

Security Meets Cyberspace: The Politics of Cyber Security

Kristoffer Kjærgaard Christensen

PhD Fellow, Department of Political Science, University of Copenhagen

Tobias Liebetrau

PhD Fellow, Department of Political Science, University of Copenhagen

First draft, please do not cite or circulate without permission

ABSTRACT: Security risks linked to information and communication technology (ICT) are often condensed in the concept of cyber security. In this article we show how different theorisations of cyber security install certain politics of cyber security in accordance with usual fault lines and understandings of security in security studies. Consequently, we argue, we should be careful to readily limit cyber security to the prevailing politics of security in the literature of security studies. We need to ensure sensibility to how cyber security may also challenge the confines of this. Therefore we, first, introduce Annemarie Mol's notion of ontological politics and the idea of multiple cyber securities as a way of opening up the politics of cyber security. Second, we point to the importance of technology and technological change through a short overview of how the concept of cyber security entered the political imaginary in debates on critical infrastructure protection and ICT. Third, we engage with the meetings between security and cyberspace in the existing security studies literature on cyber security and with their implications for security politics. Finally, we discuss avenues for further research that critically engages with the implications of bringing together security and cyberspace.

Key words: Security, cyberspace, politics, ICT, STS

INTRODUCTION

Cyber security is the new buzz word of contemporary security politics. Following the rapid advance of information and communication technologies (ICT) into almost every aspect of our lives – from communication and critical infrastructure to cars, lightbulbs and refrigerators¹ – the confluence of security and cyberspace has become increasingly prevalent in both media and policy discourse. In 2016 the cyber threat was again ranked among the biggest threats in the World Wide Threat As-

¹ This integration of the internet and e.g. household appliances is also known as “the internet of things” (IoT).

assessment of the US Intelligence Community.² (Clapper 2016) Also, in his 2015 State of the Union Address President Obama stated that

‘we’re looking beyond the issues that have consumed us in the past to shape the coming century. No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. So we’re making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism’. (Obama 2015)

Cyber security is arguably “the next big thing”.

Despite its prominence in political and media discourse, cyber security has for long been somewhat neglected in the academic literature on security. Few scholars have engaged theoretically with the issue and instead the literature on cyber security has tended to be more policy-oriented and atheoretical. (Eriksson and Giacomello 2006) In recent years cyber security has, however, received more and more attention from security scholars and has seemingly gained traction within both mainstream and critical security studies. Yet, the literature on cyber security is still rather limited. Moreover, as we show in this article, the current literature approaches cyber security in accordance with the traditional fault lines of security studies, hence perpetuating the existing understandings of security. The cyber security literature is, in other words, largely new wine in old bottles.

The ways in which we theorise and make sense of cyber security are pivotal to our abilities to address and live with these issues. Therefore this knee-jerk reaction is problematic, we argue. It neglects the ways in which the meeting between security and cyberspace transforms security politics.

² Cyber threats have been the first threats to be mentioned in these reports four years in a row. This gives some indication as to the perception of its importance in the intelligence community. It is only in 2016 that the report has been accompanied with a disclaimer stating that the order in the threats in the report does not necessarily reflect their magnitude and/or importance. Moreover, this is not just an American tendency, but a common theme in most other Western countries. E.g. the Danish Defence Intelligence Service has also ranked cyber threats from individuals, groups and other states amongst the biggest threats to Denmark in recent years. (Danish Defence Intelligence Service 2012, 2013, 2014, 2015)

We run the risk of blinding ourselves to the transformative role of ICT and to the new actors and practices of security that cyber security potentially entails. This is not an argument for readily accepting the hype of cyber security but for ensuring sensibility to both the continuities and the changes of security politics in the digital age. Rather than assuming cyberspace to be merely a new arena for “old” forms of security politics, we ought to critically engage with the complex dynamics of the meeting between security and cyberspace and its implications for security politics.

In this article we show how different theorisations of cyber security install certain politics of cyber security. Consequently, we argue, we should be careful to readily limit cyber security to the prevailing politics of security in the literature of security studies. We need to ensure sensibility to how cyber security may also challenge the confines of this. Therefore we, first, introduce Annemarie Mol’s notion of ontological politics and the idea of multiple cyber *securities* as a way of opening up the politics of cyber security. Second, we point to the importance of technology and technological change through a short overview of how the concept of cyber security entered the political imaginary in debates on critical infrastructure protection. Third, we engage with the meetings between security and cyberspace in the existing security studies literature on cyber security and with their implications for security politics. Finally, we discuss avenues for further research that critically engages with the implications of bringing together security and cyberspace.

ONTOLOGICAL POLITICS OF CYBER SECURITY

Linking security with cyberspace through the concept of cyber security is, importantly, a political move. We need to seriously engage with the political implications of bringing security and ICT together. In this article we draw attention to how the nature of cyber security is not determined a priori by a particular logic of neither security nor cyberspace. We do not see them as pre-given discrete entities that are merely joint together. Rather, we argue, the two are co-constitutive and shape each other depending on how they are linked and brought into being as cyber security. It is hence important to enable sensitivity to the relationality of cyber security and to how it is brought into being through the relations of heterogeneous elements that ‘hold together *without* actually forming a

coherent whole'. (Allen 2011:154). In other words, with inspiration from philosopher Annemarie Mol (1999, 2002), we emphasise the 'ontological politics' of cyber security.

In coupling politics with ontology, Mol argues that ordering the world is an active and open-ended process. Moreover, she emphasises that this open-endedness is not just an epistemological one – it also characterises socio-material realities. She argues that 'ontology is not given in the order of things, but [...] instead ontologies are brought into being, sustained, or allowed to wither away in common day-to-day, sociomaterial practices'. (Mol 2002:6) Following from this, the ontology of cyber security is not given outside the relations and practices through which it is assembled. The reality of cyber security is always in the making and hence precarious and, potentially, unstable. (Mol 2002; Law 2009) It depends on the relational work done in, for instance, the academic literature. That is to say that the ontology of cyber security is open to contestation; in short, it is political. This shift to ontology has important implications. A good way of highlighting these is by outlining the subtle yet important difference between an ontological approach to difference and an epistemological one.³ An epistemological approach, which is common to most critical approaches, presents difference as a difference in perspectives on a singular object. Instead an ontological approach to difference suggests that it is the result of the enactment of different objects. In other words, an epistemological take on difference, on the one hand, pluralises *meanings* of reality by allowing for competing structures of meaning; a turn to ontology, on the other hand, multiplies *realities*. (Mol 1999, 2002; Law and Singleton 2005) Cyber security is hence, ontologically speaking, 'more than one – but less than many'.⁴ (Mol 2002:55)

This multiplicity can be exemplified by turning to the Danish challenges regarding public-private collaboration on cyber security. (Christensen, Lacoppidan, and Petersen 2015) One of the major

³ Mol distinguishes between 'ontological politics' and what she calls 'perspectivalism'. (Mol 1999, 2002)

⁴ In a similar vein, drawing on the mathematical concept of fractals (lines that occupy more dimensions than one but less than two), John Law (2002:3) suggests the possibility of fractal coherences 'that cannot be caught within or reduced to a single dimension. But neither do they exist as coherences in two or three separate and independent dimensions [...] [they balance] between plurality and singularity'.

challenges to such collaboration is the discrepancies between state agencies and private companies in terms of what should be the object of collaboration; in other words, what cyber security is. The argument here would be that these discrepancies do not stem from different perspectives on cyber security. Rather the challenges to cooperation arise as public and private actors are dealing with different (cyber) *securities*.⁵ Enhanced collaboration does hence not hinge on one understanding of cyber security gaining prevalence but rather on bringing into being a common object of collaboration.

