Digital Disaster, Cyber Security and the Copenhagen School[1]

By

Lene Hansen and Helen Nissenbaum

Abstract:

This article is devoted to an analysis of cyber security, a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions. Adopting the framework of securitization theory, the article theorizes cyber security as a distinct sector with a particular constellation of threats and referent objects. It is held that 'network security' and 'individual security' are significant referent objects, but that their political importance arises from connections to the collective referent objects of 'the state', 'society', 'the nation', and 'the economy'. These referent objects are articulated as threatened through three distinct forms of securitizations: hypersecuritization, everyday security practices, and technifications. The applicability of the theoretical framework is then shown through a case-study of what has been labeled the first war in cyber space against Estonian public and commercial institutions in 2007.

Digital Disaster, Cyber Security and the Copenhagen School

This article is devoted to an analysis of 'cyber security', a concept that arrived on the post-Cold War agenda in response to a mixture of technological innovations and changing geopolitical conditions. Cyber security was first used by computer scientists in the early 1990's to underline a series of insecurities related to networked computers, but it moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects (Nissenbaum 2005). Throughout the 1990's these warnings were increasingly validated by prominent American politicians, private corporations and the media who spoke about 'electronic Pearl Harbors' and 'weapons of mass disruption' thereby conjuring grave threats to the Western world (Bendrath 2003, 50-53; Nissenbaum 2005, 67; Yould 2003, 84-88). The events on September 11 further spurred the attention given to computers, information technology and security, not least to questions of digital infrastructure protection, electronic surveillance, the terrorist use of hacking, and the Internet as a networked platform for communication across and against states (Latham 2003, 1). Outside the United States, non-democratic regimes, most conspicuously China, have repeatedly sought to block their citizens' access to those parts of the Internet considered threatening to political and societal stability. More recently, the 2007 large-scale digital attacks on Estonian public and private institutions in response to the government's removal of a World War II memorial were labeled the first war in cyberspace and NATO replied by declaring the protection of information systems a crucial component of its force transformation (North Atlantic Council 2007; *The New York Times* 2007).

Constituting something as a 'security problem' while simultaneously defining something as *not* has significant consequences in that it endows 'the problem' with a status and priority that 'non-security problems' do not have. Normatively it is therefore crucial that Security Studies engage the conceptualizations of security that are mobilized within policy discourse – be those environmental, health, or cyber security - even if the conclusion is to argue that the implications of such security discourses are problematic (Buzan, Wæver and de Wilde 1998, 29; Deudney 1990; Huysmans 2006, 124-144). Yet, in spite of the widespread references to cyber insecurities in policy, media and Computer Science discourses there has been surprisingly little explicit discussion within Security Studies of what hyphenating 'security' with 'cyber' might imply. To take a recent example the broadly conceived textbook, *Contemporary Security Studies* edited by Alan Collins has no entries for 'cyber security', 'computers', 'critical infrastructure', 'information security', or 'networks' (Collins 2007). Those Security Studies scholars who do address cyber related themes employ 'adjacent concepts' - 'cyber war' (Arquilla and Ronfeldt 1993; Der Derian 1992), 'netwar' and 'network security' (Arquilla and Ronfeldt 1996, 2001; Deibert and Stein 2002; Der Derian 2003), 'critical infrastructure protection' (Bendrath 2003), and 'information security' and 'information warfare' (Deibert 2003; Denning 1999; Der Derian 2003, 453; Latham 2003) – terms that overlap, but also have distinctive meanings that separate them from cyber security.

This article seeks to address this gap in Security Studies adopting the Copenhagen School's theory of securitization as its starting point. [2] The Copenhagen School has won wide acclaim as 'the most thorough and continuous exploration' and 'Among the most prominent and influential' approaches to the widening agenda in Security Studies

(Huysmans 1998, 480; Williams 2003, 511) and its understanding of security as a discursive modality with a particular rhetorical structure and political effect makes it particularly suited for a study of the formation and evolution of cyber security discourse. The Copenhagen School argues that security is a speech act that *securitizes*, that is constitutes one or more referent objects, historically the nation or the state, as threatened to their physical or ideational survival and therefore in urgent need of protection (Buzan, Wæver and de Wilde 1998; Wæver 1995; Wæver et al. 1993). Yet the Copenhagen School has dealt with cyber security as an example of an attempted securitization - Pentagon securitizing the catastrophic impact of hacking on critical infrastructures - that is ruled *out* on the grounds that it has 'no cascading effects on other security issues' (Buzan, Wæver and de Wilde 1998, 25). Hence, holds the Copenhagen School in its seminar study *Security: A New Framework for Analysis* from 1998, there is no need to theorize cyber security as a distinct sector akin to the military, the political, the environmental, the societal, the economic and the religious ones (Buzan, Wæver and de Wilde 1998; Laustsen and Wæver 2000).

Much however has changed since the Copenhagen School made this assessment: cyber security *is* successfully securitized as evidenced by such institutional developments as the establishment of the Commission on Critical Infrastructure Protection by President Clinton in 1996, the prominent location of cyber security within the Department of Homeland Security, President Bush's formulation of *The National Strategy to Secure Cyberspace* in 2003, and the creation of a NATO backed cyber defense centre in Estonia in 2008. Nor is it plausible to maintain the view of cyber security as insulated from other sectors of security. Indeed, in Rachel Yould's words (2003, 78) 'it appears that IT may be the common underlying factor upon which all security sectors are destined to converge.' The link to military security is fairly straightforward with digital technologies forming the backbone of the Revolution in Military Affairs (Cavelty 2008; Gray 1997), the securitization of Internet access in countries such as China, Singapore and Myanmar is legitimized through references to national-cultural as well as regime security (Deibert 2002), and the intricate connections between the commercial interests in seamless digital transactions, concerns for privacy protection, and governmental calls for surveillance and data-mining throw up crucial battles between multiple actors speaking on behalf of political, private, societal and corporate security (Saco 1999). This wealth of referent objects, competing securitizing actors, and multiple threat constellations may at first give the impression of a disjointed sector made up by incompatible discourses (Deibert 2002). Yet as this article will show it is indeed possible to develop a theoretical framework that facilitates an understanding of the connections between these discourses as well as of the political and normative implications of constructing cyber issues as security problems rather than as political, economic, criminal or 'purely' technical ones.[3]

The main goal of this article is thus to identify and locate cyber security as a particular sector on the broader terrain of Security Studies.[4] Sectors are, hold the Copenhagen School lenses or discourses rather than objectively existing phenomena and they are defined by particular constitutions of referent objects and types of threats as well as by specific forms or 'grammars' of securitization (Buzan, Wæver and de Wilde 1998, 27). Theorizing the cyber security sector therefore requires that we address the following questions: What threats and referent objects characterize cyber security; what distinguishes it from other security sectors; how may concrete instances of cyber securitizations be analyzed; and what may critical security scholars learn from taking cyber discourse seriously? The article answers these questions by proceeding through four steps. The first part of the article

introduces securitization theory with a particular emphasis on the relationship between individual and collective referent objects and on the relationship between public and private spheres of society. The second part of the article investigates the genesis of cyber security discourse showing competing articulations of threats and referent objects. The third part lays out three distinct security modalities that further specify the cyber security sector: *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. The fourth part of the paper addresses the applicability of the suggested theoretical framework through a case-study of the attacks on Estonian public and private digital structures in 2007 and the subsequent discursive and institutional responses. The case-study indicates the applicability of the framework beyond the American context and is furthermore a critical case for when and how securitizations may succeed as the attacks were widely described as the first war in cyber space.

The conclusion sums up what expanding the Copenhagen School to include cyber security entails with a particular view to the implications of our study for the wider debates over the normative and conceptual implications of securitization theory.[5] Although this paper takes the Copenhagen School's securitization theory as its starting point its ambition is not merely to add a cyber security sector to the existing framework, but to speak to critical debates over how to theorize the referent object, the politics and epistemology of who can securitize and who cannot, and whether desecuritization – the move out of a logic of security and into a political or a technical one – is desirable. Critical engagements with the Copenhagen School framework are therefore introduced throughout the article as the case of cyber security throws critical and in several respects new light upon contemporary securitization debates.

