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

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