## 1AC – Cyberwar

### Roberto’s Edits

#### The entrance of cyberwar into this year’s topic can be traced to the 2007 Bronze Night attacks in Estonia. The cyberattacks that accompanied the protests materialized cyberwar as a policy object for security analysts in NATO and the U.S. The new discursive resonance of cyberwar throughout the alliance catalyzed the apocalyptic imaginations of scenario planners while vaulting Estonia into the center of calculation for global conflict between East and West. This resonance machine that constructs endless news events of Baltic cyberconflicts always on the verge of escalation forecloses alternative political horizons by routing meaning toward actionable military scenarios.

Kaiser, 15 (Robert, Professor of Geography @ Univ. Wisconsin-Madison, PhD (Geography) from Columbia University, recipient of a Visiting Fellowship on Estonia and the Birth of Cyberwar @ Aleksanteri Institute via the University of Helsinki; "The Birth of Cyberwar," *Political Geography*. 46 (2015) 11-20.)

“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 and 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, 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, Anderson, 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.

#### The attribution of the Bronze Night cyberattacks as a Russian act of war against Estonia and NATO is not neutral, but rather an active fiction constructed by security experts and think tanks to fire the imaginations of policy makers and the public around a New Cold War. Just as Estonia’s internal ethno-political antagonisms had to be invisiblized to construct a narrative of interstate conflict, cybersecurity materializes the boundary conflicts of peoples, territories, and orders-of-meaning into constitutive threats that are then installed at the center of security concerns. The attempt to reconstruct Article 5 around cyber war reveals the performative nature of security, and the aporia of meaning at the heart of security, transparency, and expertism.

Kaiser, 15 (Robert, Professor of Geography @ Univ. Wisconsin-Madison, PhD (Geography) from Columbia University, recipient of a Visiting Fellowship on Estonia and the Birth of Cyberwar @ Aleksanteri Institute via the University of Helsinki; "The Birth of Cyberwar," *Political Geography*. 46 (2015) 11-20.)

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 and 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, Gregory, 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 and 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 et al., 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’. 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 and 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 and 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/Russian-ness – 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.

#### There is no such thing as cyberwar in any technical or “meaningful” sense – there is only the militarization of knowledge and meaning that invests epistemology as a battlespace and distributes warfare in everyday life.

#### Cyberwarfare must be understood as the deconstruction of deconstruction itself – an attack on meaning systems that impairs even our ability to know if the attack occurred. Fake wars and classified NSA cyberops materialize our anti-knowledge, turning nonwar into war, as the specter of catastrophe inscribed into the present and future by think tanks and security professionals.

#### Rather than a security dilemma, cyberwar must be understood as a conflict over meaning that erases and rewrites the very archives and epistemes that trace its existence. The question of alliances is not an inquiry into warfare, but rather an inquiry into the destruction of meaning that constitutes nonwar as ongoing catastrophe.

Joque, 18 (Justin Joque, researcher and visualization librarian @ UMich, Master's of Science of Information at the UMich School of Information, PhD in Communications at the European Graduate School. “INTRODUCTION: Root Kit,” Deconstruction machines: Writing in the age of cyberwar. University of Minnesota Press, 2018)