Securitization Theory

Over the past 15 years, the Copenhagen School has been successful in capturing the middle ground of the widening debate in Security Studies. Known most prominently for its concepts of securitization and societal security (Buzan, Wæver and de Wilde 1998; Wæver 1995; Wæver et al. 1993), it has been applied to a number of empirical contexts and problems including ethnic conflict (Roe 2005), HIV/AIDS (Elbe 2006) and trafficking (Jackson 2006). It has become the focal point for important theoretical debates on the normative implications of security discourse (Erikson 1999; Huysmans 2006; Williams 2003), the consequences of speech act epistemology (Bigo 2002; Balzacq 2005; Hansen 2000), the Western-centric status of security (Bubandt 2005; Kent 2006; Wilkinson 2007), and the importance of the media and visual representations (Hansen 2008; Williams 2003).

The Copenhagen School has three main theoretical roots, one in debates in Security Studies over whether to widen the concept beyond its traditional state-centric, military focus, one in speech act theory, and one in a classical, Schmittian understanding of the state and security politics (Huysmans 2006, 124-44; Williams 2003). Combining these influences, the general concept of 'security' is drawn from its constitution within *national* security discourse, which implies an emphasis on authority, the confronting – and construction - of threats and enemies, an ability to make decisions and the adoption of emergency measures. Security has a particular discursive and political force and is a concept that does something

– *securitize* - rather than an objective (or subjective) condition. 'Thus the exact *definition* and *criteria* of securitization is constituted by the intersubjective establishment of an existential threat with a saliency sufficient to have substantial political effects' (Buzan, Wæver and de Wilde 1998, 25). 'Saying' security defines something as threatening and in need of urgent response, and securitization should therefore be studied in discourse, 'When does an argument with this particular rhetorical and semiotic structure achieve sufficient effect to make an audience tolerate violations of rules that would otherwise have to be obeyed?' (Buzan, Wæver and de Wilde 1998, 25) Security 'frames the issue either as a special kind of politics or as above politics' and a spectrum can therefore be defined ranging public issues from the *nonpoliticized* ('the state does not deal with it and it is not in any other way made an issue of public debate and decision'), through *politicized* ('the issue is part of public policy, requiring government decision and resource allocations or, more rarely, some other form of communal governance') to *securitization* (in which case an issue is no longer debated as a political question, but dealt with at an accelerated pace and in ways that may violate normal legal and social rules) (Buzan, Wæver and de Wilde 1998, 23). This however effectively constitutes the nonpoliticized as an empty category (for an issue to be *public* rather than *private* it must presumably be either the subject of public policy, or it must be brought to the attention of the public) and since virtually all public issues are subjected to some form of regulation we find it more appropriate to redefine nonpoliticized issues as those which do not command political and/or media attention and which are regulated through consensual and technical measures; and politicized issues as those which are devoted close media and political scrutiny, generating debate and usually multiple policy approaches, while not commanding the threat-urgency modality of securitization.

Having emphasized the urgency requirement of security, the Copenhagen School argues that security discourse may constitute other referent objects than the state/nation as threatened and bring in other sectors than the military as long as this happens with the drama and saliency of national/international security and is accepted by the relevant audience. This broadening led to an explicit theorization of 'societal security' as 'the ability of a society to persist in its essential character under changing conditions and possible or actual threats', an expansion that allowed for the identification of security problems where national, religious, ethnic or racial groups feel threatened rather than protected by 'their' state (Wæver et al. 1993, 23-26). The discursive articulation of urgency and extreme measures is thus central to the Copenhagen School's delineation of the boundary between 'security proper' and concepts that bear only a semantic semblance to 'security' and hence also to how referent objects are defined. Thus 'social security' is for instance defined as 'about individuals' (and thus not about collective referent objects as in 'international security') and 'largely economic' (rather than 'security') (Buzan, Wæver and de Wilde 1998, 120) – neither are 'investment securities', or insecurities related to crime or unemployment 'real' securities (Buzan, Wæver and de Wilde 1998, 104).[6] Methodologically, there is a certain ambiguity in securitization theory as it argues that the utterance of the word 'security' is not the decisive criteria and that a securitization might consist of 'only a metaphorical security reference' (Buzan, Wæver and de Wilde 1998, 27). Yet what this entails has not been further explored, and the majority of the theory leans in the direction of a more explicit verbal speech act methodology.

The Copenhagen School has modified its earlier refusal of a concept of individual security, but it still privileges collective security concepts and tends to replicate Security Studies' traditional juxtaposition of individual and collective security (Hansen 2000; McSweeney

1996). 'In practice, the middle scale of limited collectivities has proved the most amenable to securitization of durable referent objects', and 'Security is an area of competing actors, but it is a biased one in which the state is still generally privileged as the actor historically endowed with security tasks and most adequately structured for this purpose' (Buzan, Wæver and de Wilde 1998, 36-37). This state/nation-individual dichotomy does however lock the Copenhagen School - and Security Studies - into a ritualized debate which downplays how political thought from the mid 17th century onwards has constituted security as a '*relationship* between individuals and states or societies' not as an either-or (Rothschild 1995, 61). The individual and the state are united in that the principle of state sovereignty implies that the individual allocates authority and power to the state in exchange for the state's protection of her/his security (Walker 1990; Williams 1998). To define security as 'national security' is thus implicitly to articulate an abstract conception of individual security as provided by the (idealized) state. On the other hand, to articulate security as 'individual security' – as most of Human Security, Critical Security Studies, and Feminist approaches still do - necessitates a collective conception of how and by whom the securities of individuals are going to be negotiated. Since 'individuals' do not appear in political discourse as free-standing entities, but with gendered, racial, religious, class and other collective identities, there is always going to be a tension between the different forms in which the individual can be constituted. A call for individual security against the atrocities - or even, merely overreaching - of the state is thus always also implicitly a call for an alternative political community and authority.

The concept of national security has proved remarkably stable precisely because it is linked to the principle of state sovereignty which offers a powerful resolution to questions of identity, order and authority (Walker 1990). Yet, while 'security' in the form of the political modality of national security (that is as threats, dangers, and emergency decisions) is as resilient as the state, neither the state nor 'security' is uncontested or incontestable. Both depend on political and academic practices for the reproduction of their status, and the question thus becomes whether the discourse on cyber security reinforces the state/nation as a referent object, how individual responsibility is articulated to support (or challenge) collective security and authority, and whether this rearticulates the understanding of 'security politics' itself.

Securitizing digital systems: the referent objects of cyber security

The history of cyber security as a securitizing concept begins with the disciplines of Computer and Information Science. One, if not the first usage of cyber security was in the Computer Science and Telecommunications Board's (CSTB) report from 1991, *Computers at Risk: Safe Computing in the Information Age* which defined 'security' as the 'protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves' (CSTB 1991, 2). Security comprised technical as well as human aspects and 'it has significant procedural, administrative, physical facility, and personnel components' (CSTB 1991, 17). Crucially, threats to cyber security do not only arise from (usually) intentional *agents*, but also from *systemic* threats. These systemic threats, defined by Hundley and Anderson (1995/96, 232) as 'cyberspace safety' stems from the inherent unpredictability of computers and information systems which by themselves 'create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded'. Threats arise from software as well as hardware failures and cannot be corrected through perfecting digital

technology and programming, there is in short an inherent ontological insecurity within computer systems (Denning 1999, 12; Edwards 1996, 290-292).

