Between the "Battlefield" Metaphor and Promises of Generativity: Contrasting Discourses on Cyberconflict

Artur de Matos Alves
CECL – Universidade Nova de Lisboa /
DAHCS – McGill University

ABSTRACT *This article proposes a theoretical assessment of discourses on cyberconflict, and of their relation to the current perception of the state of cyberspace. By contrasting the "battlefield" approaches to cyberconflict with theoretical and factual materials on its social and political impacts, this article suggests that the "battlefield" terminology frames the discussion of online security within a drive for the "militarization" of cyberspace. It concludes by presenting generativity-based perspectives as a contribution towards addressing contemporary challenges to network politics in cyberconflict theoretical frameworks.*

KEYWORDS *Electronic culture; New media; Internet/IP/WWW; Cyberconflict; Network politics*

RÉSUMÉ *Cet article propose une évaluation théorique des discours sur le cyberconflit, et de leur rapport à la perception actuelle de l'état du cyberespace. En opposant des approches du type «champ de bataille» au cyberconflit avec des matériaux théoriques et factuelles sur ces impacts sociaux et politiques, ce document suggère que la terminologie «champ de bataille» encadre le débat sur la sécurité en ligne dans la militarisation de l'espace cybernétique. L'article conclu en présentant des perspectives fondées sur la « générativité » comme contributions pour relever les défis contemporains aux politiques des réseaux dans les cadres théoriques du cyberconflit.*

MOTS CLÉS *Culture eléctronique; Nouveaux médias; Internet/IP/WWW; Cyberconflit; politique des réseaux*

Introduction

Conflicts of varying intensity in cyberspace are now receiving generalized attention and demanding new appraisals of the changing conditions of the online world. The rise of cybercrime, the development of cyberweapons, political activism, and widespread online surveillance also signal a changing online ecology. After several decades of expansion, digital communication networks are now facing a restructuring based on the ideas of control and stable "boundaries."

Artur de Matos Alves is Research Collaborator of CECL-Universidade Nova de Lisboa and Visiting Scholar in the Department of Art History and Communication Studies, McGill University. Email: arturjmalves@gmail.com .

Canadian Journal of Communication Vol 40 (2015) 389–405

This stage of development is characterised by the colonization of cyberspace by state and non-state actors seeking to strengthen control of information and infrastructures, in what can be read both as an attempt to limit online freedom and an effort to strengthen network security. An image of the Internet as a battlefield is hence replacing the utopia of networked computer-mediated communication in discourses of online security, giving form to new policy approaches. Proponents characterize cyberspace as increasingly chaotic, threatening, and in need of securitization. These discourses, though divided in their approach of the "battlefield metaphor," equate online communication networks with a field of military-like strife.

This article proposes a critical theoretical assessment of discourses on cyberconflict, and of their relation to the current perception of threats to, or emerging from, cyberspace. In offering a critique of the "battlefield metaphor," the aim is to show how it narrows the discussion on online security issues, by contrasting it with approaches focused on social and political impacts of cyberconflict. The use of a "battlefield" approach frames the discussion of online security around a drive towards securitization and militarization of cyberspace, exacerbating some of the risks and threats, while dismissing the negative impacts of increased control and surveillance in online trust, freedom, and creativity.

Cyberconflict: Background and definitions

This section presents some concepts and definitions of cyberconflict and related phenomena. The subsequent sections develop these concepts into a contrasting analysis of some of the possibilities of theoretical approaches framing current discussions on cyberconflict. In order to preserve a distinction between their original intellectual traditions, this article adopts "cyberconflict" as a more general term than "cyber warfare," the latter being a high-intensity form of computer-mediated conflict. "Cyberspace" is loosely defined as a socio-technological sphere supported by a global infrastructure of digital communication wherein informational exchange takes place.

Numerous reports from governments, civil organizations, military, security firms and media have highlighted a rise in frequency of damaging cyber-attacks (Anderson & Rainie, 2014; Cornish, Livingstone, Clemente & Yorke, 2010; Marinos & Sfafianakis, 2013; Reporters Without Borders, 2012; 2013; 2014). These attacks range from relatively unsophisticated website defacements to targeted attacks with more harmful (potentially physical) effects. Between these two examples it is possible to identify a continuum of actions, supported by individuals, groups of people, governments, or even thousands of personal computers under external control (botnets). Some of the actions fall in legal grey (as in the case of hacktivist practices) or dark areas (such as cybercriminal activities). Other actions concern the ability of citizens and activists to overcome informational and organizational barriers, such as in online forums, instant messaging via mobile phone or computer, social network services, among many other services.