There is no easily agreed-upon definition of cyberwar. Even within closely related literatures, there exists an ongoing debate over what constitutes cyberwar. Some, such as Rid, who has written at length declaring there is no such thing as cyberwar, question whether such a concept is a helpful lens for thinking the present situation at all.1 The term cyberwar, in most invocations, refers to the notion of cyberspace and the possibility of a war carried out in this global networked space, wherein computer systems are taken over to disrupt and surveil an enemy’s communication and networked infrastructure either as part of a “kinetic” war or as a form of low-level conflict aimed at gaining geopolitical advantages. Though it is important to follow authors, strategists, legal scholars, and others wherever they happen to see “cyberwar” occurring, one particular etymological meaning will guide this inquiry. The prefix cyber- refers to the term cybernetics. Cybernetics, originating from the Greek kubernētēs (“steersman” or “governor”), is the science and study of systems, their structures, regulation, emergent properties, and possibilities, spanning disciplines from technology to biology to society. By explicitly thinking the cyber- in cyberwar as referring to systems, it will be fruitful to understand cyberwar as a war against systems: computer systems, state systems, systems of organization, and even systems of meaning. This etymological understanding of cyberwar closely mirrors some of the earliest deployments of this term. One of the first unclassified uses of the term cyberwar comes from a 1992 publication by Arnett.2 For him, the term means the replacement of human operators with machines that decide on targets, trajectories, movement, and so on—essentially the culmination of a long history of the insertion of “intelligent machines” into the arsenal of war fighting. That same year, Der Derian used the term “in the sense of a technologically generated, televisually linked, and strategically gamed form of violence.”3 Arquilla and Ronfeldt subsequently published a paper defining cyberwar as a tactical and strategic movement whereby communication, information, and the visibility of the battlespace become the central concern. They assert that while information technology brings cyberwar to the fore, it is not necessarily a technological phenomenon. In fact, the exemplary case of cyberwar they recount is a thirteenth-century Mongol offensive against Khwarizm, where the Mongols succeeded in defeating a significantly larger army by cutting off communications and disrupting the control of forces. These definitions complement each other. Der Derian and Arnett’s definitions focus on carrying out a kinetic war through the cybernetic organization of humans and technology, while Arquilla and Ronfeldt’s definition stresses disrupting all of the enemy’s cybernetic systems regardless of whether they are human, technological, or a combination. We are faced, then, with something much more expansive than war in cyberspace; rather, what these authors begin to explore in the early 1990s is an understanding of war in which one tries to construct and defend systems of communicating, knowing, controlling, and, ultimately, existing. Simultaneously, one attempts to disrupt, infiltrate, corrupt, and destroy these same systems belonging to the enemy. Arquilla and Ronfeldt state that such a strategy “may aim to confound people’s fundamental beliefs about the nature of their culture, society, and government, partly to foment fear but perhaps mainly to disorient people and unhinge their perceptions.”4 Clearly this is not completely new. Belligerents have always attempted to deceive their opponents and disrupt economies and governments. Furthermore, war has often had as a central objective the destruction of one critical system and the infiltration of another: the body and the territory of the opponent. Despite this, we can outline three critical factors that mark cyberwar as a historical shift. First, proponents of cyberwar, such as Arquilla and Ronfeldt, stress that in cyberwar, information and structures of knowing become central rather than peripheral to conflict. They say that cyberwar “means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself.”5 Second, cyberwar attempts to disrupt not only the enemy’s knowledge but also the entire structure of knowledge. In short, cyberwar invests epistemology itself as a battlespace. Third, cyberwar seeps outside of “war” proper. In calling into question modes of knowing, cyberwar breaks down the limits of the time and space of war. Thus the term cyberwar describes two distinct but related phenomena. On one hand, it is a strategy for fighting war, and we will include whatever is named cyberwar by strategists, legal theorists, authors, and warriors. On the other hand, we will mean a historical shift—in a sense, a global cyberwar that marks a tendency whereby the critical element in war becomes the flow of information and the fortification and disruption of systems. In making this shift, cyberwar has opened an epistemological and cybernetic battlespace wherein notions of war, enmity, and knowing become directly contestable. While these concepts have always been unstable and problematic, cyberwar seizes them as systems of direct military intervention, turning what was once a question for philosophers into a domain of the global battlespace. In its most abstract sense, cyberwar has become an event that calls everything including itself into question at the moment it arrives. It is the historical possibility that all systems may break down—or, in their military occupation, be caused to break down—but it is also possible that cyberwar may undermine itself before anything actually “happens.” Cyberwar as historical event marks a moment of radical militarized unknowability. Many discussions of cyberwar, be they historical, strategic, or legal, begin not with the earliest examples or contemporary attacks but rather with a future catastrophe that demonstrates the danger of our overreliance on vast, connected, yet vulnerable systems. These catastrophes normally start with a nonstate actor or a “rogue” state hacking into key networks, destroying critical infrastructure in the United States or multiple European countries. Airplanes crash into each other, trains derail, communication channels shut down, and electrical systems are disabled. Not only are these systems forced to shut down but they are hijacked and made to spin out of control, sometimes destroying themselves so completely that they would take months to return to normal usage. These imagined scenarios often place the reader at the time immediately following the catastrophe. At this point in time, one can survey the wreckage of our technological hubris before the aftermath begins in earnest. It is the moment when the full scale of a possible collapse is revealed but not yet realized.6 Where a historical account begins in the past, it often starts with a CIA attempt to secretly destroy a Soviet gas pipeline.7 According to Thomas Reed, a National Security Council staffer, in 1982, the CIA was able to insert an intentionally faulty piece of code into a pump that the Soviet Union obtained from a Canadian company. According to Reed’s account, the pump was installed in the Trans-Siberian gas pipeline; varying pump speeds