Political Geography 46 (2015) 11–20

Contents lists available at ScienceDirect

Political Geography

journal homepage: www.elsevier.com/locate/polgeo

The birth of cyberwar

Robert Kaiser[*]

Department of Geography, University of Wisconsin-Madison, 430 Science Hall, 550 N Park St, Madison, WI 53706, USA

ARTICLE INFO

Article history:
Available online 11 December 2014

Keywords:
Anticipation
Aporia
Cyberwar
Cybersecurity
Apparatuses of security
Performativity
Premeditation
Preparedness
Resilience
Imagination
Transactors
Resonance

ABSTRACT

Within western security discourse, the threat posed by cyberwar has risen from a barely acknowledged concern to one of the greatest challenges confronting the West and the world in only a few short years. How did this happen so quickly, and what are the consequences for how security is performatively enacted? We argue that an event that occurred in 2007 catalyzed cyberwar's actualization as a new policy object, and has continued to affect the discursive practices materializing cyberwar since 2007. After a brief genealogy of cyberwar imaginings prior to 2007, the article interrogates how the 2007 events catalyzed cyberwar's materialization, and the discursive practices that have worked performatively to stabilize and institutionalize a knowledge-power assemblage named cyberwar as a new policy object. In particular, it traces the ways in which the site and situation of cyberwar's birth have affected the emerging apparatuses of cybersecurity, how the event enabled Estonian cybersecurity specialists and political and military elites as "catalyzing agents and shimmering points" in the emerging cyberwar resonance machine, while Tallinn became elevated as a cybersecurity center of calculation, and finally how the events of 2007 have served as a precautionary baseline for the anticipatory actions through which future cyberwars are made present.

> *We should pay attention to the way cyber security is understood as a problem of government, the particular vocabularies and discourses that construct this problem, and the solutions those problematizations privilege* (Bernard-Wills and Ashenden 2012, 115).

Introduction

"Hong Kong must take threat of cyberwarfare seriously" (*South China Morning Post* 2 July 2014). "Obama finally wakes up to China's cyberwar" (*USA Today* 21 May 2014). "Europe begins its largest-ever cyberwar stress test" (*Wall Street Journal* 28 April 2014). "Russia–Ukraine conflict could trigger cyberwar" (*VOA News* 20 April 2014). Hardly a week goes by when cyberwar is not a featured news story. Yet only a few years ago it was barely acknowledged as a realistic security threat, and its imaginative production was limited largely to sci-fi novels and films. What happened to bring about such a fundamental change in western security discourse?

On 26 April 2007, a monument was removed from a park in Tallinn, Estonia, sparking a riot in an event named the Bronze Night. A series of cyberattacks accompanied this event, continuing through mid-May. These cyberattacks, beginning as limited denial of service (DoS) attacks but growing to include larger and more coordinated distributed denial of service (DDoS) assaults involving botnets of computers from scores of countries, were launched against governmental, banking, media and political party websites in Estonia, and succeeded in forcing the government and the largest banks offline for brief periods. Even while these cyberattacks were underway, a cyberwar "resonance machine" (Connolly 2005) quickly emerged, and by the end of May 2007 the attacks were widely being hailed as the world's first case of cyberwar.

Almost overnight, western security assemblages seemed to wake up to the threat of cyberwar. In just a few short years cyberwarfare has been elevated from a barely mentioned security concern to one of the greatest military dangers confronting the West, and the world, rivaling terrorism itself (e.g., Clarke & Knake, 2010; Gjetlen 2010; European Commission, 2009; McAfee 2009; NATO, 2010a). The threat of cyberwar is now imagined as even more serious than the risk of more conventional or nuclear military assaults (NATO, 2010a). The perceived change in the nature of warfare is so great that some have compared it to the advent of air power, and have called for the establishment of a new branch in the US military to deal with cybersecurity threats (Conti & Surdu,

[*] Tel.: +1 608 262 2138; fax: +1 608 265 3991.
E-mail address: rjkaise1@wisc.edu.

http://dx.doi.org/10.1016/j.polgeo.2014.10.001
0962-6298/© 2014 Elsevier Ltd. All rights reserved.

2009). In October 2009, US Cyber Command was created to bring all the US military cyber units together.

While the security literature written since 9/11 has taken Foucault's work on governmentality and biopolitics in exciting new directions, providing sophisticated critical analyses of preemption and premediation, anticipation, and the calculation of risk and risk management under conditions of radical uncertainty, with rare exceptions (e.g., Barnard-Wills and Ashenden 2012) it has not explicitly addressed cyberwar's emergence and the apparatuses of cybersecurity that have proliferated since 2007 in response. This is surprising, especially given how rapidly cyberwar has risen as an imagined security threat, as well as how dramatically cybersecurity has come to dominate western security discourse.

This article cannot hope to address questions surrounding cyberwar's emergence in their entirety; its more modest objective is to flag the need to more fully interrogate risk and cyberwar by exploring both the triggering event that materialized cyberwar as a new policy object, and the consequences of this event for how cyberwar and cybersecurity are discursively practiced. To do this, we explore three elements of cyberwar's emergence. First, what was it about the cyberattacks that happened during this particular event that provided the conditions for cyberwar's birth? The cyberattacks in Estonia were certainly not the first of their kind, and by all accounts their effects on Estonia's critical information infrastructure (CII) were neither serious nor long lasting. Yet the 2007 events in Tallinn "fired the imagination" (Salter, 2008) of policymakers, cybersecurity experts and news analysts of western security, resonating powerfully enough to give birth to cyberwar and transforming the emerging field of cybersecurity in the process.

Second, the cyberattacks and their successful imagineering as the world's first cyberwar catapulted Estonia and Estonians from a position on the margins to the very center of western security discourse. The birth of cyberwar is also a story about how Estonian security concerns were able – for a time – to reshape those of NATO, the EU, and the West in cyberspace. And, just as Estonian IT experts, military and political elites became "transactors," "catalyzing agents and shimmering points" in the emerging cyberwar resonance machine (Connolly 2005; Latour 1987, 108–121, 2005, 108; Kuus, 2004), Tallinn, and more specifically sites such as the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) emerged as the new cyberwar "centers of calculation" (Barnes, 2006; Latour 1987, 232–47) within western apparatuses of security. How has this geopolitical realignment affected the way in which threats and security in cyberspace are imagined and performatively enacted?

Finally, the 2007 cyberattacks have affected the ways in which the threat of future cyberwars is made present and managed. They have been used in a series of "anticipatory actions" (Adey and Anderson 2011; Anderson, 2010a; 2010b) such as scenario planning and cyberwar exercises, and are also embedded in initial efforts to formulate international law governing the conduct of future cyberwars, in a publication tellingly named *The Tallinn Manual* (Schmitt 2013). As the event that gave birth to cyberwar, the cyberattacks against Estonia provide a precautionary baseline from which to imagine, narrate, and then stage how much worse cyberwar could have been – and will be. It established the trajectory from which worst-case cyberwar scenarios have proliferated, and this has been as constraining as it has been enabling, since even in an era of 'unknown unknowns' where imagining the unimaginable and thinking the unthinkable are the geopolitical order of the day, events make the presencing of certain futures more imaginable, more thinkable and more actionable than others.

This article adopts a performative approach to explore how cyberwar and the securitization of cyberspace are discursively practiced (Aradau, 2010; Barad 2003; Bialasiewicz et al. 2007; Butler, 1993, 2010; Kaiser 2014; Kaiser & Nikiforova, 2008; Mountz, 2010), and uses "second-order observation" to interrogate the imaginings, calculations, words and deeds through which cyberwar and cybersecurity performatively materialize. It "draws attention to the contingent choices and distinctions made by first-order observers in forging an apparatus of … security … and offers a critical understanding of how such an apparatus works" (Collier et al. 2004, 7).

After providing a brief genealogy of the discursive practices associated with cyberwar before 2007, the article focuses on how the cyberattacks associated with the Bronze Night were imagineered into the world's first cyberwar, how the site and situation of cyberwar's birth have affected the emerging apparatuses of cybersecurity, and the ways that the events of 2007 have affected the anticipatory actions associated with presencing a multiplicity of future cyberwars.