Any conflict can be defined as "a situation in which actors use conflict action against each other to attain incompatible goals and/or to express their hostility" (Bartos & Wehr, 2002, p. 28). Conflict actions, in this sense, are the behavioural expression that may be placed along a scale of coerciveness; that is, between partial agreement and complete disagreement. Rational dissent is one of the ways to establish alternative positions in order to seek a new balance, and the exercise of high coerciveness appears as a non-rational alternative that can be at odds with both sides' interests (Bartos & Wehr, 2002).

Cyberconflict can be defined as "conflict in computer-mediated environments (cyberspace)," in particular when effects spill over from the "real world" (Karatzogianni, 2006, p. 94). In other words, cyberconflict consists of the spread of conflict behaviour, especially politically motivated action, in the digital realm. The motivations for action can be played out in the political sphere by multiple kinds of actors, including social movements, religious or ethnic groups, or political parties. Similarly, concrete action may take many forms, ranging from advocacy to awareness-raising actions, in the case of cyber activism (Vegh, 2003).

Thus, "cyberconflict" can be taken as an umbrella term referring to phenomena placed along a continuum of conflict behaviour taking place via digital communication. That continuum ranges from dissenting views in an online discussion to more complex and high-intensity cyberwars. There are at least two dominant perspectives on cyberconflict that share this view of the networked sphere as a conflict space. There are, however, important divergences between these two approaches regarding how to conceptualize the diversity and seriousness of phenomena of online conflict, as well as regarding policy stances to adopt in their management.

The first of the perspectives, analytical in nature, echoes military and international affairs studies of developments in the cybersphere and places emphasis on threats to, and conflict among, states. The rationales of policybuilding, strategic planning, and countermeasures development are represented by authors such as Arquilla and Ronfeldt (1999; 2001), Libicki (2009), and Carr (2009). These authors prioritize the need to protect ICT infrastructure, online services, and retaliation options. This group is committed to the current international efforts for implementing concerted action and international cooperation regarding cyberconflict, usually framed in the institutional settings of international agreements and the military.

The second perspective focuses on civil society and open social discourse and stems from a critical tradition. This type of approach is indebted to critical and media theories, and rooted in the works of Foucault (1979), Deleuze and Guattari (1987), as well as Hardt and Negri (2004). It focuses on the study of online debates and arguments, as well as political and activist practices (online protest, hacktivism, among others). It stresses the importance of the transition of political conflict and activism into cyberspace, as illustrated by social movements and their use of digital tools (Karatzogianni, 2008; Karatzogianni & Robinson, 2010). With respect to policy, this perspective underlines the importance of participation and the democratization of political processes in the fulfilment of the potential for social progress of online conflict in discursive arenas.

Digital networks as battlefields

The analytical tradition, which will be the subject of this section, is more concerned with the construction of a theory of war in cyberspace. One key idea is that cyberspace, just as geographical space, has its own salient points, and needs to be protected, both at the infrastructure and at the informational levels. Given that contemporary society relies on ICT, it becomes a priority to understand how vulnerabilities can be corrected or, conversely, exploited. It is in this sense that digital networks became a "battlefield" for military intervention. This section concerns the adoption of the "battlefield metaphor" as military doctrine for cyberspace during the early 1990s. It shows how the conceptualization of cyberwarfare is linked to the promotion of a new military domain in cyberspace and the corresponding doctrinal body framed by the comparison to a field of battle.

Military doctrine and the use of cyberspace

"Cyber warfare" (CW) denotes a particular case of cyberconflict, which takes the shape of a state-level war in cyberspace, thus falling within the military realm. In this case, actors seek political and military advantage by trying to disable the enemy's infrastructure (informational and other) via cyberspace. The transformation in attitudes and discourses towards cyberspace policy stems from the perception of the need for stronger, more sophisticated defences against cyber-attacks, particularly with the integration of battle systems in encompassing potentially vulnerable digital networks.