and valve settings produced extreme pressures that caused an explosion large enough to be detected by U.S. satellites. The secret introduction of a so-called logic bomb—a somewhat antiquated term for a malicious piece of code inserted into software—has been touted by a number of commentators as one of the earliest examples of cyberwar. Although Reed, who made this story public for the first time in a 2004 book, never referred to this attack as cyberwar, this story has become something of an origin myth for those who write about cyberwar more generally.8 The event prefigures a number of issues that arise again and again in the myriad discourses surrounding cyberwar. Most important, it becomes clear how vulnerable complex systems of computation have become. These systems aggregate code written across the globe and parts manufactured outside the purview of their owners into complex networks that belie attempts to control them. Computation is exposed to the exterior places in which it is produced. Furthermore, even if unintentionally, the use of this event as the first in a series of international cyberattacks offers an answer to a question that is often asked of theorists of cyberwar: how can such an event lay claim to being “war”? Is this merely sabotage? Placing the origin in the Cold War responds to those critics of cyberwar hype who believe it is nothing more than a collection of high-tech tools in service of the ancient techniques of spying, deception, and sabotage. For the Cold War proved that wars need not be explosive and could consist of decades of low-level conflict. As Virilio says of the threat posed by nuclear weapons, “the weapon’s serious danger is not that it could explode tomorrow. . . but that for thirty years it has been destroying society.”9 The bomb’s destructive power has been felt directly through its threat. Likewise, as can be seen in the futuristic scenarios described earlier, cyberwar seems always to threaten catastrophe. Placing cyberwar’s origins in the Cold War suggests the possibility of a nonwar that is as destructive as a kinetic war. The second half of the twentieth century has demonstrated that even in the absence of a hot war, conflict can destroy governments and societies. Furthermore, at least for those theorists and strategists of cyberwar in the United States, this origin story contextualizes contemporary cyberwar discourses in another way. Several military and political commentators writing about cyberwar as a strategic area of study were the same theorists who worked on nuclear deterrence strategy in the latter part of the Cold War. A number of authors—many of whom work for the RAND Corporation, a think tank that was created in 1948 to provide research and analysis to the U.S. military—even attempt to employ strategies learned from nuclear deterrence research to mitigate military hacking and offensive use of global networks.10 Tying the origin of cyberwar to Cold War global strategic thinking offers an opportunity for those making the transition from strategizing in a bipolar world defined by nuclear weapons to a multipolar, interconnected global economy. While the Siberian pipeline attack’s similarity to contemporary issues surrounding cyberwar is noteworthy, the most striking aspect of the whole affair is that it possibly never happened. Following the release of Reed’s book, an ex-KGB officer with direct knowledge of the region at the time disputes Reed’s account. He acknowledged there was an explosion but claims it was at a different, smaller pipeline and was caused by specific construction mistakes, not by faulty equipment.11 Moreover, no known media reports from the time confirm an explosion, which Reed claims was the size of a small nuclear blast. Other than Reed’s account, no other documentation has been found, and the CIA has never confirmed the event.12 The origins of cyberwar in this event are seemingly impossible to verify. Pipeline explosions were common at the time, and there would have been no way for the CIA to know for certain if it was caused by their purposefully faulty equipment or accidently faulty Soviet equipment. Given our current evidence, the event is completely unknowable. Moreover, even if there was an explosion, it is impossible to verify if it was the logic bomb or a mechanical failure. Depending on one’s perspective, either the fake event or fake refutations seep into the historical record like a computer virus corrupting the system’s memory. Thus, in a largely unrecognized way, this event is archetypal for cyberwar. Cyberwar and cybersecurity weave a complicated relationship between the knowable and the unknowable. Our networked world has become so complex in sheer technical terms that the system as a whole cannot be known from the outside. Mapping even just the public Web has become a scholarly pursuit in its own right. Computers and networks represent information as tiny bits on a magnetic disk or pulses of light across a cable that, owing to their size, speed, and complexity, are on their own essentially meaningless and impenetrable to human observers. One always interacts with abstractions and complex representations of the material reality of computing. Cyberwar, in attacking these systems, is always on the verge of being meaningless itself. Moreover, in attacking systems of knowing that guarantee information, a successful attack impairs even our ability to know if something has happened. Cyberwar is fought precisely in this space between the possible catastrophe and the possibility of nothing happening at all. The event itself is ambiguous and our public historical record is already compromised. It could of course be argued that all history is ambiguous, constructed, and selective. What is unique in the case of cyberwar is that the whole structure of knowing and observing is opened as a site of direct military intervention. It is not only a question of interpretation and selective archives. The entire archive and our ability to comprehend the archive may be attacked at any moment. In a sense, we are dealing with a limit case of historical unknowability—not just ambiguity but a military attack on the data of history itself. Now, even if the victors write history, it may no longer be written from data they control. Thus an effective understanding of cyberwar will only be possible by not prematurely deciding in favor of an event happening or not happening. Cyberwar operates both as a strategy and as a mediatized cultural phenomenon directly in the space between happening and not happening. It succeeds as a military strategy by never succeeding too much. It always seems to be leading us to the verge of catastrophe and at the same time to an interminable boredom where nothing will ever actually happen. Cyberwar could easily be dismissed as not really being war or violent, but what is so virulent and dangerous about cyberwar is its ability to atomize and distribute warfare into everyday life. Cyberwar succeeds so much more effectively for being either overhyped or dismissed. Ultimately, we must resist deciding in favor of catastrophe or boredom, for in doing so, the entirety of cyberwar will certainly escape us. Instead, we must attempt to interrogate the history and discourses of cyberwar by following its vacillations between these two poles as it hides in the theoretical space between war and nonwar.

