infrastructure, is the ongoing discussion regarding the storage and management of smart meter data [38]. Within data-centered smart grid services and business models, having a central role in the storage of and access management to smart meter data provides additional leverage with respect to other stakeholders. So there exists an incentive for stakeholders to demand control over/access to this data. A recent arguement which was put forward within a security frame for example advocated for a more prominent role of Distribution System Operators (DSOs) in smart meter data management and storage: "third parties may not be completely reliable when it comes to privacy and security issues" [38, p. 28]. Here it is interesting to notice that while the proposed solution is presented as a (necessary) security requirement, there could also be different options to consider such as a third party central data hub or (decentralized) third party data access managers [38].

On the flip side, how a smart infrastructure is configured technologically also influences how security is framed. In their article on *Device Democracy*, Brody and Pureswaran for example envision a decentralized future for the Internet of Things, mediated by blockchain technology [9]. When the authors formulate their security concerns, their arguments and solutions are shaped by their infrastructural vision: "Current security models based on closed source ap-

proaches (often described as "security through obscurity") are obsolete and must be replaced by a newer approach – security through transparency. For this, a shift to open source is required. And while open source systems may still be vulnerable to accidents and exploitable weaknesses, they are less susceptible to government and other targeted intrusion, for which home automation, connected cars and the plethora of other connected devices present plenty of opportunities" [9, p. 5].

4.3.2 Other cases

Next to smart cities, we find several other instances of cybersecurity politics would be worthy to study as well. We discuss a few of those briefly here, based on our initial discussions, without claiming to be exhaustive.

E-democracy.

The realm of voting technologies has been extensively politicized [31]. Although the democratic goal of organizing elections appears to be that any citizen can vote, attempts to make some more equal than others are widespread. Stakeholders (such as political parties) have tried to get their interests embedded in technologies and regulations, advantaging their own supporters. This means that, inevitably, security arguments have been used for such purposes as well. Even the discussion around the introduction of the secret ballot (a technology to replace oral voting) was fraught with security arguments [29].

It can therefore be expected that in future initiatives to organize democracy technologically, cybersecurity politics will play a role. Discussions will take place on who gets access to which services, who might misuse such services and therefore needs to be excluded, which discussions need to be moderated, etc.

In particular, e-democracy initiatives provide a good case study for cybersecurity as a *Politikum*, because the interests of certain stakeholders are rather obvious (the parties or candidates). Therefore, if previous voting patterns are known, it is rather easy to link security arguments of these stakeholders to their (objective, public) interests. This makes it possible to connect not only infrastructures with arguments, but also arguments with interests.

Open data.

More and more initiatives pop up to make data of governments and companies publicly available. Rather than keeping the data for oneself, the idea is that in the end the benefit will be higher if the data is freely available for research and innovative services. At the same time, worries arise about what persons with bad intentions might do with such data. Even anonymized data could be traced back to individual persons, violating privacy and enabling the profiling of these individuals. Potentially sensitive map data may provide additional information to terrorists for planning attacks. Again, different framings of the contribution of open data to security are possible. At the same time, there are possibilities for making the data less 'open', thereby excluding access possibilities if the associated framings of security are successful. We therefore expect some security politics happening in this domain. Again, the paradigm outlined here can enable tracing of the final infrastructures to the arguments put forward in the discourse.

Privacy of free services.

There is already significant debate over the extent to which free online services do or do not do sufficiently safeguard user privacy. As the business model of such services involves use of data, for advertisements or otherwise, the service providers clearly have intentions to protect their own access. At the same time, the public demands security and privacy protection. It is interesting to study the response of the service providers to such demands. For example, to what extent do service providers respond to requests for more security/privacy with proposals that leave their own access untouched? To what extent are those arguments accepted by other stakeholders?

5. CONCLUSION

In this paper we have outlined the importance of research on the political dimension of cybersecurity. We discussed how cybersecurity can be understood as an ambiguous and contested concept that is prone to framing processes. Because security arguments can shape infrastructural practices and influence how an infrastructure is operated, processes of security framing play a role in infrastructure governance. Depending on how cybersecurity is framed, access and control rights are allocated differently within the infrastructure and granted to different stakeholders. These rights can relate also to other, non-security related interests and values. Hence security arguments can have a political function in the broader governance processes by which a technological infrastructure is shaped. Consequently, as illustrated in Figure 1, our paradigm consists of three major elements for study: the security arguments and discourses where security is framed, the infrastructures and systems shaped by security arguments and the practices deduced from them, and the distribution of access and control consequently put into place.