For some authors, CW is waged via strictly informational means. Drawing upon a conceptualization of power as the ability to force the will of another actor, Carr (2009) states that CW consists of the governments' attempts to "force their wills against their adversaries and find victory without bloodshed in the cyber domain" (p. 2). For this author, cyber warfare is confined to the informational space and cannot be conceived as causing physical harm. However, other authors do not exclude the use of conventional weaponry with real-world effects and casualties. Clarke and Knake (2010) consider cyber war the fifth domain of warfare, consisting of actions that aim to disrupt computer networks, thereby damaging a nation's infrastructure. With this in mind, the authors argue that there must be an extension of the virtual battlefield to all aspects of online activity, and not just military targets.

This extension is due to the fact that network-centric military technology can be seen as both an advantage (gathering and sorting information is crucial in wartime, as are its interpretation and adequate use in the battlefield) and a vulnerability. Command, control, communications, computers and intelligence (C4I)[1] systems depend on a network of satellites, antennae, cable networks, digital devices, unmanned aerial vehicles, surveillance technology, and networked soldiers and weapons. Since the 1990s, militaries are fully aware of the strategic and tactical advantages of crippling the enemy's use of cyberspace, or of using superiority in that field to achieve dominance in other areas (for example, destroying the informational infrastructure that underpins the enemy's military command). The U.S. Cyber Command was created in 2010 to approach cyberspace as the fifth military domain; that is, as a new field in which to wage war and exert military power (Singer & Friedman, 2014).

Cyber warfare refers to the exploitation of ICT for military purposes, with the introduction of high-intensity conflict into cyberspace. The efforts of nation-states and their militaries to bring doctrines and materials in line with twenty-first century technological and political trends have transformed warfare into a matter of control or use of flows of information and communication. Along with this, a new discourse about online security has been created, which argues for a further militarization of cyberspace, embodied in a competition for cyberweapons and countermeasures.

The expansion of the "battlefield metaphor" to encompass communication network activity seems to convert it into a potential target for the exertion of force or subterfuge. The effect is amplified if the countries have in place a modern network and rely on e-government structures. For example, attacks on government websites and databases can cause confusion and bring the state bureaucracy to a stop. Furthermore, the ability of the military themselves to wage even a conventional war has become increasingly dependent upon a lattice of networked elements.

Networks as battlefields: The militarization of cyberspace

Concerns over nation-wide cyber security have been heightened in the first decade of this century by news on cyberconflict that arguably contributed to exacerbating the perception of threat. Examples include the cyber-attacks on Estonia in 2007 (Landler & Markoff, 2007) and during the war in Georgia in 2008 (Danchev, 2008), several "bursts" at the end of 2009, as well as more recent news about breaches in corporate and state information systems. In the wake of these attacks, the United States announced a new policy for cyberspace (Clinton, 2010) that included the protection of the commercial Internet and civilian digital infrastructure in its security concerns (Markoff, 2010).

For Taddeo (2012a), any military intervention in cyberspace should be limited to the preservation of the "well-being" of cyberspace itself, with care to ensure that no further or greater disruption is introduced into cyberspace. Cavelty (2012) believes that militarizing cyberspace in order to prevent misuse of the networks (both military and civilian) is "based on fear" and ultimately "pointless," in part because a large portion of power in cyberspace is in the hands of private actors (p. 151). The 2013 revelations by NSA private contractor whistleblower Edward Snowden have shown that intelligence agencies' approaches to cyber security have, in fact, taken into account this factor, engaging private sector companies in their operations.

The creation of cyber weapons—i.e., computer code written with the specific purpose of destroying or sabotaging military targets by taking control of targeted systems—is conceived as a form of military attack. One of the risks in using malicious code as a weapon is its replication and reverse engineering, which may allow its use or adaptation by other actors, originating new variants targeting similar control systems (Zetter, 2011a).[2] The most well-known cyber weapon to date is the Stuxnet worm, developed by the United States and Israel with the specific purpose of impairing or delaying Iran's uranium enrichment operations, thus crippling its nuclear program by disabling parts of its infrastructure (Sanger, 2012; Singer & Friedman, 2014).