#### Cyberwar reveals the collapse of meaning through informatic erasure, as all information becomes flooded with computational propaganda where militarized digital catastrophe shapes the present by its future possibility. This uncertainty cannot be rendered transparent though geostrategic calculation, but rather as an impasse that mirrors and exceeds nuclear war.

Joque, 18 (Justin Joque, researcher and visualization librarian @ UMich, Master's of Science of Information at the UMich School of Information, PhD in Communications at the European Graduate School. *Deconstruction machines: Writing in the age of cyberwar*. University of Minnesota Press, 2018) \*modified for ableist language

The systems that are attacked through cyberwar are dual entities: on one hand, they are defined by a series of connections, and on the other hand, they are defined by the text of programs and messages that are sent through the network. The networked structure of the global Internet allows malicious programs to quickly propagate, but it is the insecurity of individual systems and the computer programs they run that are exploited to attack these networks. Without the insecurity of these programs and messages, cyberwar would never be a strategic possibility. While computer programs are often considered to be overly deterministic and simply a series of rules for a machine to follow, the very existence of cyberwar suggests that programs are not so straightforward. Programming is a textual and linguistic practice that is always carried out in languages and at levels of complexity that preclude complete mastery over what is written. Cyberwar infiltrates and subverts these programs, turning the text and logic of the program against itself. To fully grasp what is at stake in cyberwar, it is then critical to understand the logic of writing, especially the logic of writing at its most vulnerable. In this light, cyberwar is ultimately a process of deconstructing programs and undermining them from within their own logical and linguistic systems. As such, it is a form of writing itself, a writing that is aimed at both shoring up and deconstructing other texts. To understand cyberwar in this way, then, also requires a reconceptualization of deconstruction and its functioning. Admitting the textual nature of code and the machinic force of deconstruction overwhelms any attempt to maintain that deconstruction has ever been an exclusively theoretical matter or could ever be secured against its possible usage by the state and military. Cyberwar, in harnessing and exploiting the vulnerable and machinic nature of writing, is thus both a form of deconstruction and a deconstructive threat to deconstruction itself. Still, this threat to deconstruction and the logic of writing does not spell the end of deconstruction but rather guarantees its continued importance to the history of both writing and metaphysics. GLIMPSES OF THE FUTURE CATASTROPHE One of the earliest glimpses of the possible impact of an all-­out cyberwar occurred in June 1997. A small team of hackers using publicly available tools and programs was supposedly able to gain access to the power grid in nine U.S. cities, those cities’ emergency response systems, and a number of critical Pentagon networks, including those that managed military supply chains and the command-­ and-­ control structure. According to James Adams, who has written at length about these attacks, the hackers also managed to infect the human command-­ and-­ control system with a ~~paralyzing~~ level of mistrust. Orders that appeared to come from a commanding general were fake, as were bogus news reports on the crisis and instructions from the civilian command authorities. As a result, nobody in the chain of command, from the president on down, could believe anything. This group of hackers using publicly available resources was able to prevent the United States from waging war effectively.1 Luckily, the series of attacks, which have been code-­ named Eligible Receiver, were carried out by the [NSA] National Security Agency as an unannounced test of military and civilian digital infrastructure. The attackers, who were working as part of a No-­Notice Interoperability Exercise Program, were asked only to prove what was possible and not actually to destroy anything. Though the military provided no substantial evidence about Eligible Receiver, aside from interviews with the media and vague congressional testimony, for a while, Eligible Receiver was repeatedly referenced as a brief glimpse of future war and the dark nature of our digital technologies.2 Of course, there were those who were sure it was merely the media-­ security complex displaying its newest boogeyman. In a hacking publication titled The Crypt Newsletter, whose provenance and history seem to have gone the way of dial-­ up modems but which still lingers in search-­engine-­indexed text files in various parts of the Internet, Joseph K refers to Eligible Receiver as “a Pentagon ghost story repeated ad nauseum to journalists and the easily frightened in which ludicrous or totally unsubstantiated claims about menaces from cyberspace are passed off as astonishing deeds of techno-­ legerdemain performed by cybersoldiers working within a highly classified wargame.” Although Joseph K meant to dismiss Eligible Receiver, the discourse surrounding it still tells an interesting ghost story, especially if it is treated as such and read not as baseless but as a myth that functions even without proof. John Arquilla summed up the state of the public relation to the event aptly when, in an interview with PBS, he said, “Eligible Receiver is a classified event about which I can’t speak. What I can say is that when people say there is no existence proof of the seriousness of the cyber threat, to my mind, Eligible Receiver provides a convincing existence proof of the nature of the threat that we face.”3 This Kafkaesque claim is telling: he cannot tell us what transpired, but its existence, despite being under classified erasure, proves his point. This event appears in this light not then as an attack against military information systems but instead as an attack against our belief in the digital systems that increasingly provide the fabric of our everyday lives. Perhaps in Adams’s claims that no one could believe anything from the president on down, we should read a warning that we, too, outside the wargame, can no longer believe anything— ­that, ultimately, the collapse of the entire system may already be upon us. It takes little extra imagination to suggest that the implied result is some catastrophic social collapse, which may already be under way. It is not merely our military communication technologies that are at stake in Eligible Receiver but the entirety of society. Computer systems, especially when seen as data storage devices, function to guarantee that past inscriptions persist into the future. Computer security is often discussed as being founded on the “CIA triad,” standing for confidentiality, integrity, and access. Confidentially requires that only authorized users have access to information. Integrity is the need that the information that is put into a system is the same information that is retrieved, and access suggests that if authorized users cannot retrieve information, no matter how secure that information is, the system is useless.4 All of these function not just in the present but as guarantees of past and future. For a system to be secure under these conditions, the system must assure that the data entered in the past extend into the future and avoid unauthorized compromise. Cyberattacks instantly call all three of these into question in the past, present, and future. The futurity of a “real” attack like Eligible Receiver infects our belief in these systems in the present. Garrett Schubert, of EMC’s Critical Incident Response Center, tasked with protecting EMC’s data centers from cyberattacks, describes his work directly in relation to a change in temporality: “When I started in my career, the idea was, we wanted to stop a bad thing from happening. Now, we assume that the bad thing has already happened. Every single day, we walk in and we assume there is an active attack going on.”5 The future catastrophe has become a part of the daily operations of our technologies. As Parikka claims, the inscription of information in media is the invention of the accident of information erasure.6 The database always contains within it the immanent possibility that the data are, or may be, corrupted. As much as this unannounced test exercise may have been a test of military security, it is also a test of our belief in the future of our digital world. Joseph K’s mocking dismissal then appears, like a pithy sermon by an unknown sage of our digital belief, to reassure us that these events are merely phantasms thought up to terrify the gullible and will never come to pass. At the same time, the complete dismissal of this ghost story bifurcates the future: on one hand, the possibility of utter collapse, and on the other, complete faith and resilience. Likewise, it doubles the structure of belief and skepticism. Are the believers those who put faith in our technological world or those who blindly take the military’s word that the catastrophe is around any corner? If we cannot believe “anyone from the president on down,” how can we believe those who call that belief into question? THE INFORMATIONAL UNCANNY We arrive at an impasse that mirrors the Cold War nuclear catastrophe, not in terms of the destruction of life but in terms of the destruction of meaning. Though the relationship between the digital and the symbolic is complex, if the material support of meaning— be it magnetic bits, flashes of light in a fiber optic cable, or paper writing— is destroyed, then so too is the possibility of meaning. If the bits that store our digital writing are effaced, so too is any message they may carry. A nuclear catastrophe destroys meaning by destroying potential readers and the material of writing, whereas a digital catastrophe destroys meaning and inscription by destroying the microscopic material support. As these digital communications are entrusted more and more, what is at stake is the whole system of believing in the integrity of one’s information, and with it the integrity of all systems. We arrive, then, at a similar situation to what Paul Saint-­Amour refers to as the nuclear uncanny: “Because it offers the possibility of a future without symptoms, without a symbolic order— ­ in other words, no future at all— the nuclear condition can, in a sense, only cause anticipatory symptoms.”7 Likewise, the militarized digital catastrophe shapes the present by its future possibility. Saint-­Amour’s argument is helpful in that it places the futurity of such events clearly in the present. He suggests that such a catastrophe, especially because it destroys the symbolic, must produce its effects in the present. If this future catastrophe undermines the symbolic in the present, we begin to enter a space of what we could call militarized deconstruction. The ability for any program, database, or text to control its meaning and intent is instantly destabilized. As Parikka argues, “apocalypses reveal new temporalities, new layers for a media archaeology of the present.”8 The possibility of a catastrophe places the full meaning of programs and networks always in the future but their symptomatic expression in the present. Their complete meaning can only be understood after their looming breakdown. In short, despite the linear and programmatic nature of a program’s execution, the deferral of meaning and the non-­ self-­ sameness opened by its potential insecurity guarantee that the relation between the text of the program and its action in the world is governed by play, différance, and the impending possibility of its deconstruction. This catastrophic threat to the future of databases suggests that they are ultimately shaped by the structure of what Derrida calls arche-­writing (the originary structure of non-­ self-­ presence and externalization that shapes all existence— the ­ violence of our being in the world). When Hägglund explains arche-­ writing, we could easily imagine that he is speaking about a computer rather than a human subject:

#### In essence, cyberwar is built through the integral accident – the incapacity of cyber-mastery that interrupts our capacity to use or create meaning from cyber-events, even as they animate disastrous security policy.

#### Such miscalculations are intrinsic to the cybernetic autopoesis of the nonwar that is cyberwar. Computational propaganda mystifies occupations and conflicts to make any coherent theory of warfare or alliances impossible. In the sea of misattribution, there is always another opinion, and the inescapably provisional and easily falsified nature of all accounts of cyberwar energizes the death of meaning itself. In the face of the opacity of cyberconflict, desire tends toward militarized paranoia, accepting the experts of Empire just as easily as fake news. The impact is a global civil war operating at every level that far surpasses any Russian threat.

Matviyenko et al. 19 (Svitlana Matviyenko, Assistant Professor of Critical Media Analysis in the School of Communication of Simon Fraser University in Vancouver. Nick Dyer-Witheford, associate professor in the Faculty of Information and Media Studies at University of Western Ontario. “Introduction,” *Cyberwar and Revolution, Digital Subterfuge in Global Capitalism,* University of Minnesota Press,Mar 12, 2019) \*modified for ableist language