Imagining cyberwar: a brief genealogy of futures past

Industrialization led to attritional warfare by massive armies. Mechanization led to maneuver predominated by tanks. The information revolution implies the rise of cyberwar, in which neither mass nor mobility will decide outcomes; instead, the side that knows more … will enjoy decisive advantages … Cyberwar may be to the twenty first century what blitzkrieg was to the twentieth. (Arquilla & Ronfeldt, 1993, 141).

It is not as if cyberwar had not been conceived of prior to 2007. It was imaginatively produced in science fiction novels and films, from *Shockwave Rider* in 1975 (Lesk 2007: 77), to *War Games* (1983) and *Terminator* (1984), capping the period off with the 2007 blockbuster *Live Free or Die Hard*, which was playing in theaters in Tallinn during the summer of the cyberattacks. The 2007 film is particularly important here, since it featured a disgruntled former cybersecurity military analyst who used a broad-based cyberassault to take down the critical infrastructure (CI) of the United States. In Tallinn, the movie fed into the affective intensity surrounding the riots and cyberattacks, firing the imagination of policymakers and publics alike.

Cyberwar was also being discursively produced in political and military think tanks beginning in the early 1990s. One of the first examples of this is the 1993 publication "Cyberwar is coming!" which recently celebrated its 20th anniversary (Arquilla 2013; Arquilla & Ronfeldt, 1993). This work too sought to fire the imagination of its readers, spinning out anticipatory cyberwar scenarios and advocating a cyberwar doctrine to military and political analysts and other cyberwar "managers of unease" (Bigo 2002). Published at about the same time, and foreshadowing the proliferation of drone strikes in what Gregory (2011; 2014) has called "the everywhere war," "Welcome to hyperwar" painted a more dystopian vision of smart weaponry and war machinery taking over the battlespaces of the future (Arnett 1992).

Later in the 1990s, due in part to concerns surrounding Y2K and also to the rising number of denial of service (DoS) cyberattacks, increasing US governmental attention was devoted to computer security and the threat posed by cyberwarfare. In 1998, the Clinton White House issued Presidential Decision Directive 63 to assess the vulnerabilities of CI to cyberattack, and followed this up with the *National Plan for Information Systems Protection* in 2000. Titled *Defending America's Cyberspace*, this document presented cyberspace as a vulnerable dimension of the sovereign territory needing protection, largely due to the failure to build in adequate defenses when cyberspace first emerged. The authors of this document – including President Clinton and Richard Clarke, then National Coordinator for Security, Infrastructure Protection and Counter-Terrorism – billed it as "the first attempt by any national government to design a way to protect its cyberspace" (White House, 2000, iv), and also sought to fire the imaginations of their readership, conjuring up a whole host of cyber-villains meaning to do America harm.

> We are at risk. The United States depends more on computers today then ever before … We have created a gaping vulnerability in our national security and economic stability … We are vulnerable to mischief-making hackers, hardware and software failures, cyber criminals and, most alarmingly, to deliberate attack from nation states and terrorists (White House, 2000, 1).

These efforts were paralleled by Congressional hearings on the threat of cyberwar and America's preparedness – or lack thereof – to counter it (e.g., US House of Representatives, 2000).

The increasing academic, political and popular attention paid to cyberwar was matched by a growing number of high profile cyberattacks. In 1998, Tamil 'hacktivists' organized an email inundation campaign of Sri Lankan embassies. In 1999, Chinese hackers responded to the US bombardment of China's Embassy in Belgrade by attacking the American Embassy's webpage in Beijing. In 2000, Israeli and Palestinian hackers attacked the websites of Hezbollah and Israel's Foreign Ministry respectively, and American and Chinese hackers exchanged broad-based attacks against Chinese and US websites following the downing of an American spy plane over Chinese territorial waters in 2001 (Denning 2001; Lesk 2007). On the cusp of the new millennium, a rapid escalation and intensification of discursive practices were working to materialize cyberwar as a new policy object.

The events of September 11, 2001 changed all that, as the "global war on terror" (GWOT) remade the security landscape. Initiatives begun to prepare for cyberwarfare were shelved, meetings were canceled, and "critical infrastructure protection" shifted from cyberspace to more conventional spaces of security. Although some policy documents and studies continued to be produced (e.g., Billo and Chang 2004; Clarke & Knake, 2010, 120), cyberspace and cybersecurity themselves were re-imagined and re-purposed to combat global terrorist networks, and were folded into and made an integral part of the Patriot Act of 2001 and the Department of Homeland Security in 2002.

If cyberwar's performative materialization had been preempted by the GWOT in the United States, in Europe it had not yet been taken up. Although the Council of Europe had passed a Convention on Cybercrime in 2001, cyberwar itself was not considered. And at NATO's 2002 Prague Summit, which went to great lengths in discussing the ways NATO needed to transform and adapt in the wake of 9/11, cybersecurity was barely mentioned (NATO, 2002). The birth of cyberwar would have to await both the declining importance of terror as a policy object and a catalyzing event.

The birth of cyberwar

On 26 April 2007, workers under orders from the Estonian government began the process of removing a bronze soldier statue and the bodies of Red Army soldiers from a public park in Tallinn. The monument, built to commemorate the Red Army's liberation of Tallinn during WWII, had become the site of intensifying contestation between self-identifying Russians and others who felt disenfranchised in independent Estonia, and Estonian nationalists who viewed the USSR, Russia, and Russians as unwanted occupiers of their national homeland (Bruggemann and Kasekamp 2008; Kaiser 2012; Lehti, Jutila, & Jokisipila, 2008; LICHR., 2007; Paabo, 2008). Throughout April 26th, a crowd of protesters gathered, growing larger and angrier by nightfall. Rioting erupted at the site and spread to Old Town, continuing off and on for two days, in an event named the Bronze Night.

Beginning on April 27 and lasting until mid-May, a series of cyberattacks were launched against governmental, media, banking and political party websites, in a politically motivated effort to participate in the Bronze Night and extend it into cyberspace. Estonia's political and military elite, as well as news media, blamed Russia and a disloyal fifth column of Russians living in Estonia for both the riots and the cyberattacks, "remediating" (Grusin 2004) the latter as a cyberwar launched by Russia against Estonia. A cyberwar resonance machine quickly developed throughout western security assemblages, and by the end of May 2007 the cyberattacks were being widely hailed as the world's first cyberwar (BBC., 2007; Kirk, 2007; Landler and Markoff 2007; Mite, 2007; Tanner, 2007; Traynor, 2007).

First, it is important to acknowledge that if this event had happened immediately after 9/11, its affective capacity would almost certainly not have been sufficient to actualize cyberwar. Coming at a time when public and political support for the GWOT had significantly waned provided the event with the temporal distance needed for cyberwar managers of unease to capture the imagination of western policymakers and publics.

However, not just any cyberattack would do. Both the sociospatial context of the event, and also how it was managed, were critical for the production of resonance. The success of Estonia's cyberwarriors "in providing a compelling narrative for their analysis" (Salter, 2008, 237) may be attributed to their performative enactment of a familiar and believable set of Cold War place-identities featuring Russia and Russian-ness as enemy Other of Estonia, Europe and the US, and Estonia and Estonian-ness as small, vulnerable victim. Western imaginations, primed for such a threat scenario, were easily captured (Blank 2008; Davis, 2007; Robert 2012; Ruus, 2008; Weiss, 2007).

Waking the World Up to Cyberwar

World governments are trying to figure out how to defend themselves against cyber-warfare, and Estonia leads the way (Public Radio International, 2010).

That cyberspace "makes us vulnerable" is a central characteristic of cybersecurity discourse, and the more technologically advanced, the more vulnerable one is imagined to be (Bernard-Wills and Ashenden 2012, 118). Since independence Estonia had become one of the most wired countries in the world, and in this regard at least is imagined to occupy a future timespace toward which the rest of the world is headed. This, coupled with Estonia's small size and location on the border of Europe's 'Other', was prominently featured in explanations of why the cyberattacks had occurred. This "architecture of enmity" (Amoore, 2009) displaced the internal place-identity conflicts between Russian-ness and Estonian-ness that produced the Bronze Night, even as it remediated the cyberattacks into the world's first cyberwar.

> Estonia as a small, modern, technology-savvy country was an ideal test-ground for cyberattackers with political motivations … Estonia happened to experience the first large-scale attacks, but … vulnerabilities are growing in both the developed and developing world (Tiirmaa-Klaar, 2011a, 1–2).