In spite of the concerns about a possible cyberwar, the most active sources of insecurity in cyberspace remain closer to the everyday realities of online fraud and espionage. The relative success of online malicious criminal action and electronic espionage (via malware and spyware, for example) triggered a generalized concern with the vulnerabilities of online systems. "Cloud" services, online gaming companies, financial institutions, e-commerce and government websites are favourite targets for criminal hackers, as they usually integrate personal, financial, and other important data. In addition, successful attacks yield large amounts of confidential information, along with wreaking havoc on the owners' security and undermining trust.[3]

Cyber security firms and international agencies keep a record of threats and trends of attacks, and find the online environment is fraught with malicious code of criminal origin.[4] The European Network and Information Security Agency (ENISA) tracks sixteen types of threats, among which only email spam is under control (Marinos & Sfafianakis, 2013). This report illustrates a security problem for individuals, businesses and governments, but also the development of an "arms race" between cybercriminals and the cybersecurity sector. Mass-targeted attacks rely on simple methods, some of which can be found on sale online, making them more prevalent (Greenberg, 2012a; 2012b). However, high profile "targeted attacks" and "advanced persistent threats"[5] contribute disproportionately to the cyber security narrative and remain the overwhelming concern of governments and companies in their policies for cyberspace (Lawson, 2013).

In 2011, a green paper of the U.S. Department of Commerce acknowledged the trust problem and identified the political need to address specific challenges, namely "[e]nhancing Internet privacy; Improving cybersecurity; Protecting intellectual property; and Ensuring the global free flow of information" (Department of Commerce Internet Policy Task Force, 2011, p. iv). This follows a policy document of the Obama administration, "The Comprehensive National Cybersecurity Initiative" (The White House and National Security Council, 2011), which built on an earlier assessment of nation-wide cybersecurity, published as "The Cyberspace Policy Review" (The White House, 2009).

In this context, new strategies appear to take over the network "battlefield." Cyber security policies regulate technological infrastructure. A higher degree of control of the core technological mechanisms of the Internet, such as IP addresses and DNS standards, is being put in place around the world (Deibert, Palfrey, Rohozinski & Zittrain, 2008; 2010; DeNardis, 2012). During the Arab Spring, Internet kill-switches and other devices put in place as security measures were used to shut down access in Egypt and Libya. In June 2013, NSA whistleblower Edward Snowden brought new information to light that confirmed concerns about online freedom. Snowden exposed a number of covert programs that showed the extent to which online communication is being monitored and analyzed by intelligence agencies as part of a program by the United States and its allies to achieve a maximum of control of global digital communication (Greenwald, 2014). In short, the socio-technological system of cyberspace is undergoing a military turn, underpinned by the hyperbolization of systemic threats, and calling for top-down approaches to network governance.

"Netwars": Between cyberwar and online conflicts

The pattern of belligerence, which foreshadows the idea of the network as battlefield, was criticised by Arquilla and Ronfelt (2001). In *Networks and Netwars*, the authors suggested a much more nuanced view of cyberconflict as a discussion of information warfare under circumstances of global, rhizomatic cyberconflict, outside the military sphere. They suggested the term "netwar" as "a parallel concept about information-age conflict at the less military, low-intensity, more social end of the spectrum" (p. 2). Their focus was on the digitally networked organization and coordination of activity in the civilian world, potentially used for criminal, terrorist or radical action, and was not yet addressed as a serious concern by governments. The "war" in "netwar" identifies an area of intervention and a new model of managing conflict, including a rethinking of the concept of global communication.

Arquilla and Ronfelt's (2001) definition of "netwar" highlights the central aspects of a "spill-over effect" from the physical to the online world, as well as the consequences of a different model of organization for non-military engagements. "Netwar" refers to "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the actors use network forms of organization and related doctrines, strategies, and technologies attuned to the information age" (p. 6). For the authors, the transition to digital communication enabled a subversive turn by being within reach of an unprecedented number of people. The decentralized, networked methods available for "netwar" offer a greater array of options for groups seeking non-conventional ways of organization and action. "Netwar actors" (Arquilla & Ronfeldt, 2001) use the resilience and interoperability of digital networks to continuously reconfigure their social networks, but also to attack, gather data, spread propaganda and disinformation, or recruit (Karatzogianni, 2006).