Within cyberwar apparatuses, humans, for the moment, remain a necessary link or relay enlisted in multiple ways, voluntary and involuntary. Yet while humans remain in the loop, or on the loop (that is to say, with a veto on otherwise automatic processes), it is within a war-fighting system that increasingly decenters subjectivity as a “peripheral” (Gibson 2015). Because of this, the human subject of cyberwar is dazed and confused. This is in part a consequence of the intentional secrecy of cyberwar, but the possibilities of such stealth, and its intensification by contingency and accident, arise from the speed, scope, and complexity of the technology of cyberwar apparatuses. Deeply implicated as users are in the militarization of networks, their involvement is frequently unknowing or misrecognized. We are indeed “empowered” by technology—but not necessarily in the way we are told. Rather than acting as globally aware networked individuals, intervening purposefully in great political events with a few deft touches to an iPhone, our cyberwar involvement is as likely to be a misapprehending, deceived, or involuntary conduit for war whose outbreak has either passed by unnoticed or was only imagined (at least until this imagined onset provoked real counteraction), or whose combatants are drastically misidentified. In conflicts where a crucial action may be the opening of virally contaminated email, the retweeting of a message from a software agent mistaken for a human, or the invisible contribution of a hijacked computer (or digitalized refrigerator) to a massive botnet, we are in the realm of Marx’s “they do it, but they do not know it.” “Even if you do not see the war, the war sees you” is the logic of the ~~blind~~ [unknowing] gaze of cyberwar, a regime in which although “the subject does not see where [this regime] is leading, he follows” (Lacan 1998, 75). The obscurity inherent to cyberwar afflicts even those most expert in its prosecution. During the U.S. occupation of Iraq, the CIA and Saudi Arabia’s intelligence service set up a “fake” jihadi website to monitor Islamic extremist activity. In 2008, the U.S. Army and the NSA concluded that the “fake” site was actually serving as an operational planning hub for attacks by Saudi Arabian jihadists joining the Sunni insurgency. When they proposed the site be destroyed, the CIA objected, but Pentagon hackers proceeded with the “take-down.” They inadvertently disrupted more than three hundred servers in Saudi Arabia, Germany, and Texas. As a task force participant ruefully explained, “to take down a Web site that is up in Country X, because the cyber-world knows no boundaries, you may end up taking out a server that is located in Country Y.” The Saudi Arabian intelligence service, which regarded the “fake” site as a “boon,” was furious; mollification required “a lot of bowing and scraping.” The CIA, too, was resentful; the agency “understood that intelligence would be lost, and it was; that relationships with cooperating intelligence services would be damaged, and they were; and that the terrorists would migrate to other sites, and they did” (Nakashima 2010). A more serious example of unintended consequences is Stuxnet, the computer worm planted in the computers at the uranium enrichment plant outside Natanz to prevent Iran from building a nuclear bomb, an operation now widely attributed to a joint U.S.–Israeli intelligence operation. As we noted in chapter 1, the worm’s impeccable simulation of a mechanical failure apparently unrelated to software performance is considered a watershed in the development of cyberweaponry. What it is not so generally recognized, however, is that it went out of control. Stuxnet’s discovery by the security company VirusBlokAda in mid-June 2010 was the result of the virus accidentally spreading beyond its intended target due to a programming error introduced in an update. This allowed the worm to enter into an engineer’s computer connected to the centrifuges and thence travel to the internet. It then propagated to industrial sites far from Natanz, not only in Iran but in Indonesia and India, and beyond, reportedly infecting the systems of oil giant Chevron and a Russian nuclear plant. As one cybersecurity expert puts it, “By allowing Stuxnet to spread globally, its authors committed collateral damage worldwide” (Schneier 2010). Although in many of these cases, the virus did not activate, because of differences between the Natanz system it targeted and the others it accidentally infected, another consequence was that the Stuxnet code became widely available for use or adaptation by hackers other than those who developed it. Such probably inadvertent propagation can be considered what Paul Virilio (2000) terms an “integral accident,” a malfunction intrinsic to, and inevitable for, viral cyberweapons.15 Once one passes to the civilian perception of real or imagined cyberwar effects, the scope for misrecognition increases and potentially ranges from imagining wars where none exists to not noticing those that are actually raging. Zetter (2016b) reports a “misrecognized” attack on a power grid in Ukraine that occurred on December 23, 2015, when twenty-seven substations of the Prykarpattya Oblenergo, a Ukrainian power distributor that serves 538,000 customers, went dead after the company’s computers were infected by a version of a high-powered web-based malware BlackEnergy 3, in what is generally regarded as an act of Russian aggression, although the attribution, as always, is inconclusive. The cyberevent attracted the attention of cybersecurity and hacking communities: the blogosphere and specialized online channels and platforms competed for the most informed interpretation of the blackout. In Ukraine, however, where the cyberattack took place, it was unnoticed, despite successfully plunging hundreds of cities and villages into darkness. With the exception of security, administration, and technical personnel of the power station, the local population took the blackout for a common power shutdown, a nationally centralized procedure aimed at saving electricity in the country’s declining and war-afflicted economy. In a reverse example, in August 2008, cyberattacks took place in the midst of a broader armed conflict between Russia and Georgia over the disputed territory of South Ossetia. Although these attacks, allegedly coordinated or encouraged by the Russian state, did not significantly affect the ongoing kinetic action, distribution of malicious software; defacement of political, governmental, and financial websites; and multiple DoS and DDoS attacks on governmental, financial, news, and media websites generated confusion and panic among the population of the country at a time when “Georgia was the most dependent on the availability of information channels” (Tikk, Kaska, and Vihul 2010, 69–79, 72). Then, on March 28, 2011, the internet in Georgia and Armenia went down for nearly the entire day after a seventy-five- year- old Georgian woman named Hayastan Shakarian, while digging for scrap copper, accidentally cut a fiber-optic cable owned by Georgian Railway Telecom that runs through the two countries (Millar 2011). It would not have been too strange if, to a traumatized wartime population, this accident had signaled another kinetic offensive (Deibert 2013, 29). How many times would such suspicions need to be shared and commented on in social networks to become someone’s “knowledge”? To scale and speed up to the status of “fake news”? To serve as a useful context or leverage for a future cyberattack? To premediate an invasion? The cybernetic autopoiesis of unplanned and undesired incidents, unavoidable and unpreventable accidents, as well as the masterminded and preplanned operations constitute the ongoing production of events and semblances constitutive of cyberwar dynamics. Everything, even what did not have place, did not happen, or was misattributed, has a positive value in the cyberwar economy. This trompe l’oeil creates ~~blind~~ spots in the field of vision of all observers of cyberwar.16 It accelerates what Žižek (1999, 322) calls the “decline of symbolic efficiency” in digital capitalism. As Jodi Dean (2014, 213) explains, this develops the Lacanian idea that there is no longer a Master-Signifier that stabilizes meaning, that knits together the chain of signifiers and hinders their tendencies to float off into indeterminacy. While the absence of such a master might seem to produce a situation of complete openness and freedom—no authority is telling the subject what to do, what to desire, how to structure its choices—Žižek argues that in fact the result is unbearable, suffocating closure. A “setting of electronically mediated subjectivity [that] is one of infinite doubt and ultimate reflexifisation” intensifies “the fundamental uncertainty accompanying the impossibility of totalization” in a symbolic environment where “there is always another option, link, opinion, nuance or contingency that we haven’t taken into account” (Dean 2014, 212). Computational propaganda that aims to mystify invasions and occupations, or promote cynical disaffection from an adversary’s political system, actively weaponizes the “decline in symbolic efficiency,” but it is endemic to the whole field of cyberwar. The extreme uncertainty and opacity of cyberwar do not, however, inhibit the interpellative effects of contending cyberwar apparatuses as they summon up cybersoldiers, patriotic hackers, vigilante militias, and security-conscious digital citizens. On the contrary, the problems of verifying or disproving multiple alarms and accusations accelerates these processes and puts them into overdrive. To put this point in psychoanalytic terms, as we noted previously, commentators on Althusser have criticized the appropriation of Lacan’s theories of the subject in his account of ISAs. These critics point out that what Althusser misses in Lacan’s account is that the subject is always incomplete; it is precisely what can never be fixed by a specific subject position or identity. However, the implication of this incompletion is not that the subject remains some untouched and primordial haven of authenticity but rather that this lack drives to ever more compulsive (because unfulfillable) attempts to attain a definitive identity. Translating this into political terms, we would say that it is the inescapably incomplete, provisional, and easily falsified nature of all accounts of cyberwar that energizes the adoption of increasingly militarized, extreme, paranoid, and unshakable subject positions vis-à- vis its alleged events. For example, shortly after the outbreak of the rebellion that grew into the Syrian civil war, there was an abrupt but near-total shutdown of the Syrian internet. A common assumption, at least in the West, was that this was an attempt by the Assad regime to black out online dissent, as Mubarak had attempted in Egypt. But according to Edward Snowden, the event was caused by intrusion into the system conducted by the NSA—not intentionally, however, but by accident, in a botched hack of the Syrian state’s communication and electronic defense system (Ackerman 2014). Whereas the first attribution cast the Assad regime in the conventional role of despotic suppressor of civil rights, rightly opposed by liberal democracies, the second reversed the significance of the blackout, making it evidence of—once again—NSA cyberaggression against foreign states, and incompetent aggression at that. But those opposed to this characterization could point out that at the time Snowden made his diagnosis, he was reliant on Russia, a supporter of the Assad regime, for political asylum. The blackout of Syria’s internet connection thus also becomes an epistemological blackout about its cause, a blackout in which every initial position on the politics of Syria’s civil war could be preserved and reinforced. To provide a final example that is closer to home for many readers, as we suggested in chapter 1, there is now fairly convincing evidence that Russian intelligence agencies, whether directly or by proxy, attempted some intervention in the 2016 U.S. presidential election by way of “fake news.” It is also clear that some of the news reports claiming to substantiate or expand this claim, by claiming, for example, to detect Russian hackers in Vermont’s power grid or by broadly characterizing a sweepingly wide range of U.S. media outlets as accomplices of Russian cyberwar, are inaccurate and tendentious. The abyss of this double falsification—“ fake news” compounding “fake news”—becomes a zero-gravity free-fire zone within which contending factions within the U.S. political system trade charges of treason, producing a civil war effect possibly beyond the wildest dreams of the toilers at the dreary offices of St. Petersburg’s Internet Research Group.