This, importantly, brings to the fore how enacting ontologies of cyber security is a political undertaking. It may entail resistance and contestation. Nevertheless, this is not to say that these multiple ontologies are necessarily mutually exclusive. Whereas the coexistence of some realities may lead to controversies, others may dovetail with or depend on one another in various complex ways. (Mol 1999; Law 2009) Neither do they simply exist as discrete realities side by side. In the case of anaemia Mol shows, how '[t]hey are not simply opposed to, or outside, one another. One may follow from the other, stand in for the other, and [...] one may include the other'. (Mol 1999:85) Consequently, rather than seeking to define cyber security once and for all, we ought to ensure sensibility to the existence of multiple cyber securities, each with different configurations of cyberspace and security, and to the complex relations between them.

If the ontology of cyber security is not given in the order of things but is continuously enacted and potentially multiple, it follows that there is no privileged vantage point from which academic sense-making of cyber security takes place. Hence any academic engagement with cyber security also partakes in assembling and shaping the reality(ies) of cyber security. The academic literature on cyber security is not detached from cyber security practices but is equally a political intervention in them; academic work interferes with and potentially disrupts the world. (Aradau and Huysmans 2014; Aradau, Huysmans, Neal, and Voelkner 2015) The theories, methodologies and methods we em-

⁵ Tellingly, many Danish Chief Information Security Officers (CISOs) and other company representatives do not consider what they do to be “cyber security”; instead talk about e.g. “information and data security”. To them “cyber security” is what the Danish Centre for Cyber Security do.

ploy in the study of cyber security play and important part in shaping the practices with which we engage. Hence, to quote Marilyn Strathern (1992:10), ‘it matters what ideas one uses to think other ideas (with)’. In short, the academic literature on cyber security is part and parcel of the ontological politics of cyber security. [include Law and Jasanoff on the status of knowledge? Also the double sense of partial knowledge cf. Haraway and Winthereik & Verran]

It is, of course, commonplace within critical security studies and the critical literature in the social sciences in general to argue that knowledge production is political. Theorisation of social phenomena is not a neutral and detached undertaking. However, such claims generally come with a strong emphasis on epistemology whereas it is acknowledged that ‘reality is’ without presupposing the nature of its being. (Andersen 2003) This prioritisation of epistemology over ontology is not surprising, considering that much of this critical scholarship emerged as a response to the positivist and post-positivist approaches to security; and, as such, this move has been very productive in moving the discipline forward. What we suggest is, in a sense, to bring ontology back in. Importantly, we do, however, not suggest to do away with epistemology and return to ontological essentialism but to acknowledge that our sense-making of the world does not just shape our view of the world but also brings into being realities.⁶ (Gad, Jensen, and Winthereik 2015) Knowledge production is hence political, not only in an epistemological sense, but also in an ontological sense. In other words, the academic analysis and theorisation entails the production of both knowledge and worlds. (Aradau et al. 2015; Winthereik 2015) Therefore it is critical that we also scrutinise how cyber security is brought into being the academic literature. [what happens when security meets cyberspace – bringing certain realities into being rather than others...]

The question then is *how* to engage with the ontological politics of the academic literature on cyber security. Since we argue that cyber security is, in a sense, brought into being through the relations forged between security and cyberspace, we explore how the nature of each of the two is shaped in

⁶ Considering epistemologies, ideas, concepts and other structures of meaning as part of the enactment of reality is what Gad et al. (2015) call ‘ontologising epistemology’ (as opposed to the predominant tendency of ‘epistemologising ontology’ in the critical social science literature).

this meeting according to the literature. Hence we, first, engage with how cyberspace(s) is brought into being in literature. This includes the role of technology, the notion of space implied and whether the literature takes an inclusive or exclusive approach to cyberspace. Second, we engage with how security is brought into being in the form of ‘threat realities’. That is to say, what kind of security logic is at play, what/who are threatened, who are the relevant and/or responsible actors etc.

Here it is important to emphasise that such an analysis of the literature is, of course, equally a situated intervention into the ontological politics of cyber security. Recalling Strathern’s argument above, this structuring of our analysis shapes the overview of the literature that is put forward here. This is, however, not meant to be an exhaustive mapping of the cyber security literature. We find that engaging with the literature’s versions of cyber security through the ‘cyber’ and the ‘security’ components, respectively, productive in that this allows to bring to the fore the ways in which the academic scholarship on cyber security mobilises certain connections between technologies, threats, risks, vulnerabilities and actors – in short, certain realities of cyber security. [i.e., how security meets cyberspace in academic scholarship on cyber security – this distinction is an analytical heuristic] [analytical distinction – again importantly not the combination of two existing concepts but how they are brought into being through the concept of cyber security]

THE BIRTH OF CYBERSPACE

Ontological politics is not a strictly human activity. Rather the scope of politics is broadened and it takes on a socio-material character, which is to say that it includes the technological elements of cyber security. Many scholars, especially in science and technology studies, have emphasised how technology and other kinds of material artefacts play an active role in politics. The relationship between human and non-human elements is, however, not a straightforward one but one of continuous co-constitution. (Barry 2001; Jasanoff 2004) This is important for our understanding of cyber security. Cyberspace is not just a socially malleable vehicle for security, nor is it a fixed con-

tainer that determines what cyber security can be. This is why we need to empirically study the interplay between the various elements that make up cyber security.

It is impossible to think of cyber security without also engaging with the concept of cyberspace. Cyberspace, in itself a spatial metaphor as will be displayed and discussed, comes in multiple variants. (Betz and Stevens 2013:149) The concept of cyberspace is a merge of cybernetics⁷ and space. It is said to be coined by the writer William Gibson in his 1982 short story collection *Burning Chrome*, however, it popularized and became known from his 1984 novel *Neuromancer*. In the novel Gibson refers to cyberspace as ‘a consensual hallucination’. (Gibson 1984:51). Since then the discussion on the spatiality and security of cyberspace has been tenacious⁸. In this section we focus on the ways in which infrastructure and ICT have become manifest and how they have been paramount in conjuring up cyberspace. We thereby wish to raise the complexity through which we examine and understand the current cyber security literature. Also, we display how different cyberspaces are enacted in the cyber security literature, and we emphasize why these cyberspaces need to be taken serious in their multiplicity and relationality. From our perspective, infrastructures and ICT are not just objects of a cyberspace. They are socio-technical entities that inhere in and exceeds cyberspace. Infrastructure and ICT are, so to speak, active parties in the making of the social collectivities and political associations related to cyberspace and cyber security

⁷ On cybernetics and Norbert Wiener...