The definition of "netwar" excludes cyber warfare, consigning it to the military realm. It emphasises the juxtaposition of multiple social networks, and not just Internet-related phenomena.[6] The organizational aspects of this new form of conflict are brought to the core of the concept. In the sense that the central matter for the study of cyberconflict lies in the transition to ICT-based platforms in organization and action, the actors might be recognizable (terrorist groups, identity thieves, smugglers), new, mutated forms of old actors (so-called copyright pirates, black marketeers), or groups acquiring more sophisticated forms of organization (such as transnational activists or hackers), as Arquilla and Ronfeldt argue (2001).

The decentralized, leaderless, and digitally networked aspects of the organization of netwar prefigure a critical turn in the conceptualization of online conflict. By moving away from a pure "battlefield" analysis towards a socially informed analysis, Arquilla and Ronfeld (2001) introduced some aspects of a more critical view of cyberconflict. The key features, as will be seen below, are a strong reliance on decentralized organization and a high degree of dematerialization of conflict, heralded by generalized connectivity.

Critical approaches to cyberconflict

The concept of netwar anticipates a socio-political turn in theories of cyberconflict, one that underlines the importance of the decentralization of economic and political power in the new networked environment. Initially, freedom of information, along with the fluid construction of communication bonds, and the potential for new economic opportunities, gave rise to optimistic perspectives heralding a new utopia of networked communication (Castells, 2004; 2009; Toffler, 1989; 1991). In accordance with their democratic potential, communication technologies would enable new forms of work and knowledge, but also new forms of political action, social dialogue, and protest.

This section is devoted to the contextualization of cyberconflict by a critical tradition concerned with the intersection of social phenomena with the online world. Instead of underlining high-intensity belligerence as a major factor for policy, this set of authors addresses the conditions in which antagonistic positions are deployed in cyberspace.

The critical perspective to be explored in this section mobilizes social and media theory to address the changes in power structures, social relations, and organizational aspects. For example, the concern with digital rights (data protection, freedom of expression, freedom of information, privacy, among others) evokes issues such as censorship and surveillance, thereby translating into the digital realm global political matters. The rhizomatic character of online cultures—its distributed, decentralized, fluctuating and de-territorialized aspects (Deleuze & Guattari, 1987)—is essential to understanding the global drive for regulating communication flows in cyberspace. The rise of global virtual publics and of network politics signal demands for representation and transparency at the international level, including the debates about online freedom (Hardt & Negri, 2004). In pointing out the risks of disciplinary power converted into surveillance and control (including social control via globalized media), this perspective is also indebted to Foucault's (1979) work.

The multifaceted nature of cyber attacks can be ascribed to the networked logic of global economic and political power, which makes every major player in the global arena subject to highly visible cyber damage. As mentioned, politically motivated attacks try to achieve maximum media impact with spectacular operations that disrupt their targets' operations (the oil company Saudi Aramco was one such target in 2012).[7] With low opportunity costs and few barriers to entry, indifferent to national frontiers and conflict frontlines, cyber-attacks seem to be a very attractive option for actors to achieve notoriety or profit, and to spread uncertainty.

Soft strategies of managed cyber-conflict may also be linked to the emergence of a "noopolitik"; that is, the constitution of a global communication sphere. The idea of noopolitik addresses five trends of the end of the twentieth century: global interconnection, the emergence of a global civil society, soft power, the cooperative advantages rising from the changes in ICT, and the "formation of a global noosphere" (Arquilla & Ronfeldt, 1999, p. 35).[8] In brief, "[t]he noosphere concept thus encompasses cyberspace and the infosphere and has its own technological, organizational, and ideational levels. It relates to … the rise of network forms of organization that strengthen civil-society actors" (Arquilla & Ronfeldt, 1999, p. 14). The noosphere may be considered a multilayered network of norms, objects, ideas and human beings (Latour, 1993); that is, a sociotechnical system enabling generative agency (Abbate, 2012).

