 DOI: 10.17951/ms.2018.2.125-139

LINDA MONSEES

Cluster of Excellence 'Normative Orders', Goethe University Frankfurt

monsees@normativeorders.net

Encryption as a Security Technology. Notes on the German Debate on encryption, Uncertainty and Risk

Abstract. This article contributes to the emerging literature on digital encryption as a political issue by focusing on the way in which debates about encryption are embedded in a broader security discourse. Drawing on empirical material from Germany, this article shows how debates on encryption bring its ambiguous nature to the fore. Encryption is seen as both a threat and a source of protection, it thus becomes clear that technology only acquires its political meaning in discourse. Furthermore, I show that security is discussed in terms of uncertainty, risks and complexity. The article concludes by arguing that this prevailing idea of security as risk leads to security measures that attempt to deal with complexity by involving a variety of actors, making multi-stakeholder approaches as a solution more plausible.

1. Introduction: Encryption as Political Technology

Encryption technology is considered to be a core technology, not only for privacy and prevention of surveillance but also for security in general. Encryption can prevent access by third parties to communications and is thus crucial for e-commerce (Hosein 2017; Diffie, Landau 1998). Today, encryption is implemented in any networked technology. Even more so, encryption is a highly political technology. It ensures private communication by preventing unwelcome third-party access, increasing the degree of anonymity and thus allowing secure communication for everybody. But this means that it also allows secure communication for criminals, potentially preventing law-enforcement from accessing digital communication. The debate about encryption is deeply embedded in debates about privacy and the freedom of speech, in short: democracy. After the revelations by Edward Snowden, the question about the value of encryption attracted new attention (Meinrath, Vitka 2014; Schulze 2017) after a previous decline in public attention. I focus on this part of the debate that has emerged since 2013.

Scholarship on these most recent debates is only beginning to emerge and comes from a variety of disciplines. Interest in the topic is not limited to computer scien-

tists, as the political character of the debates is seen by commentators from all kinds of fields (Schneier 2013; DuPont 2015; Froomkin 1995; Gürses, Kundnani, Hoboken 2016). I expand on this research by taking an explicit interest in encryption as a security issue. This paper uses insights from the field of Critical Security Studies (CSS) to understand how encryption is located within a broader security discourse. Much research has focused on the US, but this article concentrates specifically on Germany given that it provides a contrast to the United States for several reasons. Firstly, Germany is a country traditionally very concerned with privacy (at least as its self-perception) and the assumption is thus that encryption is debated in more positive terms than in the US. Secondly, Germany is one of the main producers of encryption software. Strong encryption regulation in the US would be an asset for the German economy and its development of encryption. This is important, since claims for higher regulation are made, even though regulation would only be truly effective if successfully implemented in all countries. Political effort to regulate the export of encryption or implementing weaker encryption is thus less discussed than debates occurring in the US during the 1990s (Diffie, Landau 1998; Schulze 2017; Steiger, Schünemann, Dimmroth 2017).

The article proceeds as follows: in the next section I discuss how CSS has tried to conceptualize the security practices that emerge in relation to new networked technology. I then continue with some brief remarks on my methodology and methods. In the main section, I present my results from the discourse analysis. Two issues are core here: firstly, encryption is embedded in security discourse in an ambivalent way. It is considered to be both a threat and a means of protection. Secondly, encryption security is characterized by decentralization, uncertainty and unpredictability. Therefore encryption security can thus be said to follow a logic of risk having distinct implications for security policies. The conclusion summarizes the results and highlights the implication for our understanding of governing encryption as a security issue.

2. Security Technology

Security Studies, a sub-field of International Relations, is traditionally concerned with understanding security politics between states (Waltz 2010). This research focuses on issues such as war and foreign policy. However, the vibrant field of Critical Security Studies that emerged in the 1970s broadened its research agenda by including other security phenomena such as migration or health security (Buzan and Hansen 2009). For our discussion on encryption, two conceptual insights are important.

Firstly, researchers have shown that security practices enter everyday life and can be found in multiple places (Lyon 2003; Bigo 2012; Gaufman 2017). Security practices are no longer limited to high politics, but impact everyday activities and are both diffuse and decentered (Huysmans 2014; 2011). Analyzing security politics thus not only means

inquiring about war and foreign policy but also how it impacts the everyday life of citizens (Stevens and Vaughan-Williams 2017). Especially feminist scholars have shown how security politics is enacted in everyday practice and impacts the most vulnerable people. War is thus not only something that happens between states in an abstract way, but in order to understand war one needs to look at the ground level and scrutinize the everyday life of women and children, too (Nordstrom 1997; Wibben 2016).