⁸ However, as the web-magazine *kunstkritik.no* has pointed out, the Danish artist Susanne Ussing (1940–1998) and the architect Carsten Hoff (b. 1934) in the years 1968–1970 under the assumed name *Atelier Cyberspace* presented and exhibited numerous art works displaying their conceptualization of cyberspace. This is of more than mere historical interest since Ussing and Hoff’s conceptualization of cyberspace is quite different from Gibsons. It lends itself to a much more optimistic, concrete, architectural perception of the spatiality of cyberspace and much less to computers and the functionality of computerized machines. (Lillemose and Kryger 2015)

We do not suggest a progressive, eschatological or epochal analysis of socio-technical developments leading to the birth of cyberspace. Rather, we display how infrastructure protection and ICT emergences and landmarks have been constantly entangled with political and societal processes altogether playing a crucial role in giving birth to cyberspace and cyber security as the unification of cyberspace and security. In other words, the development and newness oftentimes attached to the concept of cyber security, we argue, makes sense only against the backdrop of sociotechnical continuity, relationality and multiplicity.

Cyberspace: Tangled up in Infrastructure and ICT

Historian of modernity, technology and infrastructure Paul Edwards argues that mature technologies – like cars, roads, buildings and sewers – ‘reside in a naturalized background’, despite the fact that our civilization fundamentally resides upon them, since they are the ‘connectivity tissues and the circulatory systems of modernity. In short, these systems have become infrastructures’ (Edwards 2003: 185). Nonetheless, as Edwards and others have noticed, infrastructures, if not all technologies, are increasingly understood as parts of sociotechnical heterogeneous assemblages (Bowker and Star 1999; Edwards 2003; Latour; 2005; Bennet; 2010 Larkin 2011; Block et. al 2016). Consequently, the former idea of fixation of infrastructures is increasingly exchanged with perceptions of infrastructures and technologies as relational and fluid. Among the first to capture this transformation was the sociologist Manuel Castells, who famously conceptualized modern ICT infrastructures as a ‘space of flows’ (Castells 1997; see also Edwards 2003; Block et. al 2016). Correspondingly, Brian Larkin in a recent review article on ethnography and infrastructure emphasizes that ‘Infrastructures are built networks that facilitate the flow of goods, people, or ideas and allow for their exchange over space...They comprise the architecture for circulation, literally providing the undergirding of modern societies, and they generate the ambient environment of everyday life.’ (Larkin 2013: 9).

Today, the computer has escaped the box. Information and communication infrastructure permeates our societies and provides the basis for our modern lives – and with the emergence of the so-

called internet of things (IoT), ICT is even built into e.g. cars, light bulbs and refrigerators. ICT is thus becoming a 'new globalization'. An 'unavoidable marker for heterogeneous and often contradictory transformations – in economic organization, social regulation, political governance and ethical regimes – that are felt to have profound though uncertain, confusing, or contradictory implications for human life'. (Ong and Collier 2008:3) Consequently, information infrastructures increasingly function as the operating systems that mediate this permeation and saturation of our lives and societies. Information infrastructures link macro, meso, and micro scales of time, space, and social organization: they form the stable foundation of modern social worlds. As Keller Easterling puts it: '...infrastructure is now the over point of contact and access between us all – the rules governing the space of everyday life.' (Easterling 2014: 11). More fundamentally, it has been a truism within both academia and politics over the past 15 years that we are witnessing a shift in the core dynamics of social, political, cultural and economic life due to the invasive spread of ICT and information infrastructures. Infrastructure and ICT has, so to speak, acquired a new sense urgency and centrality in contemporary political life. This development is most notably summarized in the enveloping concept of cyberspace. A foundational concept for much of the discussion on cyber security. (Cohen 2007; Deibert and Rohozinski 2010; Betz and Stevens 2013; Cavelti 2013) However, we argue, that cyberspace is not just a socially malleable vehicle for security, nor is it a fixed container that determines what cyber security can be. This is why we need to empirically study the interplay between the various elements that make up different cyberspaces in the scholarly literature. In the following we turn to how infrastructure and ICT have been paramount in conjuring up different ideas of cyberspaces and their relation to security.

Cyberspaces

Andrew Lakoff and Stephen Collier have persuasively traced the emergence of a specific type of infrastructure governance – vital systems security interventions- in the US from the beginning of the 20th century (Collier and Lakoff 2008; 2015). They argue that thoughts on system vulnerability found their way into military strategist thinking following the experience of the First World War. In

line with the total war argument the military strategist pointed out that disruption of systems critical to the enemy's industrial production was an essential strategic goal. A goal to be followed in the strategic bombings of World War Two. Later, during the Cold War, the system vulnerability thinking expanded and was intertwined with non-military, societal vulnerability reduction and emergency preparedness in anticipation of a nuclear attack. As the fear of a nuclear attack faded Collier and Lakoff argue that the vital systems security techniques were used to address problems other than military defense including system of critical infrastructure (Collier and Lakoff 2008; 2015).

However, it was not until the late 1980s that the concept and practice of critical infrastructure protection was explicitly articulated and gained wider political momentum. The reason for this Dunn Cavelty argues was the increased perception of a (still) ongoing transformation of all aspects of life through saturation with ICTs. (Cavelty 2008b). One of the first places where this connection between infrastructure and ICT was clearly stated was in the President's Commission on Critical Infrastructure from 1997 'We did find widespread capability to exploit infrastructure vulnerabilities. The capability to do harm – particularly through information networks – is real; it is growing at an alarming rate; and we have little defense against it.' (President's Commission on Critical Infrastructure 1997: xx). At the same time, however, it was made extremely clear in the commission's report that the policies and operational mechanisms should 'recognize the inherent differences between the physical world and cyberspace' (President's Commission on Critical Infrastructure 1997: 17). This idea of the relation between infrastructure and ICT conjuring up cyberspace as something in opposition to 'real' space is a cornerstone within cyber security thinking.

In order to exhibit and understand the core dilemmas and consequences captured in the discussion on the spatiality and security of cyberspace two diverging positions marking the end points of a continuum can be carved out from the existing literature: an exclusive and an inclusive view of cyberspace, respectively. (Betz and Stevens 2013) The first position holds a narrow conceptualization of cyberspace excluding physical infrastructure and sociality. In this view cyberspace is perceived as a virtual reality separated from the 'real world' as demonstrated above. (Barlow 1996) The second position widens cyberspace by incorporating physical infrastructure and user experiences to

various degrees (Cohen 2007; Libicki xx). An illustrative example of this last position is the definition given by Deibert and Rohozinski ‘cyberspace is comprised of both a material and a virtual realm—a space of things and ideas, structure and content’. (Deibert and Rohozinski 2010:16)

Multiply depictions of cyberspace thus enters the political imaginary as different entanglements of established ways of thinking about vital systems security, critical infrastructure and protection of government networks and classified information combined with the rising concerns about the transformations, possibilities and vulnerabilities stemming from the extensive development in ICT (Cavelty 2008; 2007; 2001, Collier and Lakoff 2008, Deibert and Rohozinski 2010; Libicki 2007; 2009....).