The noosphere supports a decentralized, networked form of politics that relies less on face-to-face sociability and more on looser forms of engaged civility, often taking the form of deliberation on global causes. At this point, Athina Karatzogianni's (2006) distinction between socio-political and ethno-religious cyberconflict countenances a broader view of the possibilities of computer-mediated conflict. The former consists on the use of "the internet as an organizational and mobilizational resource, attempting to reframe issues and take advantage of the openings of the political opportunity structures" (p. 121). Ethnoreligious cyberconflicts are "real-world conflicts with ethnoreligious characteristics which spill over into cyberspace," in which "the groups involved use the internet, not as a resource with which to reframe the issues, but rather as a weapon" (p. 154). By acknowledging the socio-political potential of the cyber sphere, the soft power conceptualization of cyber power suggested by noopolitik is in line with the decentralization and de-territorialization mentioned above. The manifestations of social conflict depend to a large degree on the preservation of a pluralistic and open environment in cyberspace.

Network politics and the promotion of generativity

The normative constraining of an open Internet culture produces changes in the online articulation of power, communication, and sociability. This section will address those changes, taking into account how analytical and critical perspectives deal with the balance between openness and security. The Internet and the networked environments it sustains—businesses, entertainment, news, social networking services, political fora—entered diplomacy and the political spotlight as a new "battlefield," where heterogeneous political groups vie for control (Deibert et al. 2008; 2010; Mueller, 2004; 2010).

The expression "network politics" refers to the discursive political nexus between technological, military, social and moral issues, or to ICT-mediated political action. It can be seen as a form of technological politics for contemporary ICT; that is, as a "system of order and governance" (Winner, 1978, p. 237). The Internet can be thought of as a sociotechnical system where knowledge and communication flows are grounded on a technical disposition of technological mechanisms (such as the TCP/IP protocol), conditioned by organizational and normative decisions (Fuchs, 2005). In turn, these decisions depend on the interaction of the multiple actors in policy arenas and their ability to exert influence in the process. Traditionally, network technologies were invested with emancipatory attributes. The idea of "independence of cyberspace" (Barlow, 1996) dominated political and social discourse towards digital communication, despite heavy criticism of its techno-utopian character (Barney, 2006; Morozov, 2011; Winner, 2005).

Network politics can also be seen as shifting towards levels of control that affect discursive practices by reframing digital rights (Deibert, 2003). Network standards and mechanisms of regulatory control are also nodes of political and economic strife. This became especially noticeable after 9/11 and the U.S.A.'s Patriot Act, when communication networks emerged as vital areas to be regulated and securitized in order to detect, isolate, and eliminate terrorist threats. Additionally, the concentration of mass communication companies during the last two decades has placed enormous power in the hands of multinational companies, which, for access and content providers, may amount to a "closing" akin to the one undergone by traditional information systems, heralding a definitive change in the political nature of the Internet (Wu, 2012). Another critical moment in this shift towards direct intervention in network politics was Hillary Clinton's (then U.S. Secretary of State) "Remarks on Internet Freedom" speech (2010). In that speech, the optimistic view of the democratizing effects of information technologies was defined as foreign policy doctrine, signalling a willingness to intervene to support computer-mediated efforts for democratic change.

Some of the regulatory changes in network standards and protocols take place at the international level, in institutional arenas such as the ICANN (International Corporation for Assigned Names and Numbers) and the ITU (International Telecommunications Unit), which regulate the changes in protocols and standards. This project to reframe some technical and normative aspects of the Internet is surrounded by protest. Network activists interpret the renewed pressures for stricter controls as attempts to impose restrictions on online freedoms and the values of Internet publics (Massit-Folléa, 2012). Legislation and agreements, such as SOPA (Stop Online Piracy Act), ACTA (Anti-Counterfeiting Trade Agreement) or PIPA (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act), have been subjected to close scrutiny by network activists. Although ostensibly promoted in order to detect digital piracy, illegal file sharing, and cyber terrorism, these regulations are criticised for establishing frameworks that restrict measures put in place to preserve the anonymity of the data traffic of individual Internet users.

The arguments for the protection of network liberties invoke the advantages of maintaining an open cyberspace. The idea of "generative systems" (Zittrain, 2009) is useful to understand this concept of a dynamic environment in the sense that "they are never fully complete, that they have many uses yet to be conceived of, and that the public can be trusted to invent and share good uses" (p. 43). This notion is consistent with the sociotechnological character of cyberspace—a hybrid, non-deterministic agency system affected by the creative practice of the actors involved (Abbate, 2012).