In line with the focus on diffuse security practices, researchers have identified how (in)security is conceptualized in terms of uncertainty. When looking at security in practice, one cannot conceptually constrain security to high-politics and phenomena such as war. New security phenomena have thus often been described by a logic of risk. The emergence of uncertainty rather than the presence of a logic of deterrence is often linked with the end of the Cold War. New security phenomena such as terrorism or environmental security have emerged, and in this context it is difficult to predict the next attack or hazard (Aradau, Van Munster 2007; Elbe 2008; Salter 2008). Although high-impact events might be rare and difficult to predict, security politics focuses on precautionary measures and *mitigating* risks (Beck 1986). This diffusion of security practices has been described using terminology that focuses on (incalculable) risks, uncertainty and precaution (Kessler and Daase 2008).

In a somewhat simplistic way one could thus say that security practices follow either a logic of risk or a logic of high politics (cf. Balzacq 2015). This should serve more as a heuristic rather than a precise description, since previous research has shown that both logics are often entangled. However, this idea of security politics as being diffuse and characterized by ever-present risks serves as a foil in Section 4.1 in order to tease out the underlying assumption of the encryption security discourse. I demonstrate how themes known from previous risk-research play out when describing encryption as a security issue.

Secondly, the pervasiveness of surveillance practices and new technologies for warfare show how networked technology alters security practices. Research over the past decade has scrutinized how security technology helps not only with the diffusion of security practices, security technology is also often highly contested and security debates revolve around specific technical questions, such as the design of body scanners or the origin of missiles (Schouten 2014; Walters 2014). As a result CSS is paying increasing attention to security technology. This meant a broadening of the research agenda in terms of its theoretical resources by engaging with the theories of science and technology studies (STS), most prominently here the actor-network-theory (ANT) as developed by Bruno Latour, Annemarie Mol, John Law and Michel Callon (Latour 1999; Callon 1984; Mol 2010). It also means expanding the object of research, focusing on technologies and security devices like drones or biometrics (Leander 2013; Jacobsen 2015).

Encryption technology has so far not been granted much attention within CSS (but see: Dunn Cavelty 2007). However it is a crucial technology for internet security

as a whole. Even more so encryption plays a crucial role in debates about surveillance and privacy, which are both essential topics for CSS (Amoore 2014; Bauman et al. 2014). Researching encryption as a security technology will thus also contribute to how security is linked to debates on privacy via surveillance. As I demonstrate below, encryption is firmly embedded in the broader discourse on security, surveillance and privacy. Regulating security practices thus also means making decisions concerning the control of security technologies such as encryption. More specific questions, like key-length, are open for contestation (Monsees 2017). Understanding security politics thus also means understanding its underlying security technology. However, when looking at encryption technology we can also see that values such as privacy and freedom are debated as well. Thus we need to pay attention to both the technology itself and the values attached to it (cf. Barry 2012).

Understanding how certain ideas and values are negotiated requires a distinct approach that not only examines the material features of the technology but also the wider context in which the technology is embedded and the political debates that revolve around it. Consequently, I analyze the debates about encryption and security and in the next section I explicate this choice and the selection of material in more detail.

3. Methodology

This section presents the methodology and methods underlying this research. The aim of this article is to understand the way in which encryption is presented as a security issue. This requires less of an analysis of the technological features and more an understanding of how actors on the level of practice present encryption, and how it becomes a security issue. A discourse analytical perspective provides the best tools to achieve this aim. In line with interpretative research, I am not interested in trying to access the 'real intention', as the mental state of some person (Yanow, Schwartz-Shea 2006), but rather the intersubjective meanings. Such a perspective is in line with discourse studies that exist in many varieties (Fairclough 2013; Wodak 1989; Foucault 1972). The general assumption behind discourse research is that studying discourse reveals structures of meaning that are intersubjectively shared. Studying texts reveals which knowledge resources are shared and, independently of personal beliefs, I can reconstruct the intersubjective meaning of texts (Keller 2007).

Through the analysis of discourse, often with a focus on specific linguistic features such as metaphors or narrative structures, it becomes possible to understand these structures of meaning. Again, the aim is not to ascribe specific intentions or motives to an author of a text. A discourse analysis is interested in understanding the shared knowledge that is present in a specific community. Analyzing this shared knowledge can, for example, make plausible why specific kinds of action seemed legitimate, or why other actions became less likely or completely unthinkable (Hajer 1995). Through

a textual analysis one can see which patterns of presenting encryption and security prevail. This allows me to understand which statements were possible to say and which not. Ultimately, I am able to reconstruct what kind of assumptions about security underly the discourse on encryption.