'Computer security' would not however in most cases by itself qualify as a security concept according to the Copenhagen School. As Helen Nissenbaum points out, the majority of computer scientists adopt a technical discourse that is focused on developing good programs with a limited number of (serious) bugs and systems that are difficult to penetrate by outside attackers. In the move from 'computer security' to 'cyber security', this technical discourse is however linked to the securitizing discourse 'developed in the specialized arena of national security' (Nissenbaum 2005, 65). 'Cyber security' can in short be seen as 'computer security' plus 'securitization'. In the 1991 CSTB report it is argued that 'We are at risk' and in a remarkable mobilization of securitizing prose that 'Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb'. No major attacks have been launched so far, but it is a key element of securitizing discourse to argue that if action is not undertaken then serious incidents will materialize in the near future, thus 'there is reason to believe that our luck will soon run out' (CSTB 1991, 7-8). The constitution of a much too complacent audience that does not realize the magnitude of these dangers is another key staple of securitizing discourse, and the CSTB laments that 'Very few individuals not professionally concerned with security … have ever been directly involved in or affected by a computer security incident. … most people have difficulty relating to the intricacies of malicious computer actions' (CSTB 1991, 159-61). 11 years later most Americans have been exposed to (scares of) computer viruses, worms and hackers, yet the Board complains that in spite of the reports produced over the past years, 'not much has changed with respect to security as it is practiced'. As the threats to cyber security have increased while the countermeasures have not, 'our ability and willingness to deal with threats have, on balance, changed for the worse' (CSTB 2002, 2). In another attempt to stress the urgency and wake up policy makers and the broader public the report is titled *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. A similar tone is struck a year later in the so far most authoritative and comprehensive statement of US cyber security policy, President Bush's *The National Strategy to Secure Cyberspace* which opens by asserting that 'In the past few years, threats in cyberspace have risen dramatically'. Although a large-scale cyber attack has not yet taken place, this is no time to 'be too sanguine' as 'the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving' (*The National Strategy* 2003, viii).

Key to understanding the potential magnitude of cyber threats is the networked character of computer systems. These networks 'control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars' (*The National Strategy* 2003, 6-7) and attacks – or 'cyberdisasters' - would 'compromise systems and networks in ways that could render communications and electric power distribution difficult or impossible, disrupt transportation and shipping, disable financial transactions, and result in the theft of large amounts of money' (CSTB 2002, 6). Although not necessarily directly connected the magnitude and simultaneity of these attacks would have cascading effects and thus networked consequences for referent objects beyond networks themselves. Networked computers have also dissolved the traditional boundary protecting the territorial nation state, 'the infrastructure that makes up cyberspace – software and hardware – is global in its design and development' and cyber attacks may operate at a distance obfuscating 'their identities, locations, and paths of entry' (*The National Strategy* 2003, 7; Yould 2003). To give

an indication of how an attack transgresses territorial boundaries, RAND's 'The Day After… in Cyberspace II' exercise in 1996 drew up a list (Anderson and Hearn 1996, 4-5) including electronic looting of European and American banks by (unspecified) Russians, software computer viruses causing financial havoc and plane and train crashes, power grid fall outs at airbases, malfunctioning of ATMs and news broadcasts, and stock market manipulation.

RAND's scenario shows aptly how cyber security discourse moves seamlessly across distinctions normally deemed crucial to Security Studies: between individual and collective security, between public authorities and private institutions, and between economic and political-military security. The private sector's fear of hackers stealing large sums of money, intellectual property owner's worry that file sharing compromises their rights and revenues (Nissenbaum 2005, 68), and public, private, and civil society scares that bugged software and computer viruses will have damaging consequences produce a powerful blending of private-economic and public-national security concerns. Not only are large parts of the networks, the hardware, and software privately produced and owned and thus governed by financial considerations, but the security logics of the economic and the cyber sector have crucial similarities. The economic sector is also 'rich in referent objects, ranging from individuals through classes and states to the abstract and complex system of the global market itself' (Buzan, Wæver and de Wilde 1998, 100) and in liberal economies instability and risk taking is built into the logic of capitalism itself. The modern economic system is, like the cyber network, constituted by trans-border flows, and authority and sovereignty is more ambiguously located than in traditional national-military security. It is in both sectors often difficult to identify where an attack originated, and with the global reach of the Internet/world economy, tricky questions of responsibility and enforcement are continuous sources of fraught cross-border and international treaty negotiations. That said, cyber security does not fully mirror the economic sector either: its securitizing potential exceeds that of the economic sector as strictly defined (Buzan, Wæver and de Wilde 1998, 116-7) and this in turn allows – or is an indication of – a much stronger link to national military security. Cyber security is *not* left to the liberal market, but implies a complex constellation of public-private responsibility and governmental authority.

Drawing upon the individual-collective resolution laid out above, the government consistently holds the private sector co-responsible for cyber security: not only does the latter own major parts of the computer network, it also possesses the knowledge – 'In general, the private sector is best equipped and structured to respond to an evolving cyber threat' (*The National Strategy* 2003, ix). Mobilizing civil liberties discourse further invokes a crucial balance between the public and the private that should not be violated: 'The federal government should likewise not intrude into homes and small businesses, into universities, or state and local agencies and departments to create secure computer networks' (*The National Strategy* 2003, 11). To the government this allows for a distribution of the financial and political burden and it strategically engages critics who point to privacy violations. To the private sector, these securitizations boost its calls for the protection of intellectual property rights, for vigilant prosecution of cyber crimes, and for combating digital anonymity (Nissenbaum 2005, 68). Negotiation of the boundaries between the public and the private and between the economic and the political thus couples the network-fragmentation implied by 'cyber' with an understanding of business and government as sharing the same goal. At the same time the political center still constitutes the private sector as responsible for major parts of the digital realm.

This academic and policy discourse articulates in sum a wide array of threats to government, business, individuals, and society as a whole perpetuated by hackers, criminals, terrorists, commercial organizations, and nations that adopt cyber strategies for financial, ideological, political or military gain (Hundley and Anderson 1995/1996, 232). Yet obviously not all political or societal actors concur with the manner in which official American cyber security discourse has attempted to keep the public-private and individual-state resolutions in place. As Ronald J. Deibert (2002) and Diana Saco (1999) have argued cyber security is a terrain on which multiple discourses and (in)securities compete.[7] Privacy advocates and cyber libertarians point to governmental violations of personal security (Saco 1999), and authoritarian (and not so authoritarian) regimes securitize transborder information flows as threats to regime/state security and national (societal) identity in a way that expands the threat-referent object constellation considerably (Deibert 2002). The question is therefore how we incorporate this complexity into our theoretical framework without loosing the sense of cyber security discourse as a distinct phenomenon? Deibert (2002) argues that cyber security is constituted through four separate discourses with distinct referent objects, threats, policy options, and world orders: national security, state security (comprising external threats to state sovereignty as well as internal threats to regime security), private security, and network security and Saco holds that national and personal security compete (Saco 1999, 270, 286).

We agree with Deibert and Saco that cyber security should be theorized as a sector where multiple discourses may be found, yet we think that understanding this multi-discursivity as arising from *competing* articulations of *constellations* of referent objects, rather than separate referent objects, better captures the securitizing and political dynamic of the field. To see cyber security discourse as fragmenting along the lines of distinct referent objects downplays the ways in which cyber security discourse gains its coherence from making connections between referent objects rather than operating at separate tracks. Particularly crucial in the case of cyber security is the linkage between 'networks' and 'individual' and human collective referent objects. Thus it is not the case that a private security discourse constitutes the individual as its referent object, but rather that 'the individual' of this discourse is linked to societal and political referent objects. Take the example of post-September 11 battles between governmental discourses legitimizing digital surveillance and data-mining through securitizing reference to the War on Terror and citizens groups fighting this legislation through reference to basic civic liberties and privacy issues. These are not two separate discourses with unrelated referent objects, but *competing* articulations of the appropriate individual-state contracts of the liberal state (Saco 1999, 290). Moreover, it is not fully clear from Deibert's and Saco's accounts whether private security discourse operates through the political rather than the semantic modality of security. This does not mean that cyber 'privacy' cannot be securitized, but this has to be mediated through a collective referent object, either a political-ideological one, questioning the appropriateness of the individual-state balance, and/or a national-societal one, mobilizing the values held to be the core of the community's identity. Similarly, a securitization of the network cannot, and does not, stop at the network itself: it is the *implications* of network break-downs for other referent objects, 'society', 'the regime', or 'the economy' (which is again in turn linked to 'state' and 'society') that makes cyber securitization a plausible candidate for political and media attention. Securitization works in short by tying referent objects together, particularly by providing a link between those that do not explicitly invoke a bounded human collectively, such as 'network' or 'individual', with those that do. Contestation and multi-

discursivity is thus found between competing articulations of linked referent objects as well as by tracing the potential internal instability of each discourse.