Generative systems support creative practices and give network politics its particular connected outlook. The networked structures of the digital world present a diverse environment for expression and exchange of ideas—discursive practices ranging from political discussion and meme-building, to flaming in online newspaper comment sections. The Internet allows low-mediation participation in transnational causes, affecting mobilization and communication by creating an alternative to institutional channels. However, it may be constrained by access barriers or restrictive network policies (such as online censorship, filtering, or blocking). The political and economic uses of the digital tools are multiple and constantly changing. Hackers and hacktivists, in particular, represent the nexus between computer-mediated protest, digital rights activism, and cyberspace-centric organization (Coleman & Golub, 2008; Denning, 2001; Taylor, 1999). In sum, generativity creates an ecosystem that expands with little control and a high degree of freedom. This openness explains the difficulty in achieving a systemic balance between security and transparency in technology. Since technological phenomena are socially constructed and not closed systems, they are vulnerable to shifts in the priorities of institutional arrangements.

In contrast, non-generative systems value orderly and controlled environments with a greater degree of restriction as to what can be coded and enunciated. Closed systems are those that trade flexibility for security, establishing gateways and walls of various types. Establishing barriers between or within systems not only means that communities gather inside (and outside), but also that constant surveillance and exclusion are needed to maintain the integrity of the systems. Closed proprietary systems, with their valuable databases and prominent security features, are a prime target for hackers. They are perceived as violating the generative and open principles of the Internet—not least because of sophisticated security measures and obscure privacy policies—thereby justifying both financially and ideologically motivated attacks.

Towards a critique of the "battlefield" metaphor

This last section links the discourses on cyberconflict to the "battlefield metaphor." It concludes by suggesting that arguments for the preservation of generativity in the online world are not compatible with the dominance of a military rhetorical field. Technical and strategic arguments in favour of tighter control of cyberspace have the potential to obfuscate the political dimensions of cyberconflict, supporting the creation of online security mechanisms with limiting and coercive effects, particularly in non-democratic political regimes. They may, in other words, promote non-generative socio-technological arrangements. They also present the online world as a territory in need of walls and surveillance, lacking global democratic supervision, where safety concerns overrule openness.

It must be added that the definition of the cyber domain as a space of military domination is far from unanimous. Taddeo (2012b) avoids isolating CW in the cyber sphere by characterizing cyberwarfare as "waged within the informational environment, with agents and targets ranging both on the physical and non-physical domain and whose level of violence may vary upon circumstances" (p. 114). This definition places CW on a continuum of intensity and across domains. It neither implies an innocuous (non-destructive) form of war, nor precludes the use of further means to deny CW capabilities to the enemies, but remains compatible with multiple non-violent forms of conflict behaviour. Rid (2012) questions the CW category itself as an inadequate construct precisely because it interprets warfare too loosely. For Rid, "all past and present political cyber-attacks are merely sophisticated versions of three activities that are as old as warfare itself: subversion, espionage, and sabotage" (p. 6). Rid argued that recent incidents did not fulfil Klausewitz criteria for "war"—violence, instrumentality and political attribution, and therefore it remains to be seen whether any war can be waged with "code as the main weapon" (p. 29).

Current doctrine states that defensive mechanisms are fragile and prone to vulnerabilities that may be discovered and exploited, while offensive measures have an "asymmetrical advantage" that is difficult to overcome (Liles, Rogers, Dietz & Larson, 2012). The assessments of the resulting changes to Internet regulation and standards made by international bodies point out that furthering the tracking of criminal, terrorist and dissenting activities by extending controls to all information exchanges may, in the medium term, also affect online public discourse (Dutton, Dopatka, Hills, Law, & Nash, 2010; Mendel, Puddephatt, Wagner, Hawtin, & Torres, 2012). This idea is consistent with critical studies of cyberconflict, which perceive the securitization of cyberspace as a concentration of power that affects the property structure and regulatory control of the Internet, thereby affecting online freedoms. This claim denies that the securitization of cyberspace can accomplish the goals of eliminating cybercrime, denying cyberwarfare capabilities to state and non-state actors. In fact, the most evident effect of enforcing controls over servers, Internet service providers and Internet traffic in general, is the generalization of surveillance, and not a more secure online environment for citizens.