The 2007 cyberattacks were universally described in media, in official documents and by cybersecurity specialists as a "wakeup call." The first question confronting policymakers charged with defending against the cyberattacks was whether or not to issue the call, to go public. Given the widespread use of the sites that were targeted, the cyberattacks would have been difficult to deny. A debate within government circles occurred, and the decision to go public owed as much to international as to domestic considerations. This event seemed to be just what western cyberwar managers of unease were waiting for:

> Here we had this example of cyberattacks actually being part of a political campaign, affecting the whole of society … In the United States lots of agencies and lots of people recognized the problem (of cyberwar) but were not successful in communicating it. Or were unable because of classification reasons to communicate it. And now we have Estonia who is willing to communicate it and to use their country as an example of what may happen. And I think Estonia and the United States together sort of … I mean, the level of conferences I participated in after 2007 was just insane. We were in the Air Force national conference with thousands of very high-ranking officers, we were briefing Congress, we were briefing the White House, at the very highest level (Interview, former Estonian Defense Ministry official, Tallinn, October 2012).

President Ilves took the lead in issuing the wakeup call, and in remediating the cyberattacks as a cyberwar launched by Russia – imagined as the constitutive outside of the civilized spaces of Estonia and Europe: “Finally, I turn to Russia, Estonia's neighbour, with a clear message – try to remain civilized! It is not customary in Europe to use computers belonging to public institutions for cyber-attacks against another country's public institutions” (Ilves, 2007a). Describing the Bronze Night as “the greatest challenge to the security” of Estonia since independence and the cyberattacks as “cyber-war” (Ilves, 2007b), Ilves proclaimed that “Estonia was attacked with a weapon and in a manner whose full significance is just beginning to dawn on the whole world in the 21st century” (Ilves, 2007c).

Former Defense Minister Aaviksoo raised the issue of invoking Article 5 (common defense) with NATO while the event was still underway (Traynor, 2007), and asserted that “what took place was according to our interpretation cyber warfare and cyber terrorism. In essence, cyberattacks against Estonia demonstrated that the Internet already is a perfect battlefield of the 21st century” (Aaviksoo 2007a). Although “NATO's political leaders judged that the cyberattacks were not an act of war, NATO's Department of Public Diplomacy later created a short film about the episode entitled *War in Cyberspace*” (Singer and Friedman 2014, 122), allowing Estonia's cyberwarriors a NATO-sanctioned platform from which to present their ‘compelling narrative’.

Aporias of cybersecurity

Following Derrida, Burke (2002, 4–5) defines an aporia as “an untotalizable problem at the heart of the concept, disrupting its trajectory, emptying out its fullness, opening out its closure.” He identifies two interlocking aporias of security: first, that claims to universal security for all humans are challenged by a foundational “aporetic distance between our ‘humanity’ and a secure identity bounded and defined by the state;” and second, that securing oneself “must be purchased at the expense of another” (Burke, 2002, 6). These aporias are central to the performative enactment of our sociospatial selves, which are bordered against a constitutive outside that is both totally excluded and at the same time occupies the very center of our place-identities (Butler, 1993; Kaiser 2014; Kaiser & Nikiforova, 2008).

The 2007 events that materialized cyberwar as a new policy object were created by these aporias of security, and at the same time embedded them at the very heart of cybersecurity. The Bronze Night and the accompanying cyberattacks were a ‘war event’ that ruptured the surface calm in Estonian society, exposing the ways in which Russia and Russian-ness performatively materialize as the constitutive outside of Estonia and Estonian-ness through a wide range of everyday discursive practices, and without which Estonia and Estonian-ness could not exist in their present form (Feldman, 2001; Kaiser 2014; Kaiser & Nikiforova, 2008). Through these performative enactments, Estonia's and Estonians' security are purchased at the expense of Russia and Russians (Feldman, 2001; Kuus, 2004).

Both the Bronze Night and the cyberattacks were remediated as acts of war, attacks on Estonia's sovereignty by Russia and a disloyal fifth column of Russian enemy Others within (Kaiser 2012). Cyberwar's materialization through this event carried this aporia of security into cyberspace, and helped to reconstitute a familiar geopolitical imaginary from the Cold War in cyberspace, now conceived as a battlespace where states – aligned into camps of western defenders and eastern attackers – wage cyberwar.

> Of course, you know, when you look on the map, then it's very clear. Estonia's a small nation but we have to be concerned about our neighbors. Thank God we are now members of NATO and the EU, and we are not alone anymore. And in cyberwar we are not alone too (Interview, Cyber Defense League, Tallinn, May 2011).

Within this battlespace, Estonia is imagined as occupying a vulnerable border between East and West, where cyberwar is an ever-present threat. This danger is also seen as an opportunity:

> We are still living between the East and the West – we are a playground for bad guys … We are looking to increase cooperation with the US. Why should the US cooperate with us? Because we are on the border. If something happens, we can give you a warning that something is coming (Interview, Cyber Defense League, Tallinn, September 2012).

Bigo argues that those acknowledged as security experts “transfer the legitimacy they gain from struggles against terrorists, criminals, spies, and counterfeiters toward other targets, most notably transnational political activists, people crossing borders, or people born in the country but with foreign parents” (Bigo 2002, 63). However, given the aporias of security, and the reiterative citationality of security practices, it seems more accurate to assert that the managers of unease derive their status *as* security experts from the boundary effects that performatively materialize such threatening Others, who in turn become embedded at the very core of the security discourse that such specialists claim expertise over. Securitization is thus a border performative, continually producing insecurity within the population and territory that must then be secured. Insecurity can never be banished and security finally procured, since insecurity occupies the very heart of securitization practices, with security itself always occupying the promised timespace of the future (Anderson, 2010a).

The cyberattacks, re-imagined as a cyberwar launched against a small, technologically advanced state by a large and aggressive neighbor, displaced the problematic relationship between Estonian nationalists in power and self-identifying Russians who felt victimized in independent Estonia that produced the Bronze Night's actualization and the cyberattacks themselves. The remediation of the cyberattacks as Russia engaging in cyberwar against Estonia and the West also transposed a familiar geopolitical b/ordering onto cyberspace: Estonia/Estonian-ness – good guys, small but capable cyberdefenders of ‘the West’ vs. Russia/Russianness – bad guys, perpetrators of cyberwar, ‘the East’. At the same time, the event provided Estonian security professionals an important opportunity to reiterate to European and American audiences that Russia remains an ever-present threat, securing for themselves the role of “transactors” (Kuus, 2004) of cybersecurity.

Estonian expertise and the performative enactment of cybersecurity

With an event that fired the imagination of policymakers throughout apparatuses of western security, Estonian managers of unease became “transactors,” “translators,” “catalyzing agents and shimmering points” in the emerging cyberwar resonance machine (Connolly 2005; Latour 1987, 108–121; 2005, 108; Kuus, 2004), while Tallinn, and more specifically the NATO CCDCOE emerged as the new cyberwar “centers of calculation” (Barnes, 2006; Latour 1987, 232–47). This section explores the discursive practices that elevated the events, as well as Estonian experts and Estonia, to the forefront of an emerging ‘western consensus’ on cyberwar.

Immediately following the 2007 events, Estonia and Estonians began to be performatively enacted as the place and people with the most experience and expertise in the realm of cyberwar and cybersecurity. This was treated in self-entrepreneurial fashion as a critical resource to be tapped in neo-liberal Estonia. The success in turning the tragedy of the Bronze Night and the cyberattacks to Estonia's advantage was the subject of numerous comments. An interviewee at Estonia's Ministry of Defence in May 2011 expressed this sentiment most clearly: “It was quite an unfortunate event for us, but it has pushed us to the forefront” of cybersecurity. Former Defense Minister Aaviksoo (2007b) went further as he joked: “We are extremely thankful for the publicity we had due … to the cyber attacks early April this year … We have modest resources; we could have never managed that publicity of our cyber activities in Estonia.” And, as is clear in President Ilves' comments on June 23, 2007 (2007c), the event provided Estonians with the opportunity to make their mark and establish a niche for themselves as cybersecurity “norm entrepreneurs” in the West.

> The European Union legislation on cyber security … is dangerously and unaccountably deficient. Estonia could and should assume the role of initiator to improve the situation both in the … EU and NATO. If we have, for many years, been racking our brains to find areas where we could be forerunners and contributors, recent events have certainly revealed one such goal to us.