The realist scholar Martin Libicki, who have written extensively on cyber security and cyber war, perceive of cyberspace as a virtual medium less tangible than water, air, space and ground. A medium with its own rules requiring us to rethink war and deterrence in this new domain. (Libicki 2007, 2009) He offers a three-layered inclusive conceptualization of cyberspace which includes ‘the physical layer, a syntactic layer sitting above the physical, and a semantic layer sitting on top’. (Libicki 2009:12) Libicki also stresses that cyberspace exists on multiple locations at once and can appear in multiple, almost infinite, manifestations and forms. (Libicki 2009:5–6) What we take from this is the possibility of a multiplicity of cyberspaces. Virtualities that are real and existing but haven’t necessarily been actualized.

[other examples from the cyber security literature on the general consensus on describing cyberspace as complex and multiple in the introduction *before* coupling it with security]

The various enactments of cyberspace display not only different representations or perceptions of an empirical realm from which cyber security is extricated. They are also always political interventions enacting multiply cyberspaces and hence conditions of possibilities for politics. This leads to our first conclusion. The relationship between infrastructures and ICT’s have been co-constitutive in conjuring up a multiplicity of cyberspaces in the academic literature. At the same time these cyberspaces have helped define the criticality, purpose, and characteristics of both infrastructures and ICT’s. In other words, we have demonstrated the multiplicity, relationality and co-construction of

infrastructures, ICT's and cyberspace. This will serve as the underpinning of our further analysis of the way cyber securities are brought into being in the academic literature when cyberspaces meets security.

SECURITY MEETS CYBERSPACE

Interestingly, the multiplicity of cyberspace is markedly absent, when cyberspace meets security. In the following we unfold how cyber security, within both a realist tradition and critical security studies tradition, is approached in accordance with the usual fault lines and understandings of security. Consequently, installing a certain politics of cyber security. We conclude that most of the academic literature on cyber security seem to accept an inclusive view of cyberspace; nevertheless, despite the repository of multiple potential cyberspaces, it is a singular cyberspace that is actualized and brought into being – also when cyberspace is more explicitly coupled with security as will be shown.

Second, we engage with the threat realities that are assembled and contested in the texts; i.e., what are the threats, what/who are the threatened, who are the relevant and/or responsible actors etc. What seems to be a common denominator is the sometimes implicit necessity to pursue cyber security as a matter of national security. As if the concept of cyber security represents certain threat realities and universal functional logics. In other, more boldly, words, security is widened to include cyberspaces, but it is at the same time folded back into the narrow straight-jacket of militarisation and state-centric national security.

Realist approach

Realist thinkers often cite an intellectual lineage going back to the likes of Hobbes and even Thucydides. Similarly many debates in the subfield of strategic studies revolve around the works of Clausewitz and Sun Tzu. They generally see themselves as continuously trying to improve our understanding of the perennial issue of war. This is also very much mirrored in their approach to cyber security – or, more specifically, to cyber warfare. Several realist scholars have provided quite

detailed and sophisticated empirical analyses of the specificity of cyberspace and the technologies related to it, as well as their implications for warfare and strategy. Notwithstanding, cyber warfare is seldom discussed as a distinct phenomenon but rather as the potential proliferation of well-known dynamics into a new space, namely cyberspace.

Despite his initial claims to the multiplicity of cyberspace, Libicki downplays this multiplicity and its connection to the materiality when cyberspace meets security. As explicated above Libicki argues that security perceptions and practices are different when they unfold in and through cyberspace. He emphasizes the specific empirical features and contexts separating cyber security from other militarised security domains such as water, air, space and ground. At the same time, however, Libicki implicitly adheres to, depend upon and sustain a particular representation of the world and a particular logic of security that stretches across the different domains. Security for Libicki is national security centered around warfare informed by military rules. Hence, security becomes more of a given than a construct. This has a range of consequences highlighted by various critical security scholars such as reproduction of; certain inside and outside divides (Campbell 1992; Walker 1993), a logic of realism. (Huysmans 1998; Williams 2003)

Cyber warfare and strategy is generally placed in a larger argument of technology as a 'force multiplier' rather than as something that fundamentally changes the dynamics of warfare as such. (Cavelty 2007; Libicki 2007, 2009) Polemically speaking, one might say that cyber warfare is just the continuation of war by other means. Or is it? There are several debates in this literature whether cyber attacks indeed qualify as war. Some discuss the legal status of cyber attacks, whereas others engage in philosophical debates on the nature of war and whether this applies to cyber issues.

A major debate in the realist literature on cyber security in strategic studies revolves around the question of the nature of cyber threats. This debate may, essentially, be divided into two interrelated and overlapping sub-debates. One is the discussion about whether cyber war will indeed take place. The other discusses the strategic (and political and legal) implications of the use of 'cyber force'; i.e., how states may address the challenges stemming from cyberspace. (Farwell and Rohozinski 2011, 2012) Whereas the former debate hence has a more of a philosophical and theo-

retical bent, the latter is more practical and problem-solving in its focus. In other words, the former discusses the nature of cyber threats while the latter more pragmatically acknowledges them as challenges that states need to handle in the best way possible.

A principal figure in the more philosophical and theoretical debate on cyber security is Thomas Rid. In an article and a book – both instructively titled ‘Cyber War Will Not Take Place’ – he argues that cyber incidents have so far not, nor will they in the future, amount to actual warfare. (Rid 2012, 2013) Rid argues that the use of cyber weapons – i.e., weaponised code – does not meet the three criteria defining an act of war: it has to be (potentially) violent, instrumental and political. (Rid 2013: xx) Central to his argument is the claim that cyber attack cannot cause physical damage on its own, he argues, as ‘weaponised code simply does not come with an explosive charge’. (Rid 2013: xx) According to Rid, cyber attacks cannot be seen as warfare, i.e. political violence, but may perform supporting functions in war in the form of espionage, subversion or sabotage. Indeed, cyber attacks help diminish rather than accentuate political violence, he argues, as weaponized code enables ‘highly targeted attacks on the functioning of an adversary’s technical systems without directly physically harming the human operators and managers of such systems’. (Rid 2013: xxx) Thus, Rid seems to have an inclusive view on cyberspace, but the main divide is not set between cyberspace and ‘real’ space, rather, he see it as a divide between the physical and the non-physical. Cyberspace alters this divide in a non-fundamental way. [still employs warfare as the yardstick for security]