The specific grammar of the cyber security sector

The Copenhagen School has argued that sectors are defined by the specific ways in which distinct 'sub-forms' or grammars of securitization tie referent objects, threats and securitizing actors together (Buzan, Wæver and de Wilde 1998, 27). This section delineates three security modalities that are specific to the cyber sector. As the discussion below lays out in more detail, even though other sectors may exhibit features that resonate with these to some extent, their acuteness is distinct to the cyber sector as is, crucially, their interplay.

Hypersecuritization

The first concept, *hypersecuritization*, has been introduced by Buzan (2004, 172) to describe an expansion of securitization beyond a 'normal' level of threats and dangers by defining 'a tendency both to exaggerate threats and to resort to excessive countermeasures' (Buzan 2004, 172). This definition has an objectivist ring to it in that to identify 'exaggerated' threats implies that there are 'real' threats that are not exaggerated. Moreover, the question of whether a securitization is seen as 'exaggerating' concerns the degree to which it is successful (unsuccessful securitizations are seen as 'exaggerating') and is not part of the grammatical specificities of sectors. Thus we suggest to drop the 'exaggerated' from the definition of hypersecuritization and to apply it to the cyber sector to identify the striking manner in which cyber security discourse hinges on multi-dimensional cyber disaster scenarios that pack a long list of severe threats into a monumental cascading sequence *and* the fact that neither of these scenarios has so far taken place.

All securitizations do of course have an element of the hypothetical in that they constitute threats that must be countered, and thus mobilize an 'if-then' logic, but what distinguishes hypersecuritizations from 'mere' securitization is their instantaneity and inter-locking effects (Denning 1999, xiii; *The National Strategy* 2003, 29). This combination draws critically from the securitization of the network (Deibert 2002), yet the power of hypersecuritization stems not only from a securitization of the network itself, but from how a damaged network would cause societal, financial, and military break-down hence bringing in all other referent objects and sectors.

Securitizations always mobilize the specter of the future to some extent, but most nevertheless articulate the past as a legitimating reference that underscores the gravity of the situation. Looking to the Cold War, the logic of nuclear deterrence relied upon projections of a nuclear exchange that had not taken place, yet there were the devastations of Hiroshima and Nagasaki to be used as a yardstick for what nuclear war would imply. Cyber securitizations on the other hand have no similar history of founding incidents to base themselves on but try to conjure historical analogies such as 'electronic Pearl Harbors' (Bendrath 2003, 50).[8] The combination of cascading disasters and the absence of a prior incident of that magnitude creates a crucial ambiguity within cyber security discourse. The extreme reliance on the future and the enormity of the threats claimed at stake makes the discourse susceptible to charges of 'exaggeration', yet the scale of the potential catastrophe simultaneously raises the stakes attached to ignoring the warnings.[9] Turning the absence of

prior incidences in the opposite direction, the difficulty of saying that it could not happen also creates a powerful space for the projection of the (im)possible.

The hypersecuritization of the entire network in cyber security creates an obvious resemblance to environmental security discourse where the fate of the planet is claimed at stake. Both discourses also emphasize irreversibility: once a species is extinct or a digital system gone, they can never be recreated in full. Yet, there are also crucial differences between the two discourses. First, the speed of the threat scenarios differ with cyber security gaining its power from the instantaneity of the cascading effects whereas environmental security usually allows for a gradual accumulation of threats and dangers until a certain threshold may be reached and events accelerate. This establishes different modalities of urgency and hence different spaces for political intervention.[10] Second, there is a crucial difference in terms of the possibility of visualizing threats, and hence for how securitizing actors communicate to their audiences (Williams 2003). The digital, networked character of cyber security – and the absence of prior disasters – is hard to represent through images, whereas environmental security discourse may mobilize for example endangered and extinct species as well as melting ice caps and forests devastated by acid rain or clear-cutting.

Everyday security practice

The second grammar of cyber security, *everyday security practices*, points to the way in which securitizing actors, including private organizations and businesses, mobilize 'normal' individuals' experiences in two ways: to secure the individual's partnership and compliance in protecting network security and to make hypersecuritization scenarios more plausible by linking elements of the disaster scenario to experiences familiar from everyday life.[11] Everyday security practices do not reinstall a de-collectivized concept of individual security, but underscore that the acceptance of public security discourses may be facilitated by a resonance with an audience's lived, concrete experiences. The concept of audience is only briefly defined by Buzan, Wæver and de Wilde (1998, 41) as 'those the securitizing act attempts to convince' and Thierry Balzacq has in a further development of the concept suggested that 'the success of securitization is highly contingent upon the securitizing actor's ability to identify with the audience's feelings, needs and interests', and that 'the speaker has to tune his/her language to the audience's experience' (Balzacq 2005, 184). Audiences do not exist 'out there' but are constituted in discourse and security discourses draw boundaries around the 'we' on whose behalf they claim to speak, and the 'you's' who are simultaneously addressed by the linking of fears and threats to 'feelings, needs and interests'. As Althusser's concept of interpellation underscores, subject positions are simultaneously constituted and individuals are called upon to identify with these. Yet, although the audience is discursively constituted, securitizing actors are not at liberty to construct independently of institutionalized subject formations.

Although elements of everyday securizations may be found in other sectors as well, they come out particularly strikingly in the case of cyber security. There is for example a marked difference between Cold War military securitizations of nuclear Holocaust which implied the obliteration of everyday life, and the securitizations of everyday digital life with its dangers of credit card fraud, identity theft and email scamming. Those few who do not own or have computers at work are nevertheless subjected to the consequences of digitization. For example, on June 4-5, 2007 20.000 Danes did not receive their medication

due to a server breakdown at the Danish Medicines Agency which routes all prescriptions from doctors to pharmacies. Even the sector with closest resemblance, the environmental one, still is unable to conjure and capitalize on a similar sense of immediate individual danger and experience (depleting the ozone layer while accumulating frequent flyer miles as opposed to downloading software that inadvertently provides outsider access to one's Internet banking) – and thus responsibilities. These experiences of threats are not, as the Copenhagen School might have it, cases of 'individual security' or 'crime', but are constituted as threats to the network and hence to society.

Cyber securitizations of everyday life are distinct furthermore in their constitution of the individual not only as a responsible partner in fighting insecurity, but also as a liability or indeed a threat. Hence both public and private actors mobilize expert positions and rhetoric constituting 'its' audience as one who *should* be concerned with its security. Adopting a simultaneously educational and securitizing discourse, OnGuard Online, set up by the Federal Trade Commission, warns for instance that through peer-to-peer file sharing 'You may download material that is protected by the copyright laws and find yourself mired in legal issues. You may download a virus or facilitate a security breach. Or you may unwittingly download pornography labeled as something else' (OnGuard 2008). The constitution of the digital as a dangerous space and the 'ordinary' individual as an ambiguous partner *and* a potential threat is supported by medical metaphors like 'viruses' and 'infected computers' that underscore the need for 'caution' and 'protection'. As in discourses of epidemics and contagion, cyber insecurities are generated by individuals who behave irresponsibly thus compromising the health of the whole. *The National Strategy* (2003, 11) proclaims that 'Each American who depends on cyberspace, the network of information networks, must secure the part that they own or for which they are responsible' and FBI officials have suggested driver licenses for computer-owners (*The Economist* 2007a). A particular concern stems from the fact that computers may be infected with software that allows them to be used by attackers to route emails or launch denial of service attacks with no immediate effect to the owner. Connecting everyday security practices with hyper cascading scenarios, it is this inadvertent or careless behavior within a networked system that move cyber security out of the realm of 'corporate security' or 'consumer trust' and into the modality of 'proper' national/societal security. Moreover, there is a further link between hypersecuritizations and everyday practices in that the claim about the possibilities of disasters happening may be substantiated by the reference to individuals' everyday experiences: the looting of Western banks by Russians and/or terrorists hackers in RAND's scenarios described above may seem much more credible if one's own credit card has been abused on-line.

The challenges generated by the securitization of digital everyday life for governmental authorities as well as private businesses are thus quite significant. Neither wishes the broader public to become so petrified that it evacuates the digital, but they simultaneously install an individual moral responsibility that may easily move the subject from helpless to careless to dangerous. The broad institutional support behind initiatives such as OnGuard Online, which is set up by the Federal Trade Commission and a long series of partners, including the Department for Homeland Security, the National Consumers League and a series of other nonprofit nongovernmental organizations may furthermore be one that makes resistance difficult. Linking back to the critical argument of securitization theory, namely that 'security' provides governments with the discursive and political legitimacy to

adopt radical measures, the question becomes at which point and how these strategies, and their harmonious constitution of state-society relations, can become contested.