As Kuus (2004; see also 2014) points out in her analysis of the two-way construction of western security discourse, the role of transactor accorded to trusted local interpreters of East European realities affords some “intellectuals of statecraft” a privileged position in determining how security is enacted.

> The question is not who causes certain constructions of security but who participates in the creation of the conditions that make certain accounts possible and others impossible. Although East European intellectuals of statecraft do not cause Western security discourses, their formal analyses as well as their informal interactions with their Western counterparts are essential for making possible particular Western representations of Eastern Europe (Kuus, 2004, 194).

The events of 2007 afforded Estonian managers of unease the opportunity to serve as transactors in the discursive practices through which cyberwar materialized as a new policy object.

Within Estonia, a *Cyber Security Strategy* was quickly drafted (Cyber Security Strategy Committee, 2008). A highly unusual document, it lays out not a military or even a political strategy for combating cyberwar, so much as a plan for affecting how cybersecurity should be practiced in the West.

> Owing to Estonia's unique experience in dealing with cyber attacks in the spring of 2007 and subsequent policy initiatives, the international community expects a major contribution from us … Estonia has assumed a leading role in introducing cyber security-related initiatives to international organisations and through bilateral co-operation … More extensive participation in international organisations is vital to ensuring recognition of the problems of cyber security generally and to drawing the attention specifically of policy-makers in other countries (Cyber Security Strategy Committee, 2008).

As the first such document in Europe, it – and the Estonian experts who crafted and implemented it – have affected the shaping cybersecurity policies and practices emerging in NATO and the EU since 2007.

NATO and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Unfortunately, NATO's *Cyber Defense Plan* (2008) remains classified, so the 2007 events' affect cannot be directly assessed. However, according to NATO's own documents, “Estonia was … a founding player in the development of NATO's cyber defence policy, adopted in 2008, raising the question of whether cyber attacks should be considered a military aggression against the Alliance” (NATO, 2009). The events of 2007 also shifted NATO's focus from “protecting the communication systems owned and operated by the Alliance” to a broader mission, “assisting those Allies who seek NATO support for the protection of their communication systems, including through the dispatch of Rapid Reaction Teams” (NATO 2012). The 2007 cyberattacks, and Estonian demands that NATO clarify its position on cyberwar and its role in assisting member states with cyberdefense – including questions of the cyberattack conditions under which articles 4 (mutual consultation) and 5 (collective defense) are invoked – provided the impetus for elevating the perceived threat level associated with cyberwar to a position comparable with terrorism (NATO, 2010a; 2010b). 2007 remains embedded within NATO's latest Policy on Cyber Defence, which uses the Estonian case to argue for the development of “a cyber dimension” across its core missions of “collective defence, crisis management, and co-operative security” (NATO 2011).

The NATO CCDCOE opened in Tallinn on 14 May 2008. While several interviewees stressed that the plans to create the center had been proposed and approved prior to 2007, it is also the case that the CCDCOE needed the birth of cyberwar to be brought to life itself. According to Peeter Lorents, the person tasked with putting together the proposal and making several of the original staffing decisions for the Center, there was a great deal of resistance from policymakers and in the media prior to 2007. The CCDCOE represented a significant investment on the part of the state, and cyberwar was not taken as a serious threat, so it was very difficult to get resources in 2006. 2007 was described by Lorents as “a gift from Putin, a good example of what might happen” (Lorents interview 6 May 2013). Lorents, who was on his way to a conference in Seattle with Bill Gates when the events happened, noted that this provided a great opportunity to demonstrate the dangers of cyberwar, to showcase Estonians' ability to handle it, and to affirm that the NATO CCDCOE was located in the right place.

Prior to the events of 2007, the NATO CCDCOE had one member state: Estonia. Afterward, it has become one of the principal centers of calculation in the performative enactment of cyberwar and cybersecurity. It hosts workshops and annual conferences, and its analysts publish and deliver numerous papers and reports at a wide variety of international cybersecurity venues. As the event that gave birth not only to cyberwar but also to the Center, 2007 has served as a central theme in publications, workshops and exercises sponsored by the CCDCOE (e.g. Czosseck et al. 2011; Geers, 2010; Kaska, Talihärm, & Tikk, 2010; Ottis 2008; 2010; Tikk & Kaska, 2010). The specialists at the center also frequently serve as cybersecurity consultants participating in research and publications that go far beyond NATO. As just one example of this, in McAfee's Virtual Criminology Report 2009: *Virtually Here: The Age of Cyber Warfare* (McAfee 2009), two of the four contributors for Europe, the Middle East and Africa were Estonians. One of these was an Estonian defense ministry official, and the other was a NATO CCDCOE legal analyst. The European section of the report, not surprisingly, featured the cyberattacks of 2007.

As cyberwar has risen to a much higher threat level within western security discourse, the NATO CCDCOE's role in training, education, research and policy-related reports and presentations has also grown. Estonia not only serves as host, but provides both the commander of the CCDCOE and the vast majority of its expert staff. The Center not only establishes Tallinn as a central node in western cybersecurity networks; it works to validate Estonians' knowledge claims to expertise and to enhance their role as cybersecurity transactors. Estonian experts rotate out of the NATO CCDCOE to occupy elite cybersecurity positions in the Ministry of Defense and Estonia's State Information Agency, to teaching positions for the newly created MS and PhD programs in cybersecurity studies, and to postings in NATO, the EU and other transnational organizations to work on their cybersecurity policies and practices. The presence of the NATO CCDCOE was also influential in Tallinn's winning the competition for the new EU IT Agency (Kallas 2011).

International institutionalization

As with NATO, Estonia's cyberwar managers of unease have used the 2007 events to push cybersecurity – and Estonia/Estonians along with it – to the forefront of the security agendas of the UN, the OSCE, the OECD and the EU. Cybersecurity became a prominent policy question when Estonia assumed the chairmanship of the OSCE Forum for Security Cooperation in 2008 (Aaviksoo, 2008), though the organization remained deadlocked due to the serious disagreement between the US and Russia over how cybersecurity should be practiced (Klimberg & Tiirmaa-Klaar, 2011, 24–5). This rift has also resulted in limited progress toward the adoption of a cybersecurity plan at the UN – here competing norm entrepreneurs from Russia and China contest those from the US (Maurer, 2011) and Estonia. However, the UN's International Telecommunications Union (ITU) launched a Global Cybersecurity Agenda in May 2007, and Hamadoun Toure, the ITU's Secretary-General, used the events in Estonia as the reason behind his call for a global cyber peace treaty (Maurer, 2011; Meyer, 2010; Toure, 2011). Additionally, the Permanent Monitoring Panel on Information Security of the World Federation of Scientists was so alarmed by the events of 2007 and the cyberattacks that accompanied the 2008 Russian-Georgian conflict that it issued the Erice Declaration on Principles of Cyber Stability and Cyber Peace in 2009 (Toure, 2011). Among the western international organizations, the OECD appears to have been the least affected by 2007 events and Estonians' translation of them. A 2011 OECD/IFP report was relatively dismissive of the threat of cyberwar, and stated that "The main reason that the 2007 cyber-attacks on Estonia had a significant impact was that the country had become highly dependent upon information infrastructures without having made a concomitant investment in cybersecurity activities" (Sommers & Brown, 2011, 76).

Estonia and Estonian transactors have had greater influence in shaping cybersecurity discursive practices within the European Union. Following the 2007 events, cybersecurity in the EU was elevated as an area of concern. On 17 January 2008, the EU Commission organized a workshop in order to discuss large-scale cyberattacks, which focused on the 2007 events in Estonia and included several Estonian experts (EU European Commission, 2008). In 2009, the EU issued a report on protecting Europe from large-scale cyberattacks, in large part based on the lessons learned from Estonia, as well as the practices and policies that had already been implemented in Estonia and NATO.

Heli Tiirmaa-Klaar – who was charged with implementing Estonia's Cyber Security Strategy – is perhaps the most successful Estonian cybersecurity transactor. Since 2008, she has moved from her position in Estonia's Ministry of Defense to a role coordinating and integrating cybersecurity policy in Estonia with emerging plans in the EU, NATO and the OSCE. She was a key advisor to NATO during the writing of its 2010 cyberdefense plan, and has since helped craft the EU's cybersecurity policy (http://ccdcoe.org/cycon/475.html). In 2011, she co-authored the EU Parliament study *Cybersecurity and Cyberpower*, which provides a detailed account of cyberattacks and cybersecurity legislation and practices in the EU, US, China and Russia, and produces a three-tiered system for categorizing cyberattacks (Klimberg & Tiirmaa-Klaar, 2011).