Common to the realist literature on cyber security is the assertion that security is state security. More specifically, it is warfare. For those familiar with the realist tradition, this is hardly surprising. ‘The main focus of security studies is easy to identify, however: it is the phenomenon of war’. (Walt 1991) Yet, it is interesting that cyberspace is hardly seen to change the dynamics of warfare and power. Rather, the age-old dynamics and principles identified by realist scholars are merely extended to the domain of cyberspace. ‘Cyber-power is therefore the manifestation of power in cyberspace rather than a new or different form of power. This is an important caveat that can be similarly applied to the allied concepts of sovereignty, war and dominion. Local circumstances may produce novel events and peculiarities, but the same general principles apply’. (Betz and Stevens

2011:44–45) The theoretical literature on cyber security in strategic studies is hence less about theorising cyber security and more about contributing to the theorisation of war as such. The realist literature on cyber security is, in short, ‘basically, old wine in new bottles’. (Eriksson and Giacomello 2006:209)

‘Critical’ approach

Cyber security has also received attention from a few security scholars who have applied ideas derived from the Copenhagen School (Buzan, Wæver, and Wilde 1998) to critically engage with the discursive and intersubjective formations of cyber security. (Cavelty 2007, 2008, 2013; Eriksson 2001; Hansen and Nissenbaum 2009) At the heart of their endeavor, in line with the Copenhagen School and its securitization framework, seem to be a goal of deepening and broadening the perception of cyber security rejecting the primacy given to warfare and military security. Also, special attention is paid to the discursive framing of cyber security as a certain political problem and representations of threats in terms of extraordinary measures, urgency and survival, thereby, constituting cyber security as something beyond normal politics.

This is accentuated by Hansen and Nissenbaum who hold that ‘The most significant lesson of bringing the Copenhagen School to cyber security may be to bring the political and normative implications of “speaking security” to the foreground’. (Hansen and Nissenbaum 2009:1172) Correspondingly, Myriam Dunn Cavelty (in her later work) aims for ‘...a broad understanding of cyber security as discursive practice by a multitude of actors inside and outside of government...’. (Cavelty 2013:106) Cavelty challenges the focus on elite expressions, usually associated with the Securitization Theory. Instead she applies an analytical frame that emphasizes ‘little security nothings’ (Huysmans 2011) and the everyday political and cyber security processes. Likewise, Hansen and Nissenbaum highlights the complex entanglement between public-private responsibility and government authority when speaking of cyber security. (Hansen and Nissenbaum 2009:1162) To sum up a multiplicity of discourses and actors involved in the process of the securitization of cyberspace is highlighted in the literature (ibid).

It seems like Cavelti at least keep the door open for envisioning cyberspace as an assemblage or entanglement of materiality and discourse. However, she keeps being caught up in semiotics and linguistics. Cavelti underlines that cyber security is ‘a combination of linguistic and non-linguistic discursive practices from many different ‘communities’ of actors’ (Cavelti 2013:108), but a little further on she stresses ‘cyber-security cannot be imagined without drawing on language used to describe the environment in which it operates’. (Cavelti 2013:??) To what effect? For Cavelti it leads to a focus on heterogeneous political manifestations that are linked to different threat representations. She speaks of three clusters of threat representations, but she fails to clarify the status of the threat representations. It is unclear what the ontological status of the representations is and thus whether the socio-linguistic threat representations precede practice and how they relate to the materiality of cyberspace. The repercussion is explicit in the conclusion in which materiality is downplayed. Instead the possibility of change in little cyber security nothings or practices is said to follow presentations of cyber-security as national security. (Cavelti 2013: 118) It thus seems as if cyber security is primarily embedded with the state and national security and not something that exist in these everyday practices.

Hansen and Nissenbaum (2009) set out to examine cyber security as distinctive sector within the Copenhagen School framework. In order to do so they ask; ‘what threats and referent objects characterize cyber security: what distinguish it from other security sectors; how may concrete instances of cyber securitizations be analysed; and what may critical security scholars learn from taking cyber discourse seriously?’. (Hansen and Nissenbaum 2009:1157) They specify the cyber security sector by laying out three security modalities inherent to it; ‘ hypersecuritization, which identifies large-scale instantaneous cascading disaster scenarios; everyday security practices, that draws upon and securitizes the lived experiences a citizenry may have; and technifications, that captures the constitution of an issue as reliant upon expert, technical knowledge for its resolution and hence as politically neutral or unquestionably normatively desirable’ (2009: ??). Nevertheless, they stress that it is not plausible to understand cyber security as insulated from other sectors of security. (Hansen and Nissenbaum 2009:1157) It seems as if Hansen and Nissenbaum simultaneously wish to maintain

cyber security as a distinct sector and underline its potential to break down the division between sectors. They emphasize the multiplicity of cyber security discourses articulated within the cyber security sector, still, they aim to freeze the sector.

Much of the critical literature inspired by the securitization theory tends to neglect the material aspects of cyber security. Instead scholars like Cavelti (2007, 2008a, 2013), Hansen and Nissenbaum (2009) and Eriksson (2001; Bendrath, Eriksson, and Giacomello 2007) focus on the discursive constitution or framing of cyber security as an issue of national security. To be sure, references to the material aspects of cyber security can still be found in many of these texts. It is, however, relegated to the margins of the texts. They hence give primacy to the linguistic dimension of cyber security. This is, as argued above, not surprising given that these scholars are situated in a literature that emerged as a critical alternative to the post-positivist mainstream and its quite materialist rendition of security. [example of discursive emphasis plus references to materiality]

Another indicator supporting the claim that Hansen and Nissenbaums theorization and analyses is too tied to a nation state configuration of security is their overall argument that cybersecurity has been successfully securitized. An argument they base on institutional developments in the United States and NATO.⁹ (Hansen and Nissenbaum 2009)

Consequently, we find that Cavelti's three clusters and Hansen and Nissenbaums three modalities of the cyber security sector are too fixated on discourse and national security. In other, more boldly, words, they widen the concept of cyberspace to include a repository of cyberspaces, but it is a singular cyberspace that is actualized and brought into being in the texts when coupled with security. At the same time as cyberspace is singularized security is folded back into the narrow straight-jacket of state-centric national security. Despite the fact that a repository of multiple potential cyberspaces and a multiplicity of discourses and actors involved in the process of securitization are emphasized

⁹ Also it can be argued that it is unclear in the article what is extraordinary and what is normal in regards to creating new institutions and publishing new strategies. Does the establishment of new institutions in and off itself qualify as proof of securitization? Further, there is no clarification on who the audience are and to what extent/how they have accepted the securitizing move.

and foregrounded in the text, they stray away from what we find to be the obvious consequence; the enactment of multiple cyber securities.