#### There is no policy literacy for the containment of cyberwar that is not already subsumed in cyber nonwar. Debate’s war games are only the re-elaboration of nonwar through the communicative model of cyberwar. Rather than seeking some truth to cyber-war and planning around it, we must subvert the militarization of meaning. Only a stance that refuses to oppose cyberwar on its own terms and instead deconstructs it can interrupt the cycle of violence that it guarantees.

Rivera 20. Alex Rivera, "Baudrillard and the Viral Violence of Cyber Security" (2020). Honors College Capstone Experience/Thesis Projects. Paper 844. <https://digitalcommons.wku.edu/stu_hon_theses/844>

TOWARD AN ILLUSORY READING OF CYBER WAR If the core of global violence manifests from the accumulation of meaning, the only regress would be to abolish such a pursuit. Yet, our weapons to challenge this immense system of semiotic exchange are extremely limited since external critique, like described above, is increasingly coopted as an information commodity within the system (Pawlett, 2016: 33-34). Even the most radical intellectual theories that appear to be in diametric contradiction with the virtue of such exchange ultimately become tolerated and commodified. One can simply look at the plethora of radical critical literature books for sale on Amazon; purchasing copies of books like The Communist Manifesto “[…] not only provides profits to a tax-dodging mega-corporation, it also demonstrates (or rather, simulates) the openness, tolerance and freedoms of the consumer capitalist system” (Pawlett, 2016: 33-34). Thus, these oppositional challenges to commodification end up lauding the virtuous nature of commodification by proving a tolerance that is so complete that it can literally tolerate advocacies of its demise. Most criticism begins at the wrong place by placing their challenge in the domain of the real. For Baudrillard, an unreal system is incapable of receiving a real death and thus our strategy must be a weaponization of simulations that stage its symbolic downfall. This is why the previously mentioned principal of reversibility is of the utmost importance; even when one injects meaning that is toxic to the system’s vitality, it will be consumed and exchanged like any other piece of information that is offered. Since the power of models that completely envelope reality derives from their excess of information, the ability to know everything in advance, they are vulnerable to paradox and irreconcilable confusion. Over identification with the voracious consumption of information and the overproduction of meaning can therefore reverse its strength against itself, “[…] like a much larger opponent being thrown by the momentum of their own weight in martial arts” (Pawlett, 2016: 33-34). One can imagine, for example, a society taking the messages of Red Bull commercials far too seriously and consuming the beverage to the point of widespread intestinal dysfunction – a self-demonstrating critique of the culture of productivity. As the entire system of symbolic exchange is a mere illusion, even a small act of deceit has the potential to cause its downfall. This is not to say that we should accelerate the proliferation of grotesque images like those of Abu Ghraib, quite the opposite, such a strategy would create obscene violence and fail to stake a true virtual challenge of the system. Rather, we should view those examples as demonstrations that even what initially appears impossible or destabilizing to exchange, will indeed be exchanged. Therefore, Baudrillard’s solution is contained within the science of imaginary solutions coined as Pataphysics; “Pataphysicians fight reality […]” not by confronting it, but by “[…] creating illusion and deceit” (Strehle, 2014). To avoid the trap of succumbing to a will to truth that landed us here in the first place, we must instead be radical enough to subvert reality by playing with simulations. Despite traditional assumptions, the purpose of radical thought should not be to “[…] recognize and analyze reality, instead it must deny and contradict its hegemony. It has to create illusion and establish a power of seduction that makes one lose the path of reality” (Strehle, 2014). This is comparable to a fishing lure, which takes advantage of the hunger and curiosity of fish to lead them astray from their normal food course. Baudrillard’s playful work mimics “[…] a simulacrum in the strongest sense” by denying seemingly obvious premises and writing in a riddle-like prose (Strehle, 2014). Language and signs are useful tools that can lead the subject to read and interrogate the event from a different angle. His propositions thus construct a new reality, and if the grand simulacrum is to oppose his illusion, it would expose its own unreality in the process. Yet critically, he is not concerned with discovering truth or crafting an evidence intensive case to create these illusions. By placing premises that contradict reality, his “[…] theories are like evil ghosts: They haunt reality by staging its excluded other—no matter if this other really exists or if it has to be feigned” (Strehle, 2014). This illusion of language attempts to replace what has been muted from the war by creating a new reality, not simply describing one that is waiting in the world. It replaces the old model with a confused and unreadable one in order to end the violence of predictability. To disrupt the destructive communicative model of cyber war, we must build and weaponize radical simulations. Baudrillard coins this strategy as theoretical terrorism; it is likened to a graffiti artist who sprays their own meanings or words over the preexisting symbols on a building (Strehle, 2014). Suddenly, a new simulacrum disfigures and misguides the building’s original connotation, imposing a code that is far less discernable than the last while laying a new reality over the old. Though we cannot spell out how this would exactly look for cyber war, as doing so would defeat the purpose of radical thought, we can be sure that it involves a shift in our model of communication. What is desperately needed is some way to pervert the supposed cleanliness of this cyber war, to confuse or distort its reality to the point of collapse. Much like how Baudrillard responded to the Gulf War by completely withholding its dose of reality-effect, our antiwar stance could work over the cyber event, never opposing it on its terms. Without such a strategy, we are doomed to replicate the violence of simulations.