Following the 2007 cyberattacks, Estonian cyberwar managers of unease became active participants in shaping western cybersecurity discourse, in determining what cyberwar looks like, who the threatening others in cyberspace are imagined to be, and how to defend against them. Estonian cybersecurity transactors and centers of calculation such as the NATO CCDCOE have succeeded in embedding their own understandings and mappings of cyberwar threats at the very heart of western cybersecurity discourse.

Anticipating cyberwar

Resilience is accepting that hey, bad things are going to happen; it's about how I power through those bad things. Because this is a problem that's going to be with us for as long as we're using the internet, and the only way you can continue to get the good is to understand that you have to manage the bad (Peter Singer, NPR Morning Edition, 20 December 2013).

Along with the rapid escalation of imagined danger associated with cyberwar, western security assemblages have dramatically increased the time, attention and resources devoted to anticipatory actions designed to prepare for future cyberwars. Although scenario planners have sought to imagine – and then plan for – worst case contingencies, 2007 remains foundational, as a precautionary baseline from which future cyberwars are made actionable in the present. As such, these events, the aporias of cybersecurity lying at their core, and the transactors and centers of calculation whose expert knowledge claims were established by them, continue to constrain even while they enable the anticipatory actions associated with cyberwar. In this final section, after briefly reviewing the literature on anticipatory actions under conditions of radical uncertainty, the article traces the ways in which the events of 2007 continue to affect how future cyberwars are imagined, planned for and performatively enacted in the present.

Anticipatory actions

"Anticipation (is) … a performative process of rendering the future actionable" in the present (Anderson, 2010a, 229). Unlike prevention, which “operates in an objectively knowable world in which uncertainty is a function of a lack of information, and … events run a predictable, linear course from cause to effect” (Massumi, 2007), preemption, preparedness and precaution operate under conditions of radical uncertainty, and work to generate a multiplicity of threats, since it is imagined that “the most effective way to fight an unspecified threat is to actively contribute to *producing* it” (Loc. cit., emphasis in original). And, because the threat is unkowable, the response to it must be prepared to intervene in the interval between the threat's materialization and its catastrophic effects, positioning life always on the brink of disaster. “The interval' is, then, a space-time of imminent danger in which action is demanded and normal priorities are reordered” (Anderson & Adey, 2011, 1099).

A shift toward “enactment-based” knowledge production and away from “archival-statistical” knowledge is especially prevalent under conditions when future threats are imagined as unknowable (Collier, 2008; Amoore and de Goede 2008). A decisive shift away from preventative strategies based on past analogs toward “preemption, precaution and preparedness” based on anticipatory actions has occurred since 9/11 (e.g., Anderson, 2010b; Anderson & Adey, 2012). At the same time, Grusin (2004; 2010) argues that “premediation” has come to dominate media coverage in the wake of 9/11:

> Premediation is not about getting the future right, but about proliferating multiple remediations of the future both to maintain a low level of fear in the present and to prevent a recurrence of the kind of tremendous media shock that the United States and much of the networked world experienced on 9/11 … Premediation imagines multiple futures which are alive in the present, which always exist as not quite fully formed potentialities (Grusin, 2010, 4, 8).

Indeed, “preemption as a security practice *requires* premediation, or a resonating fiction of a disastrous future about to unfold” (de Goede, 2008, 162, emphasis in original).

To make the future actionable in the present thus requires a threat with the resonant capacity to ‘fire the imagination’ of policymakers and publics alike (Salter, 2008). At minimum it must satisfy the “precautionary principle,” which “does not target all risk situations but only those marked by two principal features: a context of scientific uncertainty on the one hand and the possibility of serious and irreversible damage on the other” (Ewald, 2002, 282, quoted in Aradau & van Munster, 2008, 30). A past event or series of events that can be made to resonate in such a way establishes a precautionary baseline from which worst-case scenario planning can proceed. In the case of the Icelandic volcano eruption that grounded air traffic over northern Europe, for example, Adey and Anderson (2011, p. 13) note that “whilst uncertainty existed about the effects of the specific form of ash from the Eyjaf-jallajökull eruption, the possibility of damage was made present through the example of past ‘encounters with ash’.” The past event does not eliminate uncertainty associated with future threats, but rather provides a means of selecting among them, materializing some as policy objects to extrapolate from and act upon while excluding others from consideration. And, as de Goede (2008, 171) points out, because “premediation is performative … the imagination of some scenarios over others, the visualization of some futures and not others, entails profoundly political work that enables and constrains political decision-making in the present.”

Anticipating cyberwar

Since 2007, no ‘fiction of a disastrous future’ has resonated more powerfully than cyberwar. And, while grasping potential future cyberwars and making them governable in the present has focused on enactment-based knowledge/power assemblages (i.e., scenario planning, stress testing, the staging of exercises), naming the 2007 cyberattacks ‘the world's first cyberwar’ set the stage for imagining and enacting future cyberwars. This is so because “threats are contained and on the road to being controllable and manageable once housed within a name … a name depends for its power on chains of association that extend beyond it” (Anderson, 2010a, 231). Naming this case the world's first cyberwar called into service long, familiar and ominous chains of citational practices through which discourse could produce that which it named. In deploying a Cold War “architecture of enmity that (drew) stark lines between self/other; us/them; safe/risky; inside/outside” (Amoore, 2009, 51), cyberwar performatively materialized in a way that could quickly become naturalized and sedimented into the everyday discursive practices of those enacting western security. And although critics have been vocal in their skepticism of the seriousness with which cyberwar should be taken – primarily over the question of how catastrophic its effects can be (e.g. Lewis, 2011) – this has impeded neither the dramatic rise in the threat level afforded cyberwar nor the rapid proliferation of the apparatuses of cybersecurity to deal with it.

Cyberwar owes its rapid rise not only to the event that gave it birth, but also to the distinctive characteristics of the threat as it has been imagineered. First, cyberwar's indeterminacy is featured in most cybersecurity studies. Cyberwar could be initiated by state and non-state actors, from inside or outside networks, and both total systems as well as individual computers are susceptible to attack, infection, infiltration. Second, although cyberattacks to date – including those of 2007 – have not been particularly damaging, they have been treated as “near misses” (Bernard-Wills and Ashenden 2012), allowing worst-case scenario planners to imagine how much worse it might have been, and will be. As just one example of this hyping of the threat, Clarke and Knake (2010, 63–7) imagine critical infrastructure systems collapsing, resulting in Hollywood-style disaster scenes of car crashes, midair plane collisions, refinery fires, financial system meltdowns, telecommunication systems collapsing, and command-and-control centers cut off. They conclude “In all the wars America has fought, no nation has ever done this kind of damage … A sophisticated cyber war attack by one of several nation-states could do that today, in fifteen minutes, without a single terrorist or soldier ever appearing in this country.” Third, the timespace interval between cyberwar's onset and its catastrophic effects is imagined as infinitesimally short temporally and spatially global. This combination, as presented in threat scenarios, makes normal chains of command dysfunctional, providing policymakers no time to react before their CIs are overwhelmed.

Among cybersecurity practitioners, the central debate over how best to prepare for future cyberwars has focused on deterrence and resilience (European Commission, 2009; Singer and Friedman 2014; Clarke & Knake, 2010; Barnes and Gorman 2011; Elliott 2011; Libicki 2009; Klimberg & Tiirmaa-Klaar, 2011; Stevens 2012). It is perhaps not surprising that cyberdeterrence emerged first, given the importance of Cold War citational practices in cyberwar's materialization. However, although deterrence remains a prominent discourse featured in policy statements and military doctrine, most analysts have noted the difficulties with deterring cyberwar. The distinctive characteristics of deterrence help explain this: “deterrence makes use of the same epistemology prevention does, in that it assumes knowability and objective measurability. However, because it starts where prevention ends, it has no margin of error. It must know with *certainty* because the threat is fully formed and ready to detonate: the enemy has the bomb and the means to deliver it” (Massumi, 2007). Given the conditions of indeterminacy noted above, the problems with deterring cyberwar appear insurmountable.