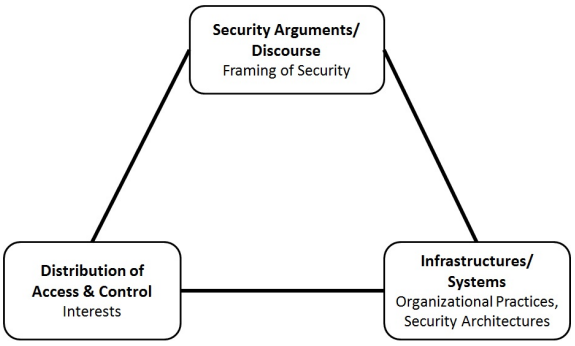

Figure 1: Paradigm Overview

In our paper, we have presented relevant conceptual work on the political dimension of cybersecurity and drafted a paradigm for studying cybersecurity as a *Politikum*. We proposed a research agenda for the systematic study of this paradigm. The paradigm is of particular importance with regard to ongoing and reoccurring discussions on who needs what access to which infrastructures (for security purposes) and who shouldn't have what access for the same (so security-related) reasons.

In the future, we will investigate cybersecurity under the paradigm more extensively, especially with regards to smart cities. We are interested in hearing about parallel studies and other cases.

Acknowledgments

The authors wish to thank Elizabeth Stobert for helpful comments. This research has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement ICT-318003 (TRE$_S$PASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.

6. REFERENCES

[1] Amsterdam smart city. Available online at: http://amsterdamsmartcity.com. Accessed on 29 April 2016.

[2] Array of things. Available online at: https://arrayofthings.github.io/. Accessed on 29 April 2016.

[3] Songdo international business district. Available online at: http://songdoibd.com/. Accessed on 29 April 2016.

[4] D. A. Baldwin. The concept of security. *Review of International Studies*, 23(1):5–26, 1997.

[5] T. Balzacq. The three faces of securitization: Political agency, audience and context. *European Journal of International Relations*, 11(2):171–201, 2005.

[6] G. Bateson. *Steps to an ecology of mind: Collected essays in anthropology, psychiatry, evolution, and epistemology*. University of Chicago Press, Chicago, IL, 1972.

[7] T. Berners-Lee and M. Fischetti. *Weaving the web: The original design and ultimate destiny of the World Wide Web by its inventor*. HarperSanFrancisco, New York, NY, 1999.

[8] A. Breeden. France seeks to extend state of emergency despite protests. *The New York Times*, Feb 2016. Retrieved from http://www.nytimes.com/2016/02/04/world/europe/france-state-of-emergency-paris-attacks.html.

[9] P. Brody and V. Pureswaran. Device democracy: Saving the future of the internet of things. *IBM Institute for Business Value Executive Report*, 09 2014.

[10] B. Buzan, O. Wæver, and J. de Wilde. *Security: A New Framework for Analysis*. Lynne Rienner Publishers, Boulder, CO, 1998.

[11] S. Childress. Could the 2016 election settle the voter id debate? *Frontline*, Jan 2016. Retrieved from http://www.pbs.org/wgbh/frontline/article/could-the-2016-election-settle-the-voter-id-debate/.

[12] D. Chong and J. N. Druckman. Framing theory. *Annu. Rev. Polit. Sci.*, 10:103–126, 2007.

[13] L. DeNardis. The emerging field of internet governance. In W. H. Dutton, editor, *The Oxford Handbook of Internet Studies*, pages 555–575. Oxford University Press, Oxford, 2013.

[14] L. DeNardis. The internet design tension between surveillance and security. *Annals of the History of Computing, IEEE*, 37(2):72–83, 2015.

[15] M. Dunn Cavelty. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1):105–122, 2013.

[16] R. M. Entman. Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4):51–58, 1993.

[17] W. A. Gamson, D. Croteau, W. Hoynes, and T. Sasson. Media images and the social construction of reality. *Annual Review of Sociology*, 18:373–393, 1992.

[18] J. P. Gee. *An introduction to discourse analysis: Theory and method*. Psychology Press, New York, NY, 2005.

[19] A. Greenberg. The father of online anonymity has a plan to end the crypto war. *Wired*, Jan 2016. Retrieved from https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/.