#### Thus, Tessa and I affirm a counter-war machine to reduce alliance commitments to NATO member states by substantially limiting the conditions under which Article 5 can be activated.

#### This is a militant deconstruction that shifts the terrain of struggle to communication and meaning itself. The counter-war machine works through slow time – reducing the velocity of cyberwar’s techno-strategic discourse to rearticulate meaning, desire, cyberspace, and collective action by opening up a space of care. Fostering corporeal care constructs an orientation that can distort the clean reality of cyberwar presupposed by the US-NATO security apparatus, constructing a radical counter power that interrupts the reality of nonwar itself.

#### Debate is a central node in the operations of the communicative model of cyberwar, making it key space for this intervention. If both war and nonwar are mobilized through the extraction of cognitive and material labor that primes workers, students, and faculty for participation in cyberwar, then transforming how we calculate risk, value, and meaning is the only ethical option.

Matviyenko et al. 19 (Svitlana Matviyenko, Assistant Professor of Critical Media Analysis in the School of Communication of Simon Fraser University in Vancouver. Nick Dyer-Witheford, associate professor in the Faculty of Information and Media Studies at University of Western Ontario. “What is to be done?,” *Cyberwar and Revolution, Digital Subterfuge in Global Capitalism,* University of Minnesota Press,Mar 12, 2019) \*modified for ableist language