Technification

The strong emphasis on the hypothetical in cyber securitizations create a particular space for technical, expert discourse. As Nissenbaum (2005, 72) points out, the knowledge required to master the field of computer security is daunting and often not available to the broader public, including Security Studies scholars. The breathtaking pace at which new technologies and hence methods of attacks are introduced (Denning 1999, xvi) further adds to the legitimacy granted to experts and the epistemic authority which computer and information scientists hold allow them the privileged role as those who have the authority to speak about the unknown. In the case of cyber security, experts have been capable of defying Huysmans' (2006, 9) description of the invisible role of security experts as they have transcended their specific scientific locations to speak to the broader public in a move that is both facilitated by and works to support cyber securitizations claimed by politicians and the media.

As in most academic fields, computer scientists have disagreed on the likelihood of different forms of attacks, and since the field is also cloaked in military or business secrecy, the 'normal' follower of these debates learns that 'that much is withheld or simply not known, and estimates of damage strategically either wildly exaggerated or understated' (Nissenbaum 2005, 72). These fluctuations also facilitate a coupling of radical threats with techno-utopian solutions.[12] *The National Strategy* for instance couples a series of securitizations with an exuberant faith in the development of 'highly secure, trust-worthy, and resilient computer systems. In the future, working with a computer, the Internet, or any other cyber system may become as dependable as turning on the lights or the water' (*The National Strategy* 2003, 35). Leaving aside that for the majority of the world's poor, and even for the impoverished American, turning on the light or water may not be entirely dependable this echoes a technological utopianism that sidesteps the systemic, inherent ontological insecurity that computer scientists consistently emphasize. It also invokes an inherent tension between disaster and utopia as the future of cyber security.

The constitution of expert authority in cyber technifications invokes furthermore the tenuous relationship between 'good' knowledge and 'bad' knowledge, between the computer scientist and the hacker. The hacker, argues Nissenbaum (2004), has undergone a critical shift in Western policy and media discourse, moving from a previous subject position as geeky, apolitical, and driven by the boyish challenge of breaking the codes to one of thieves, vandals and even terrorists.[13] Although 'hackers' as well as others speaking on behalf of 'hacktivista' – the use of hacking for dissident, normatively desirable purposes – have tried to reclaim the term (Deibert 2003), both official and dissident discourse converge in their underscoring of the general securitization of the cyber sector insofar as past political hacker naivety is no longer possible.

The privileged role allocated to computer and information scientists within cyber security discourse is in part a product of the logic of securitization itself: if cyber security is so crucial it should not be left to amateurs. Computer scientists and engineers are however not only experts, but *technical* ones and to constitute cyber security as their domain is to technify cyber security. Technifications are, as securitizations, speech acts that 'do something' rather

than merely describe and they construct an issue as reliant upon technical, expert knowledge, but they also simultaneously presuppose a politically and normatively neutral agenda that technology serves. The mobilization of technification within a logic of securitization is thus one that allows for a particular constitution of epistemic authority and political legitimacy (Huysmans 2006, 6-9). It constructs the technical as a domain requiring an expertise that the public (and most politicians) do not have and this in turn allows 'experts' to become securitizing actors while distinguishing themselves from the 'politicking' of politicians and other 'political' actors. Cyber security discourse's simultaneous securitization and technification work to prevent it from being politicized in that it is precisely through rational, technical discourse that securitization may 'hide' its own political roots.[14] The technical and the securitized should therefore not be seen as opposed realms or disjunct discursive modalities, but as deployable in complex, interlocking ways; not least by those securitizing actors who seek to depoliticize their discourses' threat and enemy constructions through linkages to 'neutral' technologies. A securitization by contrast inevitably draws public attention to what is done in the name of security and this provides a more direct point of critical engagement for those wishing to challenge these practices than if these were constituted as technical.

The Copenhagen School has stated desecuritization, the movement of an issue out of the realm of security and into the realm of the politicized as 'the optimal long-range option, since it means not to have issues phrased as "threats against which we have countermeasures" but to move them out of this threat-defense sequence and into the ordinary public sphere' (Buzan, Wæver and de Wilde 1998, 29). Taking the concept of technification to recent debates over whether and when desecuritization is political and normatively desirable (Elbe 2006; Huysmans 2006, 124-144; Williams 2003), we can add that one should be careful to distinguish a technification that depoliticizes a securitized issue, thereby taking it out of the realm of the political, from a 'proper' desecuritization that allows for contestations and hence political debate.

Technifications play a crucial role in legitimating cyber securitizations, on their own as well as in supporting hypersecuritizations and in speaking with authority to the public about the significance of its everyday practices. Expert knowledge is obviously not exclusive to the cyber sector and a significant nodal point in environmental security debates is for instance discussions of the scientific reliability of predictions about global warming, resource depletion and population growth. Military security discourse is likewise concerned with the technicalities of surveillance, SDI and remotely controlled bombings. Yet, if technifications are not exclusive to the cyber sector, they have been able to take on a more privileged position than in any other security sector. Comparing it to the public debates over environmental security, in the case of the latter the audience is expected to know more and the repeated contestation of environmental 'evidence' makes for a public view of (some) environmental actors as political ones rather than apolitical, 'objective' experts. This is not to say that computer security is objectively more technical or less political than environmental science, but simply that the socially constituted audience-expert subject positions differ and that these difference – open to historical change themselves – are important for how securitizations are legitimated or challenged.

Applying the cyber security sector: the case of Estonia

In April-May 2007, distributed denial of service attacks brought down the websites of the Estonian President, Parliament, a series of government agencies, the news media, the two largest banks, and website defamations included a fake apology letter posted by the Prime Minister (Landler and Markoff 2007) his photo being adorned by a Hitler mustache (Finn 2007). *The New York Times* called this 'the first real war in cyberspace', the Estonian defense minister defined it as 'a national security situation' (Landler and Markoff 2007) and the chairman of Estonia's cyber-defense coordination committee went as far as describing it as 'a kind of terrorism' (Blomfield 2007). The prelude to this cyber securitization was set off-line and arose from Estonian authorities' decision to remove a memorial commemorating the Soviet sacrifices during World War II from a park in the center of Tallinn to a military graveyard farther afield. This act was constituted by a significant proportion of the ethnic Russian minority as a threat to their cultural and political status: large demonstrations led to the arrest of 1300 people, the injury of 100, and the death of one (Traynor 2007). Ethnic Estonians on their part constituted the memorial as a residue of Soviet inter-war and Cold War occupation, and the removal as significant for the manifestation of cultural identity and the demarcation of political sovereignty vis a vis Russia. The memorial incident thus crystallized co-constitutive Estonian and Russian-Estonian securitizations of societal as well as political referent objects.

As the demonstrations spread from the streets to the Internet, Estonian authorities' cyber securitization articulated attacks on the network as threats to Estonian political sovereignty as well as cultural and national identity. In the words of Linnar Viik, a government IT consultant, 'This is not some virtual world. This is part of our independence. And these attacks were an attempt to take one country back to the cave, back to the Stone Age.' (Finn 2007) Both government and corporate actors have branded 'E-stonia' as the frontrunner of digital modernity and made this a crucial element in the differentiation between Western Estonia and the Soviet past – and Russian present - it has fortunately escaped (Michaels 2007). The significance of national pride also fed into explaining the importance bestowed upon the defamation of the Prime Minister's websites.[15] The gravity of the situation was underscored by a further coupling of 'network' to 'state' and 'society'. The break-down of the network meant that Estonians could not get in touch with public authorities (governmental websites were down), conduct crucial private transactions (the two largest banks were hit), get information about what was going on (media websites were targeted), or trust what was posted by ostensibly trustworthy authorities (defamations of the Prime Minister's website). By linking to central everyday practices like banking, communicating with public authorities and reading on-line news, 'individual security' was thus constructed as directly compromised and the audience outside of Estonia was reminded what cyber war could entail for their own digital routines.