Many cybersecurity practitioners advocate preparedness in the form of resilience (e.g., Singer and Friedman 2014, 170). Resilience is "central to achieving the ideal of continuous preparation for acting in and around emergencies" that are "both impossible and undesirable to eliminate … because risk (is) the source of profit as well as danger" (Anderson & Adey, 2012, 29). This has certainly proven to be the case with cyberwar, where cybersecurity firms have proliferated as wildly as the imagined threat has grown, and where the US Cyber Command "headquarters' budget alone … effectively doubled" between 2013 and 2014, even while the Defense Department overall experienced significant cuts (Singer and Friedman 2014, 134).

Although the 2007 cyberattacks are viewed as relatively primitive, the actions taken during the attacks have since become a model for how to make systems and organizations resilient during future cyberwars (Tiirmaa-Klaar, 2011b). Even when presented in generalized form, the examples for how to make systems more resilient frequently draw directly on 2007 cyberdefense activities (e.g., Singer and Friedman 2014, 171–2). And, as noted above, Estonian cyberwar transactors were instrumental in designing the policies that would make western European CII resilient to future cyberattacks.

With 2007 to burnish their international credentials, Estonian cybersecurity experts were at the forefront of the assistance provided to Georgia during the cyberattacks that accompanied armed conflict with Russia in August 2008. As presented in a Wikileaks-released document from the US Embassy in Tallinn (Wikileaks, 2008).

> Estonian experts all agree on one thing: Georgia was the latest victim of this new form of warfare, and the attacks are getting more effective each time. Estonia continues to lead international thinking on the cyber issue, having positioned itself as a niche expert on cyber defense based on its combination of past experience, a high level of IT expertise and dependence, and a small country's inevitable fears for its existence.

Two Estonian cybersecurity specialists participated in Georgia's cyberdefense, applying the lessons learned from 2007. One of the actions which lessened the impact of the cyberattacks was the decision to host the websites of the Foreign Ministry, the Ministry of Defense and the Presidency in other countries. Estonia served as backup host for Georgia's Foreign Ministry website. Estonian specialists at NATO CCDCOE immediately set to work assessing the cyberattacks, comparing them to the 2007 attacks against Estonia, and exploring the national and international legal recourses available to Georgia (Tikk et al., 2008). Estonian representatives also carried the lessons learned back to NATO and the EU, where they lobbied for improved cyberdefense strategies as well as clearer military and legal rules and procedures for responding to cyberattacks (Wikileaks, 2008).

Practicing cyberwar: cybersecurity exercises

If premediation is one process working to take the surprise out of the future, exercises are designed to make the future's indeterminacy knowable in another way. As a "technique of standardization" that makes "the unforeseeable foreseeable; rendering the event repeatable … (e)xercises are a means of effacing the singularity and unpredictability of events and producing the opposite of an event – a recognized occurrence" (Anderson, 2010a, 231).

In addition to establishing how to make CI systems more resilient, 2007 has made its way into scenario planning and cyberwar exercises. On the one hand, as a precautionary baseline, 2007 has been used to imagine how much worse cyberwar can and will become. A cybersecurity analyst at the NATO CCDCOE, for example, stated during an interview in 2011 that "The (2007) attacks were not large or serious, shutting down banks and financial transactions for a couple of hours. But what if it had been two days? And while Estonia's economy is not so critical, the attacks here raised consciousness about the prospects for cyberwarfare as a part of conventional conflict, especially if two major powers like China and the US were to go to war with one another."

Cyberwar scenarios for military exercises created by NATO, the EU, Estonia's MoD and the NATO CCDCOE have featured the 2007 and 2008 cyberattacks in Estonia and Georgia, and have reinforced the geopolitical bordering of cyberspace produced by these events and their remediation. *Cyber Europe 2010* and *2012* both featured broad-based DDoS attacks of the type launched against Estonia in 2007, even though most cybersecurity analysts interviewed for this paper argued that cyberweapons have gotten much more sophisticated and that the next cyberwar will not use such a simple and overt approach.

While cyberwar scenarios have become more elaborate and sophisticated since 2008, the boundary effect produced by naming the 2007 cyberattacks in Estonia 'the world's first cyberwar' continues to make its appearance in how allies and enemy others are imagined and performatively enacted. Beyond the 'Red Team' attacking and 'Blue Team' defending in tabletop exercises, Russia and China continue to be the assumed cyber-aggressors in a wide variety of cyberwar exercises. For example, NATO's *Cyber Coalition 2012* cyberwar exercise imagined a scenario in which a computer virus caused a NATO military transport plane to crash in Hungary while a cyberattack caused Estonia's CI to collapse. Although the attack was ostensibly launched from "an unnamed country in Africa … NATO representatives in private conversations have admitted that they consider Russia, China and Iran the key potential cyber aggressors" (RIA Novosti 2012). At approximately the same time, former US Secretary of Defense Panetta warned of American vulnerability to a "cyber-Pearl Harbor" which he visualized as "cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack." This combination Estonia 2007 – Georgia 2008 cyberwar scenario was issued as a warning in response "to increasing aggressiveness and technological advances by the nation's adversaries, which officials identified as China, Russia, Iran and militant groups" (Bumiller & Shanker, 2012).

Conclusion

Several years have passed since the Bronze Night and accompanying cyberattacks. In this period of time, the knowledge-power assemblage associated with national and international security has been transformed, as cyberwar has assumed a leading position as one of the greatest security threats facing the West and the world in the 21st century. This dramatic change has come about not as an effect of a major rupture such as 9/11, but rather from a relatively minor event on the margins of western assemblages of security. Yet both the timespace of its occurrence and the way in which it was managed amplified resonance, firing the imagination of policymakers and materializing cyberwar as a new policy object.

As cyberwar has emerged and become stabilized through an increasingly complex set of discursive practices, actors and institutions, Estonia and Estonians have used their State's location as the site of cyberwar's birth, along with their successful cyberdefense of Estonia, to establish, validate and maintain their own knowledge claims to expertise. They have established themselves as transactors of western cybersecurity, Tallinn as a critical node in the emerging cybersecurity network, and the NATO CCDCOE as a principal cyberwar center of calculation. Estonia's status as one of the most wired countries in the world, along with its small size and imagined position on a vulnerable frontier of western cyberspace, have been effectively deployed to validate Estonia's/Estonians' advanced cybersecurity status/expertise, as well as to remediate why the attacks took place. This western cybersecurity discourse also works to reproduce Russia/Russian-ness as the constitutive outside of Estonia, Europe and the West.

As cyberwar has become institutionalized over time, and as it has risen to compete with terrorism as the greatest danger confronting the West and the world, the apparatuses of cybersecurity have begun to leave the events 2007 behind, and the Estonian shimmering points in the cyberwar resonance machine have faded. Still, the originating event along with the site and situation of cyberwar's materialization continue to affect how the threat of future cyberwars is imagined, premediated and performatively enacted. The aporias of security that produced the Bronze Night and the cyberattacks, far from becoming the subject of critical analysis "to interrogate the images of self and other that animate (in)secure identities, and to expose the violence and repression that is so often relied on to police them" (Burke, 2002, 7), have been transposed onto cyberspace, and function as aporias of cybersecurity not only for Estonia and Estonians, but for how western cybersecurity itself is performatively enacted. As the initial events fade, the foundational aporias of cybersecurity become naturalized and sedimented in the everyday discursive practices through which western cyberspace is securitized.

Cyberwar and cybersecurity studies continue to be dominated by first order practitioners – intellectuals of statecraft and other cyberwar managers of unease. As they create policies, spin out scenarios, stage exercises and craft international laws to govern cyberwar, a new regime of truth becomes more firmly regularized and institutionalized, while a new set of citational practices becomes more naturalized and sedimented. This article has provided a second order analysis of cyberwar's birth and initial emergence in and through the events of 2007. It ends with a call to those who have done such brilliant work in critically interrogating risk and the war on terror to turn their attention towards this newly ascendant policy object, cyberwar.

Acknowledgments

I gratefully acknowledge the support received from the US National Science Foundation and the University of Helsinki's Aleksanteri Institute during the research and writing of this article. The article also benefited greatly from the insights and comments provided by Merje Kuus, Elena Nikiforova, James Sidaway, Gerard Toal, and four anonymous reviewers.

References

Aaviksoo, J. (2007a). *Cyber defense: The unnoticed third world war*. Estonian Ministry of Defense Website commentary on cyber defense http://www.mod.gov.ee/en/1468.