DISCUSSION

Nortje Marres has, critically, observed that Mol's brand of 'ontological politics' does not address issues of politics and democracy in the institutional sense. 'Ontological politics, in other words, is here sharply distinguished from the institutional or formal activity of capital 'P' Politics'. (Marres 2013:421) Yet, unlike Mol, we are not studying the ontological politics of anaemia or atherosclerosis here but the ontological politics of cyber security. The ways in which realities of cyber security are brought into being do have political and democratic implications – also for 'capital 'P' politics'. To invoke Foucault's (1984, 1990) idea of 'problematization', realities of cyber security constitute how being should be thought in terms of problems and solutions. They organise concepts, meanings and practices prescribing both present and future possibilities of cyber security. The ontological politics of cyber security is, in other words, important both for the worlds that are brought into being and for the policies we adopt to address living them.

[link these two paragraphs more]

The existing literature on cyber security is, as we have shown, very much a continuation of the existing debates in security studies. In a sense, the meeting between security and cyberspace brings little new to the table. Consequently, it falls short of potential new insights in terms of understanding and engaging with security politics in the digital age. More specifically, we would like to highlight to particular shortcomings of the literature here. It lacks sensibility to both the transformative role of ICT in security politics and emergence of new security actors and practices. We will elaborate on these two issues here.

First, the neglect of materiality in the critical security studies literature on cyber security has serious political implications. Hansen and Nissenbaum rightly argue that cyber security involves a

'technification' that 'construct[s] an issue as reliant upon technical, expert knowledge, but...also simultaneously presuppose[s] a politically and normatively

neutral agenda that technology serves...Cyber security discourse's simultaneous securitization and technification work to prevent it from being politicized in that is precisely through rational technical discourse that securitization may "hide" its own political roots'. (Hansen and Nissenbaum 2009:1167–1168)

They point to the importance of not just expertise – which plays a central role in most security practices (e.g. military [other examples] expertise) – but of a particular kind of *technical* expertise. Nevertheless, Hansen and Nissenbaum – and other critical scholars for that matter – remain at the level of discourse and refrain from engaging with the political significance of ICT and its materiality. To them technology is socially constituted through discourse thus downplaying the political role of technology in shaping the social practices. We thus lack a proper engagement with the politics of ICT. By giving the social (discourse) primacy to the technological with regards to cyber security, they hence, ironically, contribute to perpetuating the technification of these issues. [betz and stevens]

An important exception to this tendency to neglect the material dimensions in critical approaches to cyber security can be found in the work of Ronald Deibert. He emphasises that '[...]cyberspace is both a material and virtual realm – a space of things and ideas, structure and content'. (Deibert and Rohozinski 2010:16) He calls for a greater engagement with the technical aspects in the critical literature on cyber security (Deibert, Rohozinski, and Crete-Nishihata 2012) and argues that

'[...] IR theorists – interested in and normatively in favour of opening up spaces for alternative voices, grassroots democracy, and global democratic governance to flourish – will have to pay greater attention to the material foundations upon which global communications take place. Doing so means qualifying notions of 'ideas all the way down' and 'worlds of our making' to acknowledge the extent to which material factors of communication, albeit socially constructed, present a formidable set of real constraints of the realm of the possible [...] communication does not take place in a vacuum. It is anchored within and shaped by the material properties of the communications environment'. (Deibert 2003:529–530)

Yet, while acknowledging the importance that the technological infrastructure plays, Deibert's work contributes little to the theorisation of how the meeting between security and cyberspace may change security politics. Rather, the work of Deibert and his colleagues at the Citizen Lab is largely empirically driven. The Citizen Lab predominantly focuses on how e.g. surveillance and censorship practices – particularly in the global south – increase cyber insecurity. Indeed, their research is of a more activist nature in that it 'monitors, analyses, and impacts the exercise of political power in cyberspace'. (Citizen Lab n.d.) Their research is, as such more problem-driven, than theoretically oriented.

Deibert thus seeks to highlight how the technologies affects the conditions of possibility. The material aspects of cyberspace thus impose constraints on political action. (Deibert 2003) This is, however, not a one-way street. Deibert stresses the emergent properties of cyberspace and its complexity and volatility. This, importantly, stems both from the technological development and from actions of states, commercial actors and other users. (Deibert and Rohozinski 2010) [+other references?] Deibert's claim is, in other words, not one of technological determinism. Rather, it is a matter of taking seriously how technology shapes and is shaped by political action.

In line with Deibert's arguments, we argue that we need to examine and capture the distinctiveness and impact of cyberspace and develop analytical categories that allow us to examine the complex imbrications between cyberspace and the security dynamics through which relations and thus politics are constituted. Our claim is that cyberspaces' distinctiveness not solely lies in its impacts, but also and even more importantly in constructing and working with cyberspaces as specific objects of study, within the constitution of new sociotechnical relations, practices and domains (Latham and Sassen 2005; Latour). Cyberspaces are continuous processes of assembling subjects, objects and practices. This way of thinking offers a platform from which we can think through the relationship between stability and transformation, structure and agency. Cyberspaces are constantly enacted and practiced processes with consequences exceeding territorial boundaries, public-private relations, and national regulatory frames. At the same reenacting and upholding the same boundaries. Rewriting Latour cyberspace should not be used to explain, but rather encountered as something to be

explained. Something that is constantly re-enacted in different contexts. Cyberspaces are thus neither virtual or material. Cyberspaces are both actual and possible at the same time.

[something about the generalisability of cyber security? i.e., the problems of grand theory-making]

Second, there is a general tendency in the scholarly literature on cyber security to focus on cyber security as an issue of 'high politics'. That is to say that the primary focus is on the exceptional politics of national security and the level of state elites. In the securitisation literature on cyber security this largely follows from the delineation of the speech act of security in the original formulation of securitisation theory. Apart from theoretical parsimony and stringency, a central argument in favour of this delineation was, in fact, a normative one. It was an argument in favour of liberal and democratic political procedures and against letting the threat-defence logic of security colonise all spheres of society. Ideally, securitisation is to be avoided; it is (in most cases) seen as the failure an issue through normal political procedures. In the words of Wæver (2011:469), securitisation theory '[...] has a 'bias' for desecuritization, although a careful one'.

Historically, this normative argument has been well-taken. If we, however, follow the line of argument that we have laid out hitherto in this article, it is not politically nor democratically adequate for engaging with cyber security. Following from our emphasis on the multiplicity of cyber security, it is necessary, we argue, to – in a manner of speaking – turn the normative argument of securitisation theory on its head. That is to say, if we restrict our notion of cyber security to the exceptional politics of securitising (state) agents, we run the risk of being blindsided by those practices of cyber security that do not, in and of themselves, amount to high politics or exceptional politics. The extant literature on cyber security thus has a critical blind spot when it comes to more mundane and routinised practices, as well as non-state actors.¹⁰

However, cyber security cannot and should not be confined to high politics. It also includes 'little security nothings' (Huysmans 2011) in the practices of non-state actors, such as the private compa-

¹⁰ This is of course an oft-cited critique against the Copenhagen School in security studies (Huysmans 2006; Petersen 2011) but it holds particularly true for the literature on cyber security, as the critique in this regard is to be directed at the literature as a whole.

nies who own and operate most of the ICT infrastructure and provide the services that run on this infrastructure. A narrow focus on the exceptional politics of national security would thus seriously impair our ability to critically engage with cyber security. Therefore it is absolutely vital, we argue, to open up the political space for cyber security by also engaging with the cyber security practices of non-state actors. We need to be able to engage critically with adverse issues in the practices of e.g. private companies or interest groups that are not readily captured by the categorise of exceptional or even normal politics in the political system.