The results presented here in this article are part of a larger project which analyzed the US and German encryption discourse between 2012 and 2016 (cf. Monsees 2017). In this paper I solely focus on Germany. Since my main interest is to show how encryption was presented as a security issue in popular discourse (rather than, for instance, among cryptologists), I focused on texts published in mass media, but also included statements by politicians and experts speaking in a public setting such as in a press release for an NGO or testifying at a public hearing. The focus on the media is justified by the insight that the media discourse is of crucial importance in order to understand societal discourse. Although we live in a functionally differentiated society, media discourse is a crucial one. It can be said that the media discourse is to mediate between the different specialized discourses (Link 2013, p. 11; 2006). Analyzing mass media is one of the preferred sites for discourse analysts to discover prevailing patterns of argumentation in a society (cf. Fairclough 1995; Meier, Wedl 2014). The main part of the analysis focuses on the presentation of encryption in newspaper. Newspapers are a prime site for the analysis, as they present arguments present not in only a specialized field but make it accessible to a broader audience (Schneider 2010; Wessler et al. 2008, p. 26–28). In the newspaper I could detect patterns of argumentation stemming from popular culture or expert discourse (Link 2006). While online sources become more important, traditional newspaper are still a dominant tool for accessing news (Nossek, Adoni, Nimrod 2015). Newspaper present the arguments in an accessible way and heir arguments circulate in the broader public. In addition, I also included what I call specialized magazines, written for the general public but tailored to an audience that is interested in information technology. They thus present encryption as a security technology in accessible terms, but their coverage is often more detailed than that found in newspaper (e.g. CHIP, ComputerBILD).

To be more precise: I selected articles from June 2012 to June 2016. This included the texts published in two major German newspapers, *Süddeutsche Zeitung* and *Frankfurter Allgemeine Zeitung,* the former considered to be the more liberal and the latter the more conservative newspaper. The newspaper and magazine texts were selected with the data-bank, *factiva.* I did a rough first analysis of all remaining texts and then selected the texts for a fine-grained analysis. Another crucial source involved statements by experts at the hearing 'Digitale Agenda' at the German parliament, which took place 7 May 2014. This hearing introduced the main arguments and allowed me to gain access to the debate within Germany. Since the experts often linked technical explanations with political recommendations, it allowed me to have a sense of how experts perceived technology, and how they assessed encryption as a technology. Since the statements were quite long (about 10 pages) it allowed me to follow more

complex argumentations and assessments. These statements also formed part of the public discourse and, because of their length and detailed argumentation, they provided excellent sources for this project. In addition, I added texts by activists, choosing the main actors that are relevant to the debate. In Germany, these were: the Chaos Computer Club, which is not only the biggest hacker organization in Europe but also an important voice in the German debate, the activist group Netpilots (Netzpiloten) and the Crypto Group of the Society for Computer Science (Fachgruppe Krypto der Gesellschaft für Informatik). Politicians are surprisingly silent on the issue in Germany, the only longer statement that I found concerning encryption was a speech by then Interior Secretary Thomas de Maizière. The German BKA and BND (German Federal Police and German Secret Service) provided material on their homepage. In sum, I analyzed 51 texts in a fine grained way that allowed me to tease out the assumptions about security and technology underlying these texts. Using ancillary questions, I focused on the depiction of encryption, technology more general, security and the role of the main actors. These questions focused my analysis and form the base of the results presented below.

4. Encryption and Internet Security

4.1 Encryption as a Threat and a Means for Protection

When analyzing encryption as a security theme, we can see quite quickly that encryption is perceived both as a threat and as a solution for internet security. Encryption is considered to be a means for protection against surveillance, whereas too powerful encryption can also be considered to be detrimental to law-enforcement. This shows that encryption technology only acquires its meaning as a security technology in discourse. In this section, I discuss the different positions that encryption occupies in discourse. This serves as a background to understanding the way in which 'security' as a concept is discussed in the discourse on encryption – a topic to which I turn in the next section.

First, encryption is seen as a cause for higher insecurity. This way of presenting encryption is actually well known from the "CryptoWars" that took place in the US in the 1990s (Schulze 2017; Diffie, Landau 1998). These debates revolved around the question to what extent the state should be able to control the implementation of encryption systems (i.e. its key-length or the implementation of backdoors) or whether this would violate privacy rights and actually decrease security by weakening available encryption systems. The state – here the US state, especially the NSA and the FBI – presented encryption in negative terms. Encryption was considered to be harmful since it would prevent lawful interception by law-enforcement (Denning 1996). This same motive can be found in the current debates revolving around encryption (some-

times called CryptoWars 2.0, Meinrath, Vitka 2014). Schulze in his comparison of the two phases of the debate has shown how similar motives stemming from the 1990s appear again in the post-Snowden debates on encryption (Schulze 2017).

The theme of encryption as *increasing* insecurity emerged in the earlier days of the CryptoWars, but can be found today and is also present in the German debates. Encryption is depicted as potentially harmful by providing anonymity to criminals and preventing state actors gaining access to data. This theme can be illustrated by the statement by de Maizière at the German-French summit on cybersecurity:

"security administration should under strict requirements – constitutional requirements – be allowed and be capable of decrypting encrypted communication if this is necessary for their work and the protection of the population." (de Maizère 2015).