The ability of Estonian securitizing actors to have the attacks accepted as 'the first war in cyberspace' and to have them prominently covered by the world press makes for at least a partially successful case of cybersecuritization. British and American newspapers ran a large number of stories on the issue with editorials in *The Washington Times* and *The New York Times* defining it as a 'very real example of cyberwarfare' and the 'first real war in cyberspace' urging NATO to take on a greater role in 'collective cyber-security' (*New York Times* 2007; *Washington Times* 2007). *The New York Times'* held (2007) that the attacks 'should put the computer-dependent world on full notice that there can be many offensive forms of information warfare and figuring out how to stop it – and ultimately who is behind it – is essential to all of our security'. Yet, in spite of the invocation of 'warfare',

Estonian authorities had difficulties convincing their primary international audience, its NATO allies that the attacks constituted an attack on Estonia's political sovereignty, and hence that NATO's Article 5 should be invoked. As Estonia's defense minister, Jaak Aaviksoo complained, 'At present, NATO does not define cyber-attacks as a clear military action' (Traynor 2007). This did not mean that there was no allied support at all: NATO, the EU and Pentagon did dispatch cyber security teams, NATO put information systems on its force transformation agenda and over the course of the next year adopted a policy on cyber defense, a Cyber Defense Concept, created a Cyber Defense Management Authority and supported the creation of a Cooperative Cyber Defense Centre of Excellence in Estonia's capital Tallinn. These events indicated, in NATO's own words, a shift in its understandings of what cyber defense entailed from protecting its own encrypted structures of communication to protecting the open ones of its member states (NATO 2008).

The partial success of the Estonian securitizations illustrates well that the referent object constellation of 'network', 'society', and 'state sovereignty' makes the cyber sector a particular discursive terrain with challenges as well as opportunities. What worked against a fuller acceptance of the Estonian authorities' discourse was their inability to trace the origin of the attack to an official Russian source. The attacks were conducted through two rounds, and in the first round, Estonian officials claimed they had a trace to IP (Internet Protocol) addresses in Putin's administration. Estonia's foreign minister Urman Paet went as far as stating that 'This is the first time Russia has used these kinds of attacks on another country' (Anderson et al. 2007). Russian officials denied these allegations pointing to the absence of evidence and to the openness of their IP addresses making it quite possible for professional hackers to use them to spoil relations between the two countries (Finn 2007). The inability to pin down origin and establish culpability increased in the next phase as botnets – or zombie computers – were used to launch denial of service attacks. Illustrating the significance of technification, the reporting on these attacks is ripe with computer expert statements and 'facts' proving the cascading effects: attacks are said to have come from about 50 countries (Michaels 2007) including the United States, China, Vietnam, Egypt and Peru (Finn 2007), and to have 'infected up to a quarter of the world's computers' (Blomfield 2007). Some claimed that hackers had rented time on large servers (Landler and Markoff 2007), further boosting the claim that criminal organizations might be involved (Anderson et al. 2007), while others pointed to the events as driven by bottom-up hacktivist forces who had posted instructions on how to hack on Russian websites and chat rooms (*The Washington Times* 2007). The use of botnets played into the securitization of everyday life, as well as into the networked and deterritorialized nature of the attacks, yet, ultimately, there was no accepted evidence of a clear digital trace to Russia and NATO and the EU were careful to distance themselves from this part of the Estonian discourse.

The second challenge that the Estonian securitizations ran up against was that attackers were not able to – or interested in – penetrating critical digital infrastructures that regulate electricity, finance, energy, or traffic. Forcing a bank to close down on-line services for an hour might be hard to constitute as 'war' and as the *Daily Mail* (2007) laconically noted, 'to be frank, in Estonia no one died'. In the words of James Andrew Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, 'The idea that Estonia was brought to its knees – that's when we have to stop sniffing glue' (quoted in Schwartz 2007). In other words, the truly cascading hypersecuritization scenario could hardly be sustained, and skeptics may thus hold that the

Estonian case is quite likely to fade from memory as did the previous events who earned the 'first war in cyberspace' designation, the war over Kosovo and the Zapatista uprising (Denning 2001, 239-40; Gray 1997, 2-6; Ronfeldt et al. 1998).

Yet, skeptics notwithstanding the cyber sector's discursive and political specificity also accounted for the particular success that Estonian authorities *did* garnered. First, the institutionalized status that hypersecuritizations have achieved over the past fifteen years meant that the Estonian attacks, although not being a full-fledged scenario come true, had sufficient resonance therewith to draw strength from this institutionalized securitization while simultaneously boosting the claim that such devastating scenarios might occur. Although unable to territorialize the threat, Estonian allegations that Kremlin masterminded the attacks also resonated with long standing American concerns over China building up cyber attack capabilities (Schwartz 2007; *The Economist* 2007b).

Second, although the links between 'hackers' and Russia proper could not be proven, the securitization of hacking was boosted by Estonian officials describing it as 'terrorism' (Blomfield 2007). Constituted within the specter of the on-going War on Terror, the Estonian case raised 'the possibility of an Al Qaeda-type group replicating it' (IISS 2007), and showed how the US should secure its networks 'against al-Qaeda hackers' (Finn 2007). 'Cyber threats' and 'terrorism' thus entered a process of cross-fertilization where the securitization of one term added to the other: 'cyber threats' supported the claims to the dangerous nature of the 'terrorists', and the 'terrorist' character of the attacks made them more worthy of attention. Crucially, this articulation of terrorist-hacking involved a double de-politicization. First, in that the (potential) substantive grievances that Russian-Estonians may have had never entered government discourse or international media coverage, 'hacking' in other words is 'terrorism' with no legitimate political purpose. At the same time, all hacking is seen as terrorist-political, rather than, as in the earlier discourses on hacking, driven by a juvenile desire to conquer the firewalls. Second, the constitution of the attacks as 'terrorist-hacking' relies upon a simultaneous technification and securitization that cuts short political discussion leaving it to computer experts to design the technical properties that defend systems and trace the offenders.

Conclusion

It has been the ambition of this paper to define and theorize the cyber sector of security working from a discursive, Copenhagen School-inspired perspective. Our analysis focused first on the complexities of the referent object constellations found within this sector and we argued with Deibert and Saco for the need for a theoretical framework that allowed for the identification of multiple discourses and hence contestations within and across geographical and political boundaries. Deibert held that an understanding of multiple discourses should be based on distinct referent objects, but we suggested that a conceptualization of discourses as constellations of connected referent objects better incorporated the political dynamics at the core of security. Central to the cyber security sector was particularly the manner in which the referent objects of 'the network' and 'the individual' were linked to national and regime/state security. We further developed the analytical framework by defining three 'security grammars' distinct to the cyber security sector: hypersecuritizations, everyday security practices, and technifications. Our claim is not that these particular forms of securitizations cannot be found anywhere else, but that they are particularly striking in the cyber sector, and that their interplay gives the sector a

distinct character. The applicability of this framework was then illustrated by a case-study of the 2007 'cyber war' against Estonia.

Let us conclude by reflecting critically on the status of the theoretical framework as well as the challenges that may be ahead in further developing the cyber securitization agenda. First, while our ambition was to design a theoretical framework that captured multiple discourses and contestation, one may argue that the focus on the US as the source of most of the empirical material and the choice of the Estonian war as the case-study gives the analysis a Western-liberal bias. While we have pointed to ambiguities in the dominant discourse as well as to contestations thereof in the US as well as the Estonian case, we have not admittedly devoted explicit attention to those cases Deibert defines as 'regime security', that is the crack down on Internet use in countries like China, Belarus, and Burma. Yet, if one accepts that it is constellations rather than discrete referent objects that tie cyber discourse together, then it follows that the arguments about the constitution of networks and individuals will be of significance for discourses that center on regime stability as well. These discourses will knit together threats to regimes through network insecurities that to a large extent resonate with US discourse, yet couple these to rather different individual, privacy, society, and state configurations. Thus while the cyber security sector framework has a general applicability, it is quite possible that the different referent object configurations that are found in cases of non-democratic regime security have implications for the three grammars of the cyber sector. Studies of such cases may discover that not all of these three are equally relevant in all settings or – more likely, we assume - that catastrophes, everyday experiences, and technifications are significant but that their formulation is impacted by the society-citizen-regime-state configuration.