However, we would suggest that to conduct “cyberwar on cyberwar,” though it may sometimes be necessary, is to fight on unfavorable terrain. We have seen that hacktivism suffers problems of accountability, transparency, provocation; can itself be compromised and ensnared within the exploits of the military– ­internet complex; and is ultimately highly vulnerable to the police and intelligence apparatus. And, as Noys (2013) observes, even reliance on the speed with which networks can circulate struggles tends to discount how much more advantage such velocity today gives capital’s military– ­security complexes (in this respect, we note that the huge, worldwide, and digitally mobilized protests against the Iraq War in 2003 must be reckoned a tragic failure of networked activism). Cyberwar on cyberwar is a method of fast politics, and speed is where the user-subjects ultimately lose, encountering the inhuman acceleration of machinic processing power. To succeed, such resistance requires a break from the mainstream paradigm of today’s “platform capitalism” with all its repetitious “Twitter revolutions,” “Facebook revolutions,” or “Snapchat revolutions,” slogans that should remind us that, as Lacan once notoriously noted, an ultimate misconception of revolution is as a desire for a new master or a master in a new form that leads away from the systemic change rather than not toward it. Here we disagree with the conclusion of Brian Massumi’s (2015, 243) otherwise excellent study of the new “ontopowers” of military networking, where, discussing the logic of speed and preemption, he suggests that countermovements have no choice but to “go forward, with the flow.” While tactical resistance can involve any and all of the “memes of production” (Deterritorial Support Group 2012), a reconstitution of the left today must ask, what is the opposite of cyberwar? To this, we would answer that the antithesis of cyberwar is corporeal care of the subject achieved through the “balanced conceptions of space and time within culture” and “awareness of spatial and temporal dynamics [that] keep state and market power in check (Sharma 2013, 314). It is from this perspective that we need to recognize cyberwar’s production of time and space and envision different times and spaces— those of the care of bodies. This orientation against the social destruction, physical, psychological, and infrastructural, of cyberwar does not mean totally abandoning the digital— which, because it so much composes the very texture of everyday life, would be not only difficult but often politically fatal. But it does mean its rearticulation to a set of purposes radically different from those of digital capital. In particular, this strategy requires theoretical reconsideration and practical subversion of the addicted, complicit digital user, the figure envisioned by neoliberal Silicon Valley, by way of desynchronization and emancipation. This can be described as recognizing a position in and against the military environment of cyberwar in which all of us are now imbricated and finding ways to develop subjectivities that are simultaneously of the network and off the network. It requires the “slow” time necessary for the in-­ person (rather than online) organization of antiwar collectives, movements, and alliances; defection from compulsive social media use; trammeling corporate capacities to intensify and maintain such addictive behavior; the patient defense and reconstruction of the basic public institutions of corporeal care— ­free health services; the cultivation of mental health; the recovery and deepening of the legacy of a semidestroyed (or, in many places, never created) welfare state in a new “commonfare”; universal education provisions; worker–community control of workplaces and the means of production; ecological protections— ­and the assertion of such priorities against the expense and logic of networked militarization. In this work of solidarity, the subject exploited and excommunicated by digital capitalism can transition from alienation toward reciprocity. And to those who say that the accelerated logic of cyberwar means we don’t have time to do all this before catastrophe arrives, we just say, you may be right, but still we have to do it anyway! We can build a “counterwar machine” constructed on the diagonal line that runs between waging cyberwar on cyberwar and fostering the caring corporeality that is opposite of cyberwar. At the end of her study of world labor activism, Beverly Silver (2003, 176) notes a major reason for the shortage of militant working-­class movements in the early twenty-­ first century. Neoliberalism’s restructuring, globalization, and financialization, with its “growing structural unemployment, escalating inequalities and major disruptions,” has repeated the crisis patterns of previous eras of capitalism, with one crucial exception. The missing condition is large-­ scale armed conflict. This “global political– m ­ ilitary context contrasts sharply with . . . that [which] produced radicalized and explosive labour unrest in the first half of the twentieth century.” As Silver notes, war then involved the mass mobilization of populations that characterized total war. States depended on their working classes to provide not just millions of soldiers but labor in munition plants, shipyards and aircraft factories, hospitals, and farms. When mass mobilization met the horror of mass deaths and mutilation, revolutionary social turmoil could result. As Silver (2003, 175) observes, advanced capitalism’s turn to high technological weaponry apparently breaks this link between war and worker revolt. Cyberwar can be seen as an extension of this “automation of war.” Nonetheless, as we have suggested, the tendency of digital militarization to liquidate the labor of war is not yet completely fulfilled. Humans remain as the indispensable conscious links and relays within the networks and nodes of digital conflict. Indeed, what we have seen in this book is the surprisingly wide diffusion of participation in cyberwarfare, from the highly specialized military and intelligence units at the cutting edge of advanced cyberoperations to strata of mercenary and criminal proxies, online vigilantes, patriotic hackers, corporate and criminal marketers of cyberweaponry, cybersecurity personnel, and on to the corporate content moderators and state censors and surveillance agents now indispensable to the prosecution of war waged in cyberspace and across scores of hybrid battlefields. To these more or less intentional contributions to the mechanisms of cyberwar must be added the unknowing (or partially unknowing) participation of network users, whose online activities and addictions provide the vital vectors for the memes, exploits, and hijackings of subterranean cyberconflicts and whose reconstitution as data­subjects habituated to ceaseless state and commercial surveillance constitutes the inevitable accompaniment to such operations. Surveying this field, we can say that military mobilization has not so much been abolished from cyberwar as reconfigured in subterranean, etiolated, and unfamiliar forms. This decomposition of the labor of war, equivalent to Virilio’s state of “endocolonization” by the apparatus of high-­ technology militarism, may, as we have proposed in this chapter, contain potentials for reversal. If, to date, cyberwar is not, at least in the centers of capitalism, producing the massive havoc of earlier forms of war, the migrant refugees of hybrid conflicts around the world, fleeing algorithmically directed drones, social media– ­activated death squads, and cybernetic strikes at social utilities, bear witness to its potential to do so. Already, even in ostensibly secure zones of the planet, the costs of militarized and criminalized networks, in terms of escalating social paranoias, crumbling confidence in everyday communication and polarizing social relations, becomes daily more apparent. If this course persists, unforeseen forms of unrest by the new workforces of cyberwar may interrupt its inhuman trajectory. As both of us are academics, we are concerned with how the neoliberal university is occupied today by cyberwar. Responding to the exhortations of states and corporations for a supply of labor power adequate to cyberwar conditions, institutions of postsecondary education are proliferating cybersecurity programs (Talley 2013; Ritchie 2016; Wilson 2017). They are also the target of intensifying cyberattacks, some aimed at military-­related research (Ismail 2017; Young and Bennett 2017). But, most immediately from our point of view, the university has become a place where students receive mutually contradictory messages from faculty teaching critical theory about the risks of state and corporate surveillance and the public relations teams hired by higher administrators that encourage them to “like” the university’s profile on Facebook, follow it on Twitter, and become full participants in a regime of corporate promotion and self-­ branding. Not only does this jeopardize pedagogical work (except when one manages to use such instances as case studies for politicoeconomic analysis in class, which is admittedly rare) but it is also unethical given the general awareness (including by higher administrators and public relations teams) that youths are being aggressively targeted by corporate platforms. This targeting does not just leave young people feeling stressed, defeated, overwhelmed, anxious, nervous, stupid, silly, useless, and like a failure. It also prepares them as the unthinking data-subject cannon fodder for wars already being waged with computational propaganda, botnets, and the viral relay of virtual weaponry with real material consequence. We and our students are subjects of the “capitalist unconscious,” “the alienated subject at work in every discursive action” (Tomši č 2015, 54). Lacan traced the notion of the subject to the beginning of modern science, which initiated the emancipation of the human from theocratic social orders, replacing a ritualistic relation to the world of nature. Unfortunately, as Samo Tomši č argues, “the emancipatory political potential of scientific revolution” was captured and “neutralized” by a counterrevolutionary capitalism that “needs to be thought of as the restoration of pre-­modernity within modernity” (235). This neutralization he characterizes as the construction of “a closed world, marked by totality, finitude and centralization”—­the world market, mobilizing atomized, narcissistic, and competitive individuals in never-­ending and all-­subsuming commodity exchange, a world whose purported eternity and completion negate the perception of “contingency, infinity and instability” that is the true core of scientific emancipation. Pointing to a parallelism between Marx and Lacan, Tomši č observes that capitalist modernity “ceases at the critical point of the subject” (235­ ). He explains, While capitalism considers the subject to be nothing more than a narcissistic animal, Marxism and psychoanalysis reveal that the subject of revolutionary politics is an alienated animal, which, in its most intimate interior, includes its other. This inclusion is the main feature of a non-­ narcissistic love and consequently of a social link that is not rooted in self-­ love. (233­ ) The atavistic “pre-­ modernity within modernity” of capitalism, and the disaster of its capture of advanced science, is nowhere more clearly demonstrated today than by its tendencies toward cyberwar. As the young Althusser (1946, 14) wrote in the midst of the “apocalyptic panic” following the explosion of the first atomic weapons, “the world in which humanity trembles before what it has itself wrought is an extravagant image of the proletarian condition, in which the worker is enslaved by his own labour: it is quite simply, the same world.”