Aaviksoo, J. (2007b). *Cyberspace: A new security dimension at our fingertips*. CSIS Statesmen's Forum (Transcript by Federal News Service), 28 November http://csis.org/files/media/csis/events/071128_estonia.pdf.

Aaviksoo, J. (2008). Estonian approach to cyber security: Estonian national strategy on cyber security and Cooperative Cyber Defence Centre of Excellence. In *Address to the joint meeting of the OSCE Forum for Security Cooperation and Permanent Council, 3 June*. FSC-PC.DEL/18/08.

Adey, P., & Anderson, B. (2011). Anticipation, materiality, event: the Icelandic ash cloud disruption and the security of mobility. *Mobilities, 6*(1), 11–20.

Amoore, L. (2009). Algorithmic war: everyday geographies of the war on terror. *Antipode, 41*(1), 49–69.

Amoore, L., & de Goede, M. (2008). Transactions after 9/11: the banal face of the preemptive strike. *Transactions of the Institute of British Geographers, 33*(2), 173–185.

Anderson, B. (2010a). Security and the future: anticipating the event of terror. *Geoforum, 41*(2), 227–235.

Anderson, B. (2010b). Preemption, precaution, preparedness: anticipatory action and future geographies. *Progress in Human Geography, 34*(6), 777–798.

Anderson, B., & Adey, P. (2011). Affect and security: exercising emergency in 'UK civil contingencies'. *Environment and Planning D: Society and Space, 29*(6), 1092–1109.

Anderson, B., & Adey, P. (2012). Governing events and life: 'emergency' in UK civil contingencies. *Political Geography, 31*(1), 24–33.

Aradau, C. (2010). Security that matters. *Security Dialogue, 41*(5), 491–514.

Aradau, C., & van Munster, R. (2008). Taming the future. The dispositif of risk in the war on terror. In L. Amoore, & M. de Goede (Eds.), *Risk and the War on Terror* (pp. 23–40). New York and London, NY, USA: Routledge.

Arnett, E. (1992). Welcome to hyperwar. *The Bulletin of the Atomic Scientists, 48*(7), 14–21.

Arquilla, J. (2013). Twenty years of cyberwar. *Journal of Military Ethics, 12*(1), 80–87.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy, 12*(2), 141–165.

BBC. (2007). *Estonia hit by Moscow 'cyber war'*. BBC News, London, UK, 17 May http://news.bbc.co.uk/2/hi/europe/6665145.stm.

Barad, K. (2003). Posthumanist performativity. *Signs, 28*(3), 801–831.

Barnes, T. (2006). Geographical intelligence: American geographers and the research and analysis in the Office of Strategic Services 1941-1945. *Journal of Historical Geography, 32*(2), 149–168.

Barnes, J., & Gorman, S. (15 July 2011). Cyberwar plan has new focus on deterrence. *Wall Street Journal*.

Bernard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture, 15*(2), 110–123.

Bialasiewicz, L., Campbell, D., Elden, S., Graham, S., Jeffrey, A., & Williams, A. (2007). Performing security. *Political Geography, 26*(4), 405–422.

Bigo, D. (2002). Security and immigration: toward a critique of the governmentality of unease. *Alternatives, 27*(1), 63–92.

Billo, C., & Chang, W. (2004). *Cyber Warfare: An analysis of the means and motivations of selected Nation States*. Hanover, NH, USA: Institute for Security Technology Studies at Dartmouth College.

Blank, S. (2008). Web war I: Is Europe's first information war a new kind of war. *Comparative Strategy, 27*(3), 227–247.

Bruggemann, K., & Kasekamp, A. (2008). The politics of history and the 'war of monuments' in Estonia. *Nationalities Papers, 36*(3), 425–448.

Brunner, J. (1975). *The shockwave rider*. New York, NY, USA: Harper & Row.

Bumiller, E., & Shanker, T. (2012). Panetta warns of dire threat of cyberattack on U.S. *New York Times, New York, NY, USA*, 11 October.

Burke, A. (2002). Aporias of security. *Alternatives, 27*(1), 1–27.

Butler, J. (1993). *Bodies that Matter: On the discursive limits of "Sex"*. New York and London, NY, USA: Routledge.

Butler, J. (2010). Performative agency. *Journal of Cultural Economy, 3*(2), 147–161.

Clarke, R., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What To Do About It*. New York, NY, USA: HarperCollins.

Collier, S. (2008). Enacting catastrophe: preparedness, insurance, budgetary rationalization. *Economy and Society, 37*(2), 224–250.

Collier, S., Lakoff, A., & Rabinow, P. (2004). Biosecurity: towards an anthropology of the contemporary. *Anthropology Today, 20*(1), 3–7.

Connolly, W. (2005). The Evangelical-capitalist resonance machine. *Political Theory, 33*(6), 869–896.

Conti, G., & Surdu, J. (2009). Army, Navy, Air Force and Cyber – is it time for cyberwarfare branch of military? *IAnewsletter, 12*(1), 14–18.

Cyber Security Strategy Committee. (2008). *Cyber security strategy*. Tallinn, Estonia: Ministry of Defence.

Czosseck, C., Ottis, R., & Taliharm, A.-M. (2011). Estonia after the 2007 cyber attacks: legal, strategic and organizational changes in cyber security. *Journal of Cyber Warfare and Terrorism, 1*(1), 24–34.

Davis, J. (2007). Hackers take down the most wired country in Europe. *Wired Magazine, 15*(9), 21 August http://www.wired.com/politics/security/magazine/15-09/.

Denning, D. (2001). Cyberwarriors: activists and terrorists turn to cyberspace. *Harvard International Review, 23*(2), 70–75.

Elliott, D. (2011). Deterring strategic cyberattack. *IEEE Security and Privacy, 9*(5 (Sept/Oct)), 36–40.

European Commission. (2008). *Workshop on learning from large scale attacks on the internet: Policy implications*. Brussels, Netherlands: EU Commission, 17 January.

European Commission. (2009). *Protecting europe from large scale cyber-attacks and disruptions: Enhancing preparedness, security and resilience*. Brussels, Netherlands: Commission of the European Parliament, 30 March.

Ewald, F. (2002). The return of Descartes' malicious demon: an outline of a philosophy of precaution. In T. Baker, & J. Simon (Eds.), *Embracing risk* (pp. 273–302). Chicago, IL, USA: University of Chicago Press.

Feldman, M. (2001). Russia and Europe in the Estonian security discourse. In P. Joenniemi, & J. Viktorova (Eds.), *Regional Dimensions of Security in Border Areas of Northern and Eastern Europe* (pp. 254–264). Tartu, Estonia: Tartu University Press.

Foucault, M. (2008). *The birth of biopolitics*. Hampshire, UK and New York, NY, USA: Palgrave Macmillan.

Geers, K. (Spring 2010). *Cyber defence. Glance at the Mirror 2009: Estonia as reflected by foreign media*. Estonian Ministry of Foreign Affairs, Tallinn, Estonia. First published in Common Defence Quarterly http://www.vm.ee/?q=node/9071#lahing.

Gjetlen, T. (2010). *Seeing the internet as an information weapon. NPR*, 23 September http://www.npr.org/templates/story/story.php?storyId=130052701.

de Goede, M. (2008). Beyond risk: premediation and the post-9/11 security imagination. *Security Dialogue, 39*(2–3), 155–176.

Gregory, D. (2011). The everywhere war. *The Geographical Journal, 177*(3), 238–250.

Gregory, D. (2014). Drones and the everywhere war. In *Yi Fu Tuan Lecture series*. Department of Geography, University of Wisconsin – Madison, Madison, WI, USA, 28 March.

Grusin, R. (2004). Premediation. *Criticism, 46*(1), 17–39.

Grusin, R. (2010). *Premediation: Affect and Mediality after 9/11*. New York, NY, USA: Palgrave Macmillan.

Ilves, T. (2007a). My smozhem postroit' nashe obshchee budushchee. *Narvskaya Gazeta*, 2 May.

Ilves, T. (2007b). *President Ilves: Our own careless satisfaction and slack thinking that everything is okay are among Estonia's greatest enemies*. Press Reports, 1 June. Office of the President, Public Relations Department, Tallinn, Estonia.

Ilves, T. (2007c). *President of the Republic on Victory Day, 23 june 2007, in Rapla*. President of the Republic of Estonia, Speeches, 23June.