Second, while suggesting our framework may be applicable outside of a Western context we also do want to heed the recent anthropological critique that the word 'security' may not be used in specific contexts, that it might be used to signify other discursive modalities, and that the very threat-danger-fear-uncertainty discourse that the Copenhagen School defines as securitization is not universal, but 'contextually and historically linked to shifting ontologies of uncertainty' (Bubandt 2005, 291; Kent 2006; Wilkinson 2007). Particularly in cases of regime insecurity it is furthermore important to recognize the limitations of an explicit speech act epistemology that requires that threats are articulated in order to count. As Lene Hansen (2000) has argued, this creates a 'silent security' problem for the Copenhagen School in that those repressed are forced to quell their dissent or be further threatened by articulating their insecurities. Taking the concepts of cyber security suggested here into the context of regime insecurity thus requires an openness to finding other modalities through which insecurity is expressed, for instance by reading digital activities as text. A further challenge of cases of regime insecurity is that these will to a larger extent than the Estonian one - where securitizations were aimed largely at an international audience - concern a domestic audience and hence required linguistic skill and intimate knowledge of the political and social dynamics in place.

The most significant lesson of bringing the Copenhagen School to cyber security may be to foreground the political and normative implications of 'speaking security'. Cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, and from the political to the technified, and it takes an inter-disciplinary effort to asses the implications of the move, and possibly to counter it. Thus while this paper has spoken primarily to an IR audience,

our wider ambition is to create a space for inter-disciplinary discussions across the fields of Computer Science, Political Science, Information Law, Philosophy, Communication, Anthropology, Visual Culture and Science Studies. As the analysis has sought to bring out, cyber security stands at the intersection of multiple disciplines and it is important that both analysis and academic communication is brought to bear upon it. The technical underpinnings of cyber security require for instance that IR scholars acquire some familiarity with the main technical methods and dilemmas and vice versa that computer scientists become more cognizant of the politicized field in which they design and how their decisions might impact the (discursively constituted) trade-offs between security, access, trust, and privacy.

Notes

[1] *Authors' note.* An earlier version of this paper was presented at the 49th Annual Convention of the International Studies Association, San Francisco, March 26-29, 2008, and to the International Relations Research Seminar at the University of Copenhagen, April 23, 2008. We thank Barry Buzan, Terrell Carver, Ulrik Pram Gad, Peter Viggo Jakobsen, Morten Kelstrup, Alan Klæbel, Mark Lacy, Karen Lund Petersen, Cindy Vestergaard, Ole Wæver, Michael C. Williams, Anders Wivel and the three anonymous referees for very constructive and incisive comments. Helen Nissenbaum gratefully acknowledges the support of the U.S. National Science Foundation, grants ITR-0331542 and CNS 0613893, for work relating to this project; Lene Hansen the support of the MODINET (Media and Democracy in the Network Society) project and a travel grant from the Department of Political Science, University of Copenhagen.

[2] Epistemologically, we take a critical constructivist view of security as 'the product of an historical, cultural, and deeply political legacy' (Williams 2007, 17; Walker 1990), and as a discursive and political practice rather than a material condition or a verifiable fact (Baldwin 1997, 12).

[3] We use 'normative' to point to the policies, identities and modes of governance that are invoked by securitizations thus continuing discussions laid out in Elbe (2006), Huysmans (2006) and Williams (2003).

[4] Myriam Dunn Cavelty's (2008) recent book on cyber security and the Copenhagen School adds framing analysis and agenda setting to securitization theory while not discussing the concept of sector at greater length.

[5] In this respect, the analytical ambition is parallel to Deudney's (1990) work on environmental security, Elbe's (2006) on the securitization of HIV/AIDS, or Neocleous's (2006) on social security.

[6] These distinctions have been challenged as in Neocleous's (2006, 380-1) argument that New Deal policies in the 1930's constituted social-economic security with precisely the drama and urgency required by the Copenhagen School.

[7] We are less convinced by Deibert's claim that the material conditions of the communications environment will determine the winning discourse as this constitutes material structures as outside and above political decisions and discursive processes.

[8] The use of science fiction within cyber security literature is thus not as far fetched as it may sound: the popular coinage of Reagan's SDI program as Star Wars exemplified that in the face of unknown coordinates, the imaginary would have to do (Edwards 1996, 288).

[9] The emphasis on catastrophic potentiality of the future resonates with risk theory in the tradition of Ulrich Beck, yet since 'security' rather than 'risk' is the dominant policy as well

as academic concept, it is not pursued in further detail in this paper (see Aradau and van Munster 2007).

[10] The securitization of pandemics shares the instantaneity with cyber security, but is – except for the most gruesome science fiction scenarios – still more containable to parts of the system/globe than cyber security.

[11] Everyday security practices refers to 'normal' citizens/individuals and thus points to a different subject and set of practices than those linked to the 'everyday, ordinary practices' of security professionals identified by Bigo (2002, 73) and Huysmans (2006, 5). We agree with Iver B. Neumann (2002, 628) that practices are discursive 'both in the sense that some practices involve speech acts … and in the sense that practice cannot be thought 'outside of' discourse'.

[12] The most striking example of this fusion of securitization and techno-utopia is perhaps President Reagan's SDI program which has been resuscitated by President George W. Bush.

[13] The constitution of expert-hacker subjectivity also throws light upon the gendering of cyber discourse. The technical realm invokes on the one hand a hypermasculine discourse, yet, the geeky, disembodied subjects that are constituted as its inhabitants works against a straight ahead masculine-feminine gendering. Whether male or female, experts or hackers, the authoritative subjects of cyberspace are generally cast as lacking in their ability to conform to stereotypical notions of gender. Take for instance the constitution of female cyber savvy characters in *The Net*, *Rising Sun*, *Criminal Minds*, and *Navy CSI* as tomboys, disabled, overweight, or punks.

[14] There is general agreement in the cyber security literature that digital technologies were securitized only after the end of the Cold War. Yet as Paul N. Edwards (1996) aptly demonstrates, computer technology and Cold War security discourse were in fact deeply intertwined. It is remarkable how these political roots of computer security have been subsumed by a technical, depoliticized discourse.

[15] The significance of cyber info-war is further evidenced by US military personnel calling for 'clandestinely recruiting or hiring prominent bloggers or other persons of prominence already within the target nation, group, or community to pass the US message' (Kinniburgh and Denning 2006, 9) and claims that 'Coalition forces are now less concerned with an insurgent's use of viruses and other malware than with these cyber-related issues of mobilization and manipulation' (Thomas 2006, 24).

References

Anderson, Robert, Daniel Dombey, Stephen Fidler, Isabel Gorst, and Maija Palmer. 2007. "US warns cyber-attacks will increase." *Financial Times*, May 18.

Anderson, Robert H., and Anthony C. Hearn. 1996. *An Exploration of Cyberspace Security R&D Investment Strategies for DARPA: "The Day After … in Cyberspace II"*. Santa Monica: RAND.

Aradau, Claudia, and Rens van Munster. 2007. "Governing Terrorism Through Risk: Takng Precautions, (un)Knowing the Future." *European Journal of International Relations* 13 (1): 89-115.

Arquilla, John, and David Ronfeldt. 1993. "Cyberwar is Coming!" *Comparative Strategy* 12 (2): 141-65. Reprinted in *In Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds., Santa Monica: RAND, 23-60.

Arquilla, John, and David Ronfeldt. 1996. *The Advent of Netwar*. Santa Monica: RAND.

Arquilla, John, and David Ronfeldt. eds. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND.

Baldwin, David A. 1997. "The concept of security." *Review of International Studies* 23 (1): 5-26.

Balzacq, Thierry. 2005. "The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations* 11 (2): 171-201.

Bendrath, Ralph. 2003. "The American Cyber-Angst and the Real World – Any Link?" In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 49-73.

Bigo, Didier. 2002 "Security and Immigration: Toward a Critique of the Governmentality of Unease." *Alternatives* 27 (supplement): 63-92.

Blomfield, Adrian. 2007. "Estonia calls for a NATO strategy on 'cyber-terrorists' after coming under attack." *The Daily Telegraph*, May 18.

Bubandt, Niels. 2005. "Vernacular Security." *Security Dialogue* 36 (3): 275-96.