[20] A. Greenberg. Hackers remotely kill a jeep on the highway – with me in it. *Wired*, July 2015. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[21] C. Herley and W. Pieters. "If you were attacked, you'd be sorry": Counterfactuals as security arguments. In *Proceedings of the 2015 New Security Paradigms Workshop*, NSPW '15, pages 112–123, New York, NY, USA, 2015. ACM.

[22] J. Hofmann, C. Katzenbach, and K. Gollatz. Between coordination and regulation: Conceptualizing governance in internet governance. *New Media & Society*, 03 2014.

[23] B. Jacobs. De computer de wet gesteld. Inaugural speech, Katholieke Universiteit Nijmegen, 2003.

[24] X. Kurowska. Solana milieu: Framing security policy. *Perspectives on European Politics and Society*, 10(4):523–540, 2009.

[25] J. Lyne. Heartbeat heartbleed bug breaks worldwide internet security again (and yahoo). *Forbes*, Apr 2014. Retrieved from http://www.forbes.com/sites/jameslyne/2014/04/08/heartbeat-heartbleed-bug-breaks-worldwide-internet-security-again-and-yahoo/#7948d9d9e572

[26] D. S. Meyer. Framing national security: Elite public discourse on nuclear weapons during the cold war. *Political Communication*, 12(2):173–192, 1995.

[27] D. Mutimer. *The weapons state: proliferation and the framing of security*. Lynne Rienner Publishers, Boulder, CO, 2000.

[28] H. Nissenbaum. Where computer security meets national security. *Ethics and Information Technology*, 7(61):61–73, 2005.

[29] J. Park. England's controversy over the secret ballot. *Political Science Quarterly*, 46(1):51–86, March 1931.

[30] R. Price. There's a huge debate over an encryption expert's plan solve the problem of online privacy. *Business Insider*, Jan 2016. Retrieved from http://uk.businessinsider.com/david-chaum-privategrity-proposal-furious-debate-privacy-cryptography-privacy-cmix-2016-1.

[31] R. G. Saltman. *The history and politics of voting technology*. Palgrave Macmillan, New York, NY, 2006.

[32] W. Sanders. Quantitative security metrics: Unattainable holy grail or a vital breakthrough within our reach? *Security & Privacy, IEEE*, 12(2):67–69, Mar 2014.

[33] R. Sennett. Noone likes a city that's too smart. *The Guardian*, Dec 2012. Retrieved from http://www.theguardian.com/commentisfree/2012/dec/04/smart-city-rio-songdo-masdar.

[34] D. J. Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego Law Review*, 44:745–772, 2007.

[35] S. L. Star. The ethnography of infrastructure. *American Behavioral Scientist*, 43(3):377–391, 1999.

[36] S. L. Star. Infrastructure and ethnographic practice: Working on the fringes. *Scandinavian Journal of Information Systems*, 14(2):6, 2002.

[37] International Telecommunication Union. Internet of things global standards initiative. Available online at: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx. Accessed on 29 April 2016.

[38] P. Van den Oosterkamp, P. Koutstaal, A. Van der Welle, J. De Joode, J. Lenstra, K. Van Hussen, and R. Haffner. The role of DSOs in a smart grid environment. *Report for the European Commission's Directorate–General for Energy*, 04 2014. Retrieved from http://ec.europa.eu/energy/sites/ener/files/documents/20140423_dso_smartgrid.pdf.

[39] M. Van Eeten and M. Mueller. Where is the governance in internet governance? *New Media & Society*, 15(5):720–736, 2012.

[40] J. Vidal and S. Goldenberg. Snowden revelations of nsa spying on copenhagen climate talks spark anger. *The Guardian*, Jan 2014. Retrieved from https://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spying-copenhagen-climate-talks

[41] Wetenschappelijke Raad voor het Regeringsbeleid. *Onzekere veiligheid: Verantwoordelijkheden voor fysieke veiligheid*. Amsterdam University Press, Amsterdam, 2008.

[42] P. J. Weber. Texas agrees to weaken voter id law for november elections. *The Dallas Morning News*, 08 2016. Retrieved from http://www.dallasnews.com/news/politics/headlines/20160803-texas-agrees-to-weaken-voter-id-law-for-november-elections.ece.

[43] M. Wines. Federal judge bars north dakota from enforcing restrictive voter id law. *The New York Times*, 08 2016. Retrieved from http://www.nytimes.com/2016/08/02/us/north-dakota-voter-identification-law.html?_r=0.

[44] J. Wolff. What we talk about when we talk about cybersecurity: Security in internet governance debates. *Internet Policy Review*, 5(3), 2016.