Kaiser, R. (2012). Reassembling the event: Estonia's bronze night. *Environment and Planning D: Society and Space, 30*(6), 1046–1063.

Kaiser, R. (2014). Performativity, events and becoming-stateless. In R. Rose-Redwood, & M. Glass (Eds.), *Performativity, Politics, and the Production of Social Space* (pp. 121–143). New York, NY, USA: Routledge.

Kaiser, R., & Nikiforova, E. (2008). The performativity of scale. *Environment and Planning D: Society and Space, 26*(3), 537–562.

Kallas, K. (2011). *IT Agency: the European Union's greatest IT challenge? Hea Eesti Idee*, 11 January http://hei.eas.ee/index.php?option=com_content&view=article&id=1242:it-agency-the-european-unions-greatest-it-challenge&catid=93:2011-january.

Kaska, K., Talihärm, A.-M., & Tikk, E. (2010). Developments in the legislative, policy and organisational landscapes in Estonia since 2007. In E. Tikk, & A.-M. Talihärm (Eds.), *International Cyber Security Legal and Policy Proceedings* (pp. 40–66). Tallinn, Estonia: CCD COE Publications.

Kirk, J. (2007). Cyber-war – the way of the future? *IDG News Service*, 18 May.

Klimberg, A., & Tiirmaa-Klaar, H. (2011). *Cybersecurity and Cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU*. Brussels, Netherlands: European Parliament, Directorate-General for External Policies. Policy Department (EP/EXPO/B/SEDE/FWC/2009-01/Lot6/09).

Kuus, M. (2004). 'Those goody-goody Estonians': toward rethinking security in the European Union candidate states. *Environment and Planning D: Society and Space, 22*(2), 191–207.

Kuus, M. (2014). *Geopolitics and expertise*. Chichester, UK: John Wiley & Sons.

Landler, M., & Markoff, J. (29 May 2007). After computer siege in Estonia, war fears turn to cyberspace. *New York Times*.

Latour, B. (1987). *Science in action*. Cambridge, MA, USA: Harvard University Press.

Latour, B. (2005). *Reassembling the Social*. Oxford, UK and New York, NY, USA: Oxford UP.

Lehti, M., Jutila, M., & Jokisipila, M. (2008). Never-ending second world war: public performances of national dignity and the drama of the bronze soldier. *Journal of Baltic Studies, 39*(4), 393–418.

Lesk, M. (2007). The new front line: Estonia under cyberassault. *IEEE Security & Privacy, 5*(4 (July/Aug)), 76–79.

Lewis, J. (2011). Cyber attacks, real or imagined, and cyber war. *CSIS Commentary*, 11 July http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war.

Libicki, M. (2009). *Cyberdeterrence and cyberwar*. Santa Monica, CA, USA: Rand Corp.

LICHR. (2007). *Bronze Soldier: April crisis*. Tallinn, Estonia: Legal Information Centre for Human Rights.

Massumi, B. (2007). Potential politics and the primacy of preemption. *Theory and Event, 10*, 2. no pagination.

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations* (Discussion Paper #2011-11). Cambridge, MA, USA: Harvard Kennedy School, Belfer Center for Science and International Affairs.

McAfee. (2009). *Virtual Criminology Report 2009: Virtually Here: The Age of Cyber Warfare*. Santa Clara, CA, USA: McAfee. www.mcafee.com.

Meyer, D. (2010). ITU head: cyberwar could be 'worse than tsunami'. *ZDNet*, 3 September http://www.zdnet.com/itu-head-cyberwar-could-be-worse-than-tsunami-3040089995/.

Mite, V. (2007). Estonian attacks seen as 'cyberwar'. *RFE/RL*, 30 May.

Mountz, A. (2010). *Seeking Asylum*. Minneapolis, MN, USA: University of Minnesota Press.

NATO. (2002). *Prague Summit declaration*. NATO Press Release, Prague, Czech Republic. #127, 21 November.

NATO. (2009). *NATO and cyber defence*. NATO Parliamentary Assembly Committee Report 173 DSCFC 09 E bis, NATO Parliamentary Assembly; Brussels, Netherlands.

NATO. (2010a). Active engagement, modern defence. In *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization. Adopted at the NATO Lisbon Summit, 17–19 November*. Brussels, Netherlands: NATO Public Diplomacy Division.

NATO. (2010b). *NATO 2020: Assured security, dynamic engagement*. Brussels, Netherlands: NATO Public Diplomacy Division, 17 May.

NATO. (2011). *Resolution 387 on cyber security*. NATO Parliamentary Assembly http://www.nato-pa.int/Default.asp?SHORTCUT=2629.

NATO. (2012). *NATO and cyber defence*, 2 August http://www.nato.int/cps/en/natolive/topics_78170.htm.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare and Security, Plymouth, 2008* (pp. 163–168). Reading, UK: Academic Publishing Limited.

Ottis, R. (2010). The vulnerability of the information society. *Futuregov Asia Pacific*, 70–72. August-September.

Paabo, H. (2008). War of memories: explaining 'memorials war' in Estonia. *Baltic Security and Defence Review, 10*(1), 5–28.

Public Radio International. (2010). *Estonia: The cyber-defense capitol of the world*. PRI's The World, Minneapolis, MN USA, 8 July.

RIA Novosti. (2012). Russia potential aggressor for NATO. *RIA Novosti*, 18 October (http://en.ria.ru/military_news/20121018/176715380.html.

Robert, S. (2012). The state of cyberwar in the U.S. *DiploNews*, 6 February http://www.diplonews.com/reports/2012/20120205_L_CyberWar.php.

Ruus, K. (2008). Cyber war I: Estonia attacked from Russia. *European Affairs*, 9(Winter/Spring). http://www.europeaninstitute.org/2007120267/Winter/Spring-2008/.

Salter, M. (2008). Risk and imagination in the war on terror. In L. Amoore, & M. de Goede (Eds.), *Risk and the War on Terror* (pp. 233–246). New York and London, NY, USA: Routledge.

Schmitt, M. (Ed.). (2013). *Tallinn Manual on International Law applicable to Cyber Warfare*. Cambridge, UK: Cambridge University Press.

Singer, P., & Friedman, A. (2014). *Cybersecurity and cyberwar*. New York, NY, USA: Oxford University Press.

Sommers, P., & Brown, I. (2011). Reducing Systemic cybersecurity risk. In *OECD/IFP Project "Future global shocks" report IFP/WKP/FGS(2011)3*. OECD, Paris, France, 14 January.

Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy, 33*(1), 148–170.

Tanner, J. (2007). Is Russia waging cyberwar? – Web crashes threaten Estonia's security. *redOrbit*, 18 May http://www.highbeam.com/doc/1P2-21786747.html.

Tiirmaa-Klaar, H. (2011a). Cyber security threats and responses at global, nation-state, industry and individual levels. *Ceri SciencesPo*. March http://www.ceri-sciences-po.org.

Tiirmaa-Klaar, H. (2011b). *How Estonia is helping to shape cyber resilience*. Defence IQ Press, London, UK, 24 July.

Tikk, E., Kaska, K., Runnimeri, K., Kert, M., Taliharm, A., & Vihul, L. (2008). *Cyber attacks against Georgia: Legal lessons learned*. Tallinn, Estonia: CCD COE.

Tikk, E., & Kaska, K. (2010). Legal cooperation to investigate cyber incidents: Estonian case study and lessons. In *Proceedings of the 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01–02 July* (pp. 288–294). Reading, UK: Academic Publishing Limited.

Toure, H. (2011). *The Quest for cyber peace*. Geneva, Switzerland: International Telecommunications Union.

Traynor, I. (2007). Russia accused of unleashing cyberwar to disable Estonia. *The Guardian*, 19 May http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

US House of Representatives. (2000). *Computer Security: Are We Prepared for Cyberwar?* Washington, DC, USA: US Government Printing Office. Serial No. 106-160, 9 March.

Weiss, M. (2007). *Here come the cyberwars*. Reason, 17 August http://reason.com/archives/2007/08/17/here-come-the-cyber-wars/print.

White House. (2000). *Defending America's Cyberspace: National Plan for Information Systems Protection 1.0*. The White House, Washington, DC, USA.

Wikileaks. (2008). *Estonia charts legal, military future of cyber warfare (including applicability of Nato's Article V)*, 22 September http://wikileaks.org/cable/2008/09/08TALLINN326.html.