To be clear, de Maizière is keen on emphasizing the importance of privacy and the need for encrypted data for the economy. The quote above is a rare stark statement presenting encryption as a threat for security. For example, actors such as the BND or the BKA (secret service and federal police of Germany) present the increasing risks through networked technology and thus try to depict a threat-scenario that then makes stronger control of digital communication necessary. To give one example: the BND starts its discussion on cyber-security with reference to the increasing threat of espionage and the harm this does to the economy. Only in the last paragraph does the BND state that "[the BND] has the permission and the technical capabilities for the strategic capture of international data traffic" (BND 2018). This means that the BND argues for the need to access encrypted information – but does not present encryption as a threat in a straightforward way. The need to have access to all kinds of data traffic is linked with a broader concern for security in the networked world (Monsees 2017). They only implicitly consider too strong encryption that cannot be broken by law-enforcement as a problem.

However, in the German discourse the opposing view is dominant. Encryption is perceived as a means for protection and state regulation of encryption is seen as deeply problematic (Monsees 2017). Not only is encryption considered to be a corner stone for the security of the economy and especially global finance, it is also seen as an antidote to the ever-present surveillance by the state and global ICT companies. Especially after the Snowden revelations, encryption was again discussed in mass media as a possible solution against surveillance. Furthermore, activists supported the spread of encryption software in order to strengthen the privacy of citizens. The core threat is here not encryption or espionage but the increasing surveillance by secret services that are "out of control" (as activists present the threat in: Neumann 2014, Kurz/Rieger 2013). From this perspective, it is crucial that citizens use encryption in order to be secure *from* the state. This sentiment comes to the fore in the quote by the activist vollkorn from the Chaos Computer Club, who argues against current actions by the state and its secret services:

"Rather than investing millions in the digital armament *against their own population*, the CCC demands investing this money in better technological education" (vollkorn 2015, my own emphasis).

Here encryption is seen as a *source* for protection. Interestingly, security is thus not a good provided by the state, but the state itself becomes the threat. Much political thought relies on the idea that the state provides security for its citizens, but in this instance we can see that the relationship is reversed and that citizens take precautions against harmful actions by the state.

Activists and civil-society actors highlight the huge capabilities of encryption. For them, the relevance of encryption lies mostly in its ability to safeguard privacy which is understood as a fundamental right. This link is made most explicitly in a headline by the group on encryption within the German Crypto Group of the Society for Computer Science ('*Fachgruppe Krypto*'):

"Cryptography protects basic rights – especially in the era of massive espionage of data traffic on the internet". (Fachgruppe Krypto 2014).

Encryption is considered to be a very powerful tool and a corner stone for security. Security from this perspective is much more encompassing, including the notion of privacy and security from the state. Encryption thus acquires meaning as a privacy protection tool. This is the more prevailing view in Germany – not only are activists vocal there, it is also the dominant view in mass media. The main German newspaper reported quite critically about the power of secret services and global companies, and often present encryption as a way to prevent surveillance (cf. Steiger et al. 2017; Monsees 2017).

In sum, we can see that encryption acquires its meaning and status only in discourse. Encryption is discussed as both a source for and a threat to internet security; whereas internet security means security from the state or security by the state, respectively. Encryption technology as such is quite ambiguous, and how it is evaluated is decided in discursive struggles. Even though state agents wish to have more control over encryption, these claims cannot be made in a straightforward way. Even state actors have to acknowledge that strong encryption is necessary for the economy, and that the possibility of surveillance needs to be balanced by claims for privacy. The opposing view presents encryption as a tool for higher security. Encryption is crucial for protection against the state, namely illegitimate surveillance and data-retention. This short discussion indicates the ambiguous character of technology.

4.2 Uncertainty, Risk and Encryption

The previous section summarized the main position concerning encryption as a security issue. This section now looks even more closely at what kind of understandings of security are present. I focus on how 'security' is actually conceptualized by the actors and show how encryption is embedded in an understanding of (cyber-)security that

relies on the notions of risk, uncertainty and unpredictability. I structure the discussion along the three themes of uncertainty, knowledge and the role of human actors.

The first theme here is that security is understood not as an existing state of affairs, but something that can actually never be achieved. Since networked technology is so complex and consists of so many human and non-human parts, complete security is impossible. To illustrate this point, consider this example by one of the main legal experts, Nikolas Härting, on IT-security in Germany, when speaking in front of a parliamentary hearing: "*Secure communication* within the net was impossible at any time when considered realistically." (Härting 2014). The idea of secure communication via networked technology is already seen as an incorrect assumption. Härting continued to develop this issue in his statement. According to him, the structure of the internet itself is insecure. Complete security was never possible, and from that it follows that it cannot be achieved by improving just one aspect. The statement by internet security expert Sandro Gaycken at the same hearing follows the same sentiment, when he states that "systems are complex [and] IT-systems produce effects that [...] cannot be anticipated". He assumes that IT systems are no longer controllable and their properties are no longer measurable (Gaycken 2014). This idea that effects and risks are incalculable speaks to the above discussed research on risk. While traditionally the risks of an attack were considered to be calculable, the dominance of uncertainty prevents this calculation (Kessler, Daase 2008). In the discussion on encryption and security, similar patterns and ideas can be identified. Future attacks are not measurable, the impact of the next attack is not known and complete security is impossible.