CONCLUSION: WHERE TO GO FROM HERE?

Our impetus for turning to the ontological politics of cyber security in the academic literature has been to provide an ‘ontological opening’. (de la Cadena 2014; Lien 2015) As we have shown in this article, the scholarly literature on cyber security is perpetuating existing debates in security studies [elaborate a little]. Engaging with the ontological politics of cyber security paves the way for a different kind of analysis. It reminds us that ‘there is no obvious context out there waiting to be revealed, no theory providing the obvious analytical anchor for the material at hand, but instead, endless opportunities for association and juxtaposition, each with the potential for taking the analysis in a new direction’. (Lien 2015:5) This ‘ontological opening’ enables a critical analytical sensibility to the heterogeneous, transformative and, not least, multiple nature of cyber security. It draws attention to how academic work brings cyber security into being through the actualisation of one (or more) among many from a virtual repository of multiple potential cyber *securities*. In sum, it allows to remain open to how cyber security may indeed challenge conventional accounts of security.

It is one thing to say that cyber security is multiple. This does not in itself tell us something about the ontological politics of cyber security but it is a productive assumption for an analytical strategy. (Gad et al. 2015) It opens up the space of the politics of cyber security and for new avenues for academic engagement with it; these are of course equally multiple but we would like to highlight two of them here. First, if we acknowledge the implications of ICT for theory and politics, it remains to be explored, both empirically and theoretically, how and under what conditions different

cyber securities as political events come about, what it takes to produce them as political sites, and not the least how the relevant political collectives are ordered and composed. Second, we need to take seriously that engage with how the cyber security practices of private actors bring new political spaces into being, thus challenging conventional notions spatiality in security politics. Instructively, historian of the internet John Naughton likens the notion of determining the impact of the internet once and for all to asking people a couple of decades after the invention of the Gutenberg press about its likely impact on the world. (Naughton 2012) That is to say, we can hardly predict the full extent of potential implications of technological developments and the uses of new technologies. Likewise, we should not readily determine the impact of cyber security on security politics. As scholars, we need to continuously and meticulously engage with the multiple and changing ways in which it is practiced.

BIBLIOGRAPHY

- ALLEN, JOHN. (2011) Powerful Assemblages? *Area* 43: 154–157.
- ANDERSEN, NIELS ÅKERSTRØM. (2003) *Discursive Analytical Strategies: Understanding Foucault, Koselleck, Laclau, Luhmann*. Bristol: Policy Press.
- ARADAU, CLAUDIA, and JEF HUYSMANS. (2014) Critical Methods in International Relations: The Politics of Techniques, Devices and Acts. *European Journal of International Relations* 20: 596–619.
- ARADAU, CLAUDIA, JEF HUYSMANS, ANDREW NEAL, and NADINE VOELKNER, Eds. (2015) *Critical Security Methods: New Frameworks for Analysis*. Abingdon, Oxon ; New York, NY: Routledge.
- BARLOW, JOHN PERRY. (1996) A Declaration of the Independence of Cyberspace. Available at: <https://projects.eff.org/~barlow/Declaration-Final.html>. (Accessed September 22, 2015).
- BARRY, ANDREW. (2001) *Political Machines: Governing a Technological Society*. London ; New York: The Athlone Press.
- BENDRATH, RALF, JOHAN ERIKSSON, and GIAMPIERO GIACOMELLO. (2007) From “Cyberterrorism” to “Cyberwar”, Back and Forth: How the United States Securitized Cyberspace. In *International Relations and Security in the Digital Age*, London: Routledge.
- BETZ, DAVID J., and TIM STEVENS. (2013) Analogical Reasoning and Cyber Security. *Security Dialogue* 44: 147–164.
- BETZ, DAVID J., and TIM STEVENS. (2011) Chapter One: Power and Cyberspace. *Adelphi Series* 51: 35–54.
- BUZAN, BARRY, OLE WÆVER, and JAAP DE WILDE. (1998) *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.
- DE LA CADENA, MARISOL. (2014) The Politics of Modern Politics Meets Ethnographies of Excess through Ontological Openings. *Cultural Anthropology*. Available at: <http://www.culanth.org/fieldsights/471-the-politics-of-modern-politics-meets-ethnographies-of-excess-through-ontological-openings>. (Accessed February 23, 2016).
- CAMPBELL, DAVID. (1992) *Writing Security: United States Foreign Policy and the Politics of Identity*. Minneapolis: University of Minnesota Press.
- CAVELTY, MYRIAM DUNN. (2008a) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. 1 edition. London: Routledge.
- CAVELTY, MYRIAM DUNN. (2007) Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics* 4: 19–36.
- CAVELTY, MYRIAM DUNN. (2013) From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review* 15: 105–122.
- CAVELTY, MYRIAM DUNN. (2008b) Like a Phoenix from the Ashes: The Reinvention of Critical Infrastructure Protection as Distributed Security. In *Securing ‘the Homeland’: Critical Infra-*

structure, Risk and (In)Security, edited by Myriam Dunn Cavelty and Kristian Soby Kristensen. London: Routledge.

CHRISTENSEN, KRISTOFFER KJÆRGAARD, OSCAR VEJEN LACOPPIDAN, and KAREN LUND PETERSEN. (2015) *Trusler, Kommunikation, Nytte: Udfordringer Ved Offentlig-Privat Samarbejde Om IKT-Sikkerhed*. Copenhagen: Centre for Advanced Security Theory, University of Copenhagen. Policy brief. Available at: http://cast.ku.dk/pdf/Policy_brief_1__med_citater_.pdf. (Accessed August 18, 2016).

CITIZEN LAB. www.citizenlab.org. *The Citizen Lab*. Available at: <https://citizenlab.org/>. (Accessed September 5, 2016).

CLAPPER, JAMES R. (2016) *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*. Washington D.C.: Office of the Director of National Intelligence. Available at: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf. (Accessed September 2, 2016).

COHEN, JULIE E. (2007) Cyberspace As/and Space. *Columbia Law Review* 107: 210–256.

DANISH DEFENCE INTELLIGENCE SERVICE, DDIS. (2012) *Efterretningsmæssig Risikovurdering 2012: En Aktuel Vurdering Af Forhold I Udlandet Af Betydning for Danmarks Sikkerhed*. Copenhagen: Danish Defence Intelligence Service. Available at: <http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2012.pdf>. (Accessed October 27, 2014).

DANISH DEFENCE INTELLIGENCE SERVICE, DDIS. (2013) *Efterretningsmæssig Risikovurdering 2013: En Aktuel Vurdering Af Forhold I Udlandet Af Betydning for Danmarks Sikkerhed*. Copenhagen: Danish Defence Intelligence Service. Available at: <http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2013.pdf>. (Accessed October 27, 2014).