Buzan, Barry 2004. *The United States and the Great Powers: World Politics in the Twenty-First Century*. Cambridge: Polity.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework For Analysis*. Boulder: Lynne Rienner.

Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US efforts to secure the information age*. London: Routledge.

Collins, Alan, ed. 2007. *Contemporary Security Studies*. Oxford: Oxford University Press.

Computer Science and Telecommunications Board. 1991. *Computers at Risk: Safe Computing in the Information Age*. Washington, D.C.: National Academy Press.

Computer Science and Telecommunications Board. 2002. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*. Washington, D.C.: National Academy Press.

Daily Mail. 2007. "Attack of the Cyber Terrorists." May 28.

Deibert, Ronald J. 2002. "Circuits of Power: Security in the Internet Environment." In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. James N. Rosenau and J. P. Singh. Albany: State University of New York, 115-142.

Deibert, Ronald J. 2003. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium* 32 (3): 501-30.

Deibert, Ronald J., and Janice Gross Stein. 2002. "Hacking Networks of Terror." *Dialog-IO* 1 (1): 1-14.

Denning, Dorothy E. 1999. *Information Warfare and Security*. Reading, Massachusetts: Addison-Wesley.

Denning, Dorothy E. 2001. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, eds. John Arquilla and David Ronfeldt. Santa Monica: RAND, 239-288.

Der Derian, James. 1992. *Antidiplomacy: Spies, Terror, Speed, and War*. Oxford: Basil Blackwell.

Der Derian, James. 2003. "The Question of Information Technology in International Relations." *Millennium* 32 (3): 441-56.

Deudney, Daniel. 1990. "The Case Against Linking Environmental Degradation and National Security." *Millennium* 19 (3): 461-476.

Edwards, Paul N. 1996. *The Closed World: Computers and the Politics of Discourse in Cold War America*. Cambridge, Massachusetts: MIT Press.

Elbe, Stefan. 2006. "Should HIV/AIDS Be Securitized? The Ethical Dilemmas of Linking HIV/AIDS and Security." *International Studies Quarterly* 50 (1): 119-144.

Erikson, Johan. 1999. "Observers or Advocates?: On the Political Role of Security Analysts." *Cooperation and Conflict* 34 (3): 311-333.

Finn, Peter. 2007. "Cyber Assaults on Estonia Typify a New Battle Tactic." *The Washington Post*, May 19.

Gray, Chris Hables. 1997. *Postmodern War: The New Politics of Conflict*. London: Routledge.

Hansen, Lene. 2000. "The Little Mermaid's Silent Security Dilemma and the Absence of Gender in the Copenhagen School." *Millennium* 29 (2): 285-306.

Hansen, Lene. 2008. "Visual Securitization: Taking Discourse Analysis from the Word to the Image." Paper presented at the 49th International Studies Convention, San Francisco, March 26-29.

Hundley, Richard O., and Robert H. Anderson. 1995/96. "Emerging Challenge: Security and Safety in Cyberspace." *IEEE Technology and Society*, 19-28. Reprinted in *In Athena's Camp: Preparing for Conflict in the Information Age*, eds. John Arquilla and David Ronfeldt. Santa Monica: RAND, 231-251.

Huysmans, Jef. 1998. "Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe." *European Journal of International Relations* 4 (4): 479-505.

Huysmans, Jef. 2006. *The Politics of Insecurity: Fear, migration and asylum in the EU*. London: Routledge.

IISS. 2007. "NATO – Cyber-Crime and Cyber-Security." Invitation to panel discussion on July 19.

Jackson, Nicole J. 2006. "International Organizations, Security Dichotomies and the Trafficking of Persons and Narcotics in Post-Soviet Central Asia: A Critique of the Securitization Framework." *Security Dialogue* 37 (3): 299-317.

Kent, Alexandra. 2006. "Reconfiguring Security: Buddhism and Moral Legitimacy in Cambodia." *Security Dialogue* 37 (3): 343-361.

Kinniburgh, James B., and Dorothy E. Denning. 2006. "Blogs and Military Information Strategy." *IO Sphere*, Summer: 5-13.

Landler, Mark, and John Markoff. 2007. "Data assault hits Estonia were it hurts." *International Herald Tribune*, May 30.

Latham, Robert. 2003. "Introduction." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 1-21.

Laustsen, Carsten Bagge and Ole Wæver. 2000. "In Defence of Religion: Sacred Referent Objects for Securitization." *Millennium* 29 (3): 705-739.

McSweeney, Bill. 1996. "Identity and security: Buzan and the Copenhagen school." *Review of International Studies* 22 (1): 81-93.

Michaels, Jim. 2007. "NATO to study defense against cyberattacks; Computer assault staggered Estonia." *USA Today*, June 15.

NATO. 2008. "Defending against cyber attacks." http://www.nato.int/issues/cyber_defence/practice.html. Accessed July 3, 2008.

Neocleous, Mark. 2006. "From Social to National Security." *Security Dialogue* 37 (3): 363-384.

Neumann, Iver B. 2002. "Returning Practice to the Linguistic Turn: The Case of Diplomacy." *Millennium* 31 (3): 627-651.

Nissenbaum, Helen. 2004. "Hackers and the contested ontology of cyberspace." *New Media & Society* 6 (2): 195-217.

Nissenbaum, Helen. 2005. "Where computer security meets national security." *Ethics and Information Technology* 7 (2): 61-73.

North Atlantic Council. 2007. "Final Communique: Meeting of the North Atlantic Council in Defence Ministers Session." Press Release (2007)067, 14 June.

OnGuard. 2008. "P2P Security." Posted at http://www.onguardonline.gov/topics/p2p-security.aspx, accessed on October 31, 2008.

Roe, Paul. 2005. *Ethnic Violence and the Societal Security Dilemma*. London: Routledge.

Ronfeldt, David, John Arquilla, Graham Fuller, and Melissa Fuller. 1998. *The Zapatista "Social Netwar" in Mexico*. Santa Monica: Rand Corporation.

Rothschild, Emma. 1995. "What is Security?" *Dædalus* 124 (3): 53-98.

Saco, Diana. 1999. "Colonizing Cyberspace: "National Security" and the Internet." In *Cultures of Insecurity: States, Communities, and the Production of Danger*, eds. Jutta Weldes, Mark Laffey, Hugh Gusterson and Raymond Duvall. Minneapolis: University of Minnesota Press, 261-291.

Schwartz, John. 2007. "When Computers Attack." *The New York Times*, June 24.

Thomas, Timothy L. 2006. "Cyber Mobilization: A Growing Counterinsurgency Campaign." *IO Sphere*, Summer: 23-28.

The Economist. 2007a. "A good bot roast; Cyber-crime." June 23.

The Economist. 2007b. "Cybersecurity: Beware of the Trojan panda." September 8.

The National Strategy to Secure Cyberspace. 2003. Washington, D.C.: The White House.

The New York Times. 2007. "A Cyberblockade in Estonia." June 2.

The Washington Times. 2007. "Cyberwarfare worries." June 2.

Traynor, Ian. 2007. "Russia accused of unleashing cyberwar to disable Estonia." *The Guardian*, May 17.

Wæver, Ole. 1995. "Securitization and Desecuritization." In *On Security*, ed. Ronnie Lipschutz. New York: Columbia University Press, 46-86.

Wæver, Ole, Barry Buzan, Morten Kelstrup, and Pierre Lemaitre. 1993. *Identity, Migration and the New Security Agenda in Europe*. London: Pinter.

Walker, R. B. J. 1990. "Security, Sovereignty, and the Challenge of World Politics." *Alternatives* 15 (1): 3-27.

Wilkinson, Claire. 2007. "The Copenhagen School on Tour in Kyrgyzstan: Is Securitization Theory Useable Outside Europe?" *Security Dialogue* 38 (1): 5-25.

Williams, Michael C. 1998. "Identity and the Politics of Security." *European Journal of International Relations* 4 (2): 204-225.

Williams, Michael C. 2003. "Words, Images, Enemies: Securitization and International Politics." *International Studies Quarterly* 47 (4): 511-529.

Williams, Michael C. 2007. *Culture and Security: Symbolic power and the politics of international security*. London: Routledge.

Yould, Rachel E. 2003. "Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 74-97.