The second theme concerns the limited knowledge about security. Knowledge about the 'behavior' of technology is limited, and the effect of technology is often impossible to know because of unintended consequences (on this topic see the classic account by Winner 1980). Part of the problem is that an attack can happen at any time and target any kind of object. This idea of uncertain 'behavior' by technology becomes clear in the headline by Eugene Kaspersky in a German Newspaper, which states that cyber-attacks "can hit anyone who has access to the internet." He then continues:

"Such cyber-attacks can sabotage pivotal infrastructure – water reservoirs, air traffic control or the food chain – and have catastrophic effects. Every modern infrastructure is networked to a very high degree. […] Even the attacking country can become the victim to its own weapon; it is called the boomerang-effect" (Kaspersky 2012).

The insecurity of the technology lies here in its 'boomerang-effect'. Technology is something that cannot be easily controlled – it might fail or act in an unpredictable way. Later in the same text, Kaspersky talks about the 'side-effects' of technology, again emphasizing that technology cannot be controlled. The side-effects are rather a characteristic of a networked technology that is complex and multi-layered, and thus cannot be fully secured. Because the technology is so complex and inherently insecure, rendering security is difficult. What is needed is constant adaptation – hu-

man input is crucial. This theme runs through the whole debate: since the technology is so complex and its affect unpredictable, human action is necessary.

But even when emphasizing the role of humans we run into a problem: the knowledge of experts is limited, too. Importantly, these limits are acknowledged by the actors themselves. Consider this quote by an expert speaking in 2014:

"Even crypto-experts do not know how long the current algorithms will provide protection. […] Therefore, it is necessary to inform oneself about the possibilities of exchange or for upgrades [lit.: upgrade-paths] before one (starts) using an encryption-solution" (Ries 2014).

Uncertainty as a prevailing theme thus also manifests in the depiction of expert knowledge. The value of knowledge for assessing the future is limited. Space is opened up for thinking about the role for human action and, with the emphasis on the limited knowledge of experts, where even resorting to specialists is not a straightforward option. Uncertainty thus even covers the limits of knowledge – and not only technology.

This brings us to the *third* theme: the role of humans. In a context that is characterized by uncertainty and limited knowledge, not only do we need better technological solutions, constant adaptation by humans is also necessary. A technological fix does not by default solve the complex problems. This becomes especially apparent if texts are analyzed that look closer at how encryption works. Since encryption relies heavily on mathematics, such a base is crucial for encryption to work. The following quote stems from an article that deals with encryption and internet security published in *CHIP*, a specialized magazine on IT-issues. Mathematics serves as an indicator for the potency of encryption, but at the same time the article problematizes the technology.

"According to Snowden, strong encryption offers the best tool to protect oneself against global espionage, but in the way the browser and server use HTTPS-connections, the strength of the encryption does not come into play. […] Furthermore, in PFS the session key is not sent over the internet but computed by every party – this is based on *pure maths*. If PFS is *implemented correctly*, both session keys are deleted as soon as the communication ends" (Mandau 2014, my own emphasis).

PFS refers to perfect forward secrecy, a specific kind of encryption that is supposed to offer the best security. The emphasis on the strengths of mathematics and the strong capabilities of encryption contrasts its dependency on proper implementation by humans (users) and the technological environment, which needs to work as well. Although encryption (and its mathematical base) is assigned strong abilities to increase security, all actors are aware that encryption always relies on implementation by human users. This sentiment is taken up by multiple calls to focus on the education of the user, who needs to become more knowledgeable. Thorsten Schröder a German IT-expert states that "customers must be […] educated" (Schröder 2014), and activists groups such as the Chaos Computer Club or the Electronic Frontier Foundation have been vocal in trying to educate users about surveillance and the role of encryption in providing better privacy and security. The mathematical parts of encryption are thus

weak if they are not accompanied by knowledgeable users. Complexity thus means also that mathematics, technology and a skilled end-user all have to come together to achieve higher security.

This section showed how security is conceptualized with references to complexity, risk, uncertainty and unpredictability. The analysis revealed that this is the dominant framework for cybersecurity in which encryption is discussed. This shift to a risk-paradigm in connection with highlighting the importance of not only technology but also human actors make certain security measures possible. Even though actors disagree about the assessment of encryption for security, a common reference point of complexity and uncertainty make it possible to acknowledge the role of all actors (users, governments, companies) and technology as crucial for security. Encryption only works if the technical part is accompanied by skilled users and means that allow the governing of the complexity of networked technology. Measures such as multi-stakeholder approaches or public-private-partnerships are thus more likely to come into being. Understanding that 'security' is not a simple task that can be provided by the state makes it possible to promote alternative modes of governing.

4. Conclusion: multi-stakeholderism and internet security

This article presented insights into the German public discourse on encryption. Based on a discourse analysis, this article focused on two main themes. I firstly showed the ambiguous role of encryption in the broader security discourse. Encryption is presented as both a threat and a solution for more security. Encryption is associated with two different, opposing meanings in terms of security. While too strong encryption is considered to be an obstacle for law-enforcement, encryption is also presented as the best tool to provide security *from* the state.