DANISH DEFENCE INTELLIGENCE SERVICE, DDIS. (2014) *Efterretningsmæssig Risikovurdering 2014: En Aktuel Vurdering Af Forhold I Udlandet Af Betydning for Danmarks Sikkerhed*. Copenhagen: Danish Defence Intelligence Service. Available at: <http://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2014.pdf>. (Accessed November 4, 2014).

DANISH DEFENCE INTELLIGENCE SERVICE, DDIS. (2015) *Efterretningsmæssig Risikovurdering 2015: En Aktuel Vurdering Af Forhold I Udlandet Af Betydning for Danmarks Sikkerhed*. Copenhagen: Danish Defence Intelligence Service. Available at: <https://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2015.pdf>. (Accessed July 5, 2016).

DEIBERT, RONALD J. (2003) Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace. *Millennium - Journal of International Studies* 32: 501–530.

DEIBERT, RONALD J., and RAFAL ROHOZINSKI. (2010) Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4: 15–32.

DEIBERT, RONALD J., RAFAL ROHOZINSKI, and MASASHI CRETE-NISHIHATA. (2012) Cyclones in Cyberspace: Information Shaping and Denial in the 2008 Russia–Georgia War. *Security Dialogue* 43: 3–24.

- ERIKSSON, JOHAN. (2001) Cyberplagues, IT, and Security: Threat Politics in the Information Age. *Journal of Contingencies and Crisis Management* 9: 200–210.
- ERIKSSON, JOHAN, and GIAMPIERO GIACOMELLO. (2006) The Information Revolution, Security, and International Relations: (IR)relevant Theory? *International Political Science Review* 27: 221–244.
- FARWELL, JAMES P., and RAFAL ROHOZINSKI. (2011) Stuxnet and the Future of Cyber War. *Survival* 53: 23–40.
- FARWELL, JAMES P., and RAFAL ROHOZINSKI. (2012) The New Reality of Cyber War. *Survival* 54: 107–120.
- FOUCAULT, MICHEL. (1984) Polemics, Politics and Problematizations: An Interview. In *The Foucault Reader*, edited by Paul Rabinow. London: Penguin Books.
- FOUCAULT, MICHEL. (1990) *The History of Sexuality, Volume 1: The Use of Pleasure*. New York: Vintage Books.
- GAD, CHRISTOPHER, CASPER BRUUN JENSEN, and BRIT ROSS WINTHEREIK. (2015) Practical Ontology: Words in STS and Anthropology. *NatureCulture* 3: 67–86.
- GIBSON, WILLIAM. (1984) *Neuromancer*. New York: Ace Books.
- HANSEN, LENE, and HELEN NISSENBAUM. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* 53: 1155–1175.
- HUYSMANS, JEF. (1998) Security! What Do You Mean? From Concept to Thick Signifier. *European Journal of International Relations* 4: 226–255.
- HUYSMANS, JEF. (2006) *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. London: Routledge.
- HUYSMANS, JEF. (2011) What's In An Act? On Security Speech Acts and Little Security Nothings. *Security Dialogue* 42: 371–383.
- JASANOFF, SHEILA, Ed. (2004) *States of Knowledge: The Co-Production of Social Order*. London: Routledge.
- LAW, JOHN. (2009) Actor Network Theory and Material Semiotics. In *The New Blackwell Companion to Social Theory*, edited by Bryan S. Turner. Chichester; Malden, MA: Wiley-Blackwell.
- LAW, JOHN. (2002) *Aircraft Stories: Decentering the Object in Technoscience*. Durham & London: Duke University Press.
- LAW, JOHN, and VICKY SINGLETON. (2005) Object Lessons. *Organization* 12: 331–355.
- LIBICKI, MARTIN C. (2007) *Conquest in Cyberspace, National Security and Information Warfare*. Cambridge University Press. Available at: <http://ep.fjernadgang.kb.dk/login?url=http://dx.doi.org/10.1017/CBO9780511804250>. (Accessed May 25, 2016).
- LIBICKI, MARTIN C. (2009) *Cyberdeterrence and Cyberwar*. Santa Monica: Rand Corporation.

- LIEN, MARIANNE ELISABETH. (2015) *Becoming Salmon*. Oakland: University of California Press. Available at: <http://www.ucpress.edu/book.php?isbn=9780520280571>. (Accessed February 23, 2016).
- LILLEMOSE, JACOB, and MATHIAS KRYGER. (2015) The (Re)invention of Cyberspace. *Kunstkritikk*. Available at: http://www.kunstkritikk.dk/kommentar/the-reinvention-of-cyberspace/?do_not_cache=1. (Accessed September 5, 2016).
- MARRES, NOORTJE. (2013) Why Political Ontology Must Be Experimentalized: On Eco-Show Homes as Devices of Participation. *Social Studies of Science* 43: 417–443.
- MOL, ANNEMARIE. (1999) Ontological Politics: A Word and Some Questions. *The Sociological Review* 47: 74–89.
- MOL, ANNEMARIE. (2002) *The Body Multiple: Ontology in Medical Practice*. Durham & London: Duke University Press.
- NAUGHTON, JOHN J. (2012) *From Gutenberg to Zuckerberg: What You Really Need to Know about the Internet*. London: Quercus.
- OBAMA, BARACK. (2015) Remarks by the President in State of the Union Address | January 20, 2015. *whitehouse.gov*. Available at: <https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015>. (Accessed June 10, 2016).
- ONG, AIHWA, and STEPHEN J. COLLIER. (2008) *Global Assemblages: Technology, Politics, and Ethics as Anthropological Problems*. Malden, MA: Blackwell Publishing.
- PETERSEN, KAREN LUND. (2011) *Corporate Risk and National Security Redefined*. 1 edition. Abingdon; New York, NY: Routledge.
- RID, THOMAS. (2012) Cyber War Will Not Take Place. *Journal of Strategic Studies* 35: 5–32.
- RID, THOMAS. (2013) *Cyber War Will Not Take Place*. London: Hurst.
- STRATHERN, MARILYN. (1992) *Reproducing the Future: Essays on Anthropology, Kinship and the New Reproductive Technologies*. Manchester: Manchester University Press.
- WÆVER, OLE. (2011) Politics, Security, Theory. *Security Dialogue* 42: 465–480.
- WALKER, R. B. J. (1993) *Inside/Outside: International Relations as Political Theory*. Cambridge: Cambridge University Press.
- WALT, STEPHEN M. (1991) The Renaissance of Security Studies. *International Studies Quarterly* 35: 211–239.
- WILLIAMS, MICHAEL C. (2003) Words, Images, Enemies: Securitization and International Politics. *International Studies Quarterly* 47: 511–531.
- WINTHEREIK, BRIT ROSS. (2015) Den Ontologiske Vending I Antropologi Og Science and Technology Studies. *STS Encounters: Research Papers from DASTS* 7: 1–32.