In building on this, I scrutinized what kind of understanding of security underlies the encryption discourse. This understanding of security in terms of uncertainty and incalculable risks is not unique to the cyber discourse. Indeed, scholars of international security have long observed this shift in a variety of fields, such as health, aviation and financial security (Rasmussen 2001; Amoore 2013; Elbe 2008; Salter 2008). Critical analyses have shown how ideas like the precautionary principle constitute a distinct form of governing security (Aradau and Van Munster 2007). In the context of encryption, references to uncertainty make it possible to discuss the role of end users, infrastructure and software as part of a complex security landscape. Encryption has a crucial role in this network since it is perceived as a crucial technology.

These insights are not only important for our understanding of encryption as a security issue as such, but they also have political implications. If security is discussed in terms of complexity, uncertainty and unpredictability, then this also has repercussions on what kind of governing practices are considered to be most effective.

Since cyber security involves all kind of actors, technologies that transgress traditional scales and cause uncertainty then the core challenge is to cope with this complexity. Approaches such as multi-stake holderism or public private partnerships become the most plausible governance mechanisms (Hofmann 2016; Carr 2016). These methods of governing are perceived to be most plausible to account for the unintentional effects of technology, the ambiguous role of encryption and the need to educate the end-user. The presentation of encryption as a security issue in the way that I described above thus makes policy approaches such as multi-stakeholder governance more plausible. Although German activists are critical about the role of companies, their insistence on the complexity of the issue plus resentment about the power of state actors (secret services) allow the discursive underpinning of security measures that give power and responsibility to a multiplicity of actors, including companies, end-users, states and NGOs. In line with the discourse theoretical tenets I described above, I am not claiming that the relationship between 'logic or risk' and 'multi-stakeholder governance' is deterministic, and I also do not clam that this is the best (or only) way to think about governing encryption. Answering this question would involve discussing who 'we' want to be responsible for increasing security and who will or should be empowered by security measures. This article is just a first step in tackling these broader questions.

References

Amoore L. (2013). *The Politics of Possibility: Risk and Security beyond Probability*. Duke University Press: Durham and London.

Amoore L. (2014). Security and the Claim to Privacy. *International Political Sociology,* vol. 8 (1), pp. 108–12.

Aradau C., Van Munster R. (2007). Governing Terrorism Through Risk: Taking Precautions, (Un) Knowing the Future. *European Journal of International Relations*, vol. 13 (1), pp. 89–115.

Balzacq T. (2015). Legitimacy and the "Logic" of Security. In T. Balzacq (Ed.). Contesting Security: Strategies and Logics. PRIO New Security Studies. Routledge: New York, pp. 1–9.

Barry A. (2012). Political Situations: Knowledge Controversies in Transnational Governance. *Critical Policy Studies,* vol. 6 (3), pp. 324–36.

Bauman, Z., Bigo, D., Esteves P., Guild E., Jabri V., Lyon D., Walker R.B.J. (2014). After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology,* vol. 8 (2), pp. 121–44.

Beck U. (1986). *Risikogesellschaft: Auf Dem Weg in Eine Andere Moderne*. Suhrkamp: Frankfurt am Main.

Bigo D. (2012). *Security, Surveillance and Democracy.* In K. Ball, K. Haggerty, D. Lyon (Eds.). *Routledge Handbook of Surveillance Studies*. Routledge: London and New York.

BND. (2018). *Bundesnachrichtendienst – Cyber-Sicherheit*. http://www.bnd.bund.de/DE/Themen/Lagebeitraege/Cyber-Sicherheit/Cyber-Sicherheit_node.html;jsessionid=DEED-619592FF2B9156149BAEA6843424.2_cid377, 01.12.2018.

Buzan B., Hansen L. (2009). *The Evolution of International Security Studies*. Cambridge University Press: New York.

Callon M. (1984). Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. *The Sociological Review,* vol. 32 (1_suppl), pp. 196–233.

Carr M. (2016). Public–Private Partnerships in National Cyber-security Strategies. *International Affairs,* vol. 92 (1), pp. 43–62.

Denning D. (1996). *The Future of Cryptography*. In *Crypto Anarchy, Cyberstates, and Pirate Utopias.* MIT Press: Cambridge, pp. 85–101.

Diffie W., Landau S. (1998). *Privacy on the Line the Politics of Wiretapping and Encryption*. MIT Press: Cambridge.

Dunn Cavelty M. (2007). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. CSS Studies in Security and International Relations. Routledge: New York.

DuPont Q. (2015). Opinion: It's Time to Rethink Polarizing Encryption Debate. *Christian Science Monitor*, vol. 2 December 2015. http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/1202/Opinion-It-s-time-to-rethink-polarizing-encryption-debate, 1.12.2018.

Elbe S. (2008). Risking Lives: AIDS, Security and Three Concepts of Risk. *Security Dialogue,* vol. 39 (2–3), pp. 177–98.

Fachgruppe für Angewandte Kryptographie in der Gesellschaft für Informatik. (2013). *Kryptographie schützt Grundrechte- gerade im Zeitalter der massenhaften Ausforschung des Datenverkehrs im Internet*, Pressemitteilung vom 16.09.2013, http://fgkrypto.gi.de/presse/nsa-ueberwachung.html, 15.11.2018.

Fairclough N. (1995). *Media Discourse*. Arnold: London.

Fairclough N. (2013). *Critical Discourse Analysis: The Critical Study of Language.* Taylor and Francis: Hoboken.

Foucault M. (1972). *The Archaeology of Knowledge,* Pantheon Books: New York.

Froomkin M. (1995). *The Metaphor Is the Key: Cryptography, The Clipper Chip, and the Constitution*. 24.06.1995. http://groups.csail.mit.edu/mac/classes/6.805/articles/froomkin-metaphor/text.html, 1.12.2018.

Gaycken S. (2014). *Öffentliches Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema ‚IT-Sicherherheit', Schriftliche Stellungnahme von Dr. Sandro Gaycken*, http://www.bundestag.de/bundestag/ausschuesse18/a23/anhoerungen/-/281524, 1.12.2018.

Gaufman E. (2017). *Security Threats and Public Perception: Digital Russia and the Ukraine Crisis*. Palgrave Macmillan: London.

Gürses S., Kundnani A., Van Hoboken J. (2016). Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy. *Media, Culture & Society*, vol. 38 (4), p.. 576–90.

Hajer M. (1995). *The Politics of Environmental Discourse: Ecological Modernization and the Policy Process*. Clarendon Press: Oxford.

Härting N. (2014). *Schriftliche Stellungnahme zum Fragenkatalog für das öffentliche Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema IT-Sicherheit am Mittwoch*, 7.05.2014, http://www.bundestag.de/bundestag/ausschuesse18/a23/anhoerungen/-/281524, 1.12.2018.

Hofmann J. (2016). Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice. *Journal of Cyber Policy,* vol. 1 (1), pp. 29–49.

Hosein G. (2017). Digital Citizenship and Surveillance| Compromising Over Technology, Security, and Privacy — Commentary. *International Journal of Communication;* Vol 11, http://ijoc.org/index.php/ijoc/article/view/6825.

Huysmans J. (2011). What's in an Act? On Security Speech Acts and Little Security Nothings. *Security Dialogue,* vol. 42 (4–5), pp. 371–83.

Huysmans J. (2014). *Security Unbound: Enacting Democratic Limits*. Critical Issues in Global Politics. Routledge: New York.

Jacobsen K. (2015). Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees. *Security Dialogue,* vol. 46 (2), pp. 144–64.

Kaspersky E. (2012). AUSSENANSICHT; Angriff aus dem Netz; Hoch entwickelte Computerviren zeigen: Viele Länderbereiten sich auf den Cyber-Krieg vor. Die Attacken können jeden treffen, der einen Internetanschluss hat. *Süddeutsche Zeitung* 12.09.2012, retrieved via factiva 12.06.2014.

Keller R. (2007). *Diskursforschung: eine Einführung für SozialwissenschaftlerInnen*. 3., aktualisierte Aufl. Qualitative Sozialforschung 14. VS, Verl. für Sozialwiss: Wiesbaden.

Kessler O., Daase C. (2008). From Insecurity to Uncertainty: Risk and the Paradox of Security Politics. *Alternatives: Global, Local, Political,* vol. 33 (2), pp. 211–32.

Kurz C., Frank R. (2013). Snowdens Maildienst gibt auf. Die neuen Krypto-Kriege. In *Frankfurter Allgemeine Zeitung* 09.08.2013 (retrieved via Factiva 12.06.2014).

Latour B. (1999). 'On Recalling ANT'. In J. Law, J. Hassard (Eds.). *Actor Network Theory and After*. Wiley: New York, pp. 15–25.

Leander A. (2013). Technological Agency in the Co-Constitution of Legal Expertise and the US Drone Program. *Leiden Journal of International Law,* vol. 26 (04), pp. 811–31.

Link J. (2006). Diskursanalyse Unter Besonderer Berücksichtigung von Interdiskurs Und Kollektivsymbolik, R. Keller, A. Hirseland, W. Schneider, W. Viehöver (Eds.). *Handbuch Sozialwissenschaftliche Diskursanalyse,* vol. 1, pp. 433–58.

Link J. (2013). Diskurs, Interdiskurs, Kollektivsymbolik. *Zeitschrift Für Diskursforschung,* vol. 1 (1), pp. 7–23.

Lyon D. (2003). 'Surveillance as Social Sorting, Computer Codes and Mobile Bodies'. In D. Lyon (Ed.). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* Routledge: New York, pp. 13–30.

Mandau M. (2014). Die abhörsichere Verschlüsselung. In *CHIP*, 01.02.2014 (retrieved via Factiva 12.06.2014.

de Maizière T. (2015). *Rede des Bundesinnenmisters beim Forum International de la Cybersécurité*, 20.01.2015, www.bmi.bund.de/SharedDocs/Reden/DE/2015/01/internationales-forum-fuer-cybersicherheit.html, 1.12.2018.

Meier S., Wedl J. (2014). *Von Der Medienvergessenheit Der Diskursanalyse*. In J. Angermuller, M. Nonhoff, E. Herschinger, F. Macgilchrist, M. Reisigl, J. Wedl, D. Wrana, A. Ziem. *Diskursforschung: Ein Interdisziplinäres Handbuch*. Transcript: Bielefeld, pp. 411–35.

Meinrath S., Vitka S. (2014). Crypto War II. *Critical Studies in Media Communication,* vol. 31 (2), pp. 123–28.

Mol A. (2010). Actor-Network Theory: Sensitive Terms and Enduring Tensions. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie. Sonderheft,* vol. 50, pp. 253–69.

Monsees L. (2017). *International Security and the Politicisation of Technology. Studying the International Political Sociology of Encryption*. PhD-thesis, University of Bremen.

Neumann L. (2014). *Effektive IT-Sicherheit fördern Stellungnahme zur 7. Sitzung des Ausschusses Digitale Agenda des Deutschen Bundestages*, http://www.bundestag.de/bundestag/ausschuesse18/a23/anhoerungen/-/281524, 1.12.2018.

Nordstrom C. (1997). *A Different Kind of War Story*. The Ethnography of Political Violence. Univ. of Pennsylvania Press: Philadelphia.

Nossek H., Adoni H., Nimrod G. (2015). Media Audiences| Is Print Really Dying? The State of Print Media Use in Europe. *International Journal of Communication,* vol. 9, p. 21.

Rasmussen M. (2001). Reflexive Security: NATO and International Risk Society. *Millennium-Journal of International Studies,* vol. 30 (2), pp. 285–309.

Ries U. (2014). *Die richtige Krypto-Software – Verschlüsselung ist Vertrauenssache*. In Computerwoche, 02.06.2014, (retrieved via factiva 12.06.2014).

Salter M. (2008). Imagining Numbers: Risk, Quantification, and Aviation Security. *Security Dialogue,* vol. 39 (2–3), pp. 243–66.

Schneider S. (2010). 'Empirische Legitimationsforschung'. *Prekäre Legitimitäten. Rechtfertigung von Herrschaft in Der Postnationalen Konstellation,* Frankfurt Am Main, pp. 45–67.

Schneier B. (2013). The NSA Is Breaking Most Encryption on the Internet. *Schneier on Security* (blog). 9.05.2013, https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html, 1.12.2018.

Schouten P. (2014). Security as Controversy: Reassembling Security at Amsterdam Airport. *Security Dialogue,* vol. 45 (1), pp. 23–42.

Schulze M. (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. *Media and Communication,* vol. 5 (1), pp. 54–62.

Schröder T. (2014). *Stellungnahme von Thorsten Schröder zum Fragenkatalog für das öffetnliche Fachgespräch des Ausschusses Digtale Agenda des Deutschen Bundestages zum Thema*, IT-Sicherherheit' am Mittwoch, 7.05.2014, http://www.bundestag.de/bundestag/ausschuesse18/a23/anhoerungen/-/281524, 1.12.2018.

Steiger S., Schünemann W., Dimmroth K. (2017). Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany. *Media and Communication,* vol. 5 (1), pp. 7–16.

Stevens D. (Daniel Peter), Vaughan-Williams N. (2017). *Everyday Security Threats: Perceptions, Experiences, and Consequences*. Manchester University Press: Manchester.

Vollkorn. (2015). *CCC fordert Ausstieg aus unverschlüsselter Kommunikation*. Press release of the CCC, 22.01..2015, https://www.ccc.de/de/updates/2015/ccc-fordert-ausstieg-aus-unverschlusselter-kommunikation, 1.12.2018.

Walters W. (2014). Drone Strikes, Dingpolitik and beyond: Furthering the Debate on Materiality and Security. *Security Dialogue*, vol. 45 (2), pp. 101–18.

Waltz K. (Ed.), (2010). *Theory of International Politics*. Waveland Press: Long Grove.

Wessler H., Peters B., Brüggemann M., Kleinen-von Königslöw K., Sifft S. (2008). *Transnationalization of Public Spheres. Transformations of the State*. Palgrave Macmillan: New York..

Wibben A. (Ed.), (2016). *Researching War: Feminist Methods, Ethics and Politics*. Routledge: New York.

Winner L. (1980). Do Artifacts Have Politics?, *Daedalus,* vol. 109 (1), pp. 121–36.

Wodak R. (1989). *Language, Power and Ideology: Studies in Political Discourse*. John Benjamins Publishing: Amsterdam.

Yanow D., Schwartz-Shea P. (Eds.), (2006). *Interpretation and Method: Empirical Research Methods and the Interpretive Turn*. Sharpe: Amonk, NY.