Most cyber-attacks are criminal in nature. Online criminal activity has more immediate effects on the lives of citizens, and more damaging consequences, which delegitimize approaches to cyberconflict as a strictly military construct representing the online world as a battlefield. A 2011 OECD study stated that cyberwar doctrines use hyperbolic terminology and that a purely military approach has limited usefulness in the protection of individual citizens against more probable risks (Sommer & Brown, 2011). In fact, by 2010, cyber security was becoming a top concern in the lists of perceived public threats, along with terrorism, as a British poll revealed (AFP, 2010).

Spaces of debate and social networking services like Twitter, Facebook or YouTube, among many others, are territories of symbolic strife, of conflict. Some of their characteristics are borrowed from previous forms of online sociability, like multi-user dungeons (MUDs and MOOs), or online forums, and are carried over to those means of synchronous and asynchronous communication. Online activists arguing for an open Internet object to the commodification, concentration and regulatory efforts on the grounds of their negative effects on generativity. Unwarranted walling or securitization not only present challenges to online activism in all societies, but also to the generativity of the Internet as an inclusive, global communication network.

The decisive shift in approaches to cyberconflict has led actors to intensify the exploitation of digital networks, albeit with the explicit goal of securing them. Institutions and governments implement security measures, despite indications that most breaches can be attributed to human error, lack of awareness of online threats, and over-reliance on ICT (Singel, 2010). This reasoning, akin to doctrines of physical warfare, prioritizes the acquisition of cyber capabilities, on the one hand, and the surveillance of conflict in cyberspace, on the other, while the promotion of online security literacy is overlooked. The regulation of cyberspace thus acquires new meaning, both as a drive for better control of infrastructure on the part of national and international entities, and as a form of implementing surveillance programs that target online dissenters as well as cybercriminals. Noopolitics, as we have seen, calls for the adoption of a soft approach to cyberconflict, more attuned to what may be called the post-modern, decentralized international system of cyberspace.

Conclusion

This article aimed to show that the "battlefield metaphor" approach to online security and the future of online digital communication may contribute to narrow the perception of cyberconflict and its nuances. If cyberconflict is to be understood as a multiplicity of behaviours and actions, ranging from dialogue to the coercive, an excessive focus on one of the ends of the spectrum is detrimental to that pluralism. Both the analytical and the critical points of view acknowledge the role of computer-mediated conflict in an age of digital communication, incorporating views on the purposes, actors, and institutions active in cyberconflict scenarios. However, the analytical approach can be contrasted by relying on a more negative perspective of conflict, informed by the stringencies of a "battlefield" metaphor.

By adopting this "battlefield" view, some of the recent regulating interventions in digital networks face several pitfalls, contributing to reduced democratic, economic, and sociocultural generativity. Firstly, their adopters are prone to obfuscate the root causes of conflicts that democratic societies need to address, thereby placing limits on the circulation of opposing views being played out in public spheres. Secondly, cybercrime remains a risk for everyday uses of digital devices, even as the emphasis is placed on the protection against extreme scenarios of cyberwar and cyberterrorism. Lastly, by militarizing and securitizing digital networks, they compromise established mechanisms of trust, tightening surveillance and control at the expense of privacy, anonymity, and net neutrality.

The critical and analytical discourses are at odds with each other regarding the degree to which the political economy of the Internet should be changed. This matter does not seem to be amenable to a simplistic dichotomy of open *versus* closed digital networks, of discursive conflict versus cyberwar. The main risks for individuals (and social movements) pertain to data security breaches of trust and privacy, where human error represents the weakest link. In this sense, the promotion of digital literacy and of security standards for consumer services merits as much attention as the creation of national and regional network security mechanisms. The preservation of the openness of digital networks, both for its economic potential and for its communicational affordances, does not rest solely on establishing security mechanisms. In fact, one of the greatest challenges on the horizon for policymakers and online activists is the promotion of online freedoms in an age of generalized surveillance.

Notes

[1] There are several other versions of the acronym (C3I, C4ISR), all referring to the ability to integrate military forces and the data they produce or require in a seamless communications network.

[2] "DuQu" was a computer worm that exploited a vulnerability in the Windows operating system. It was discovered in October 2011 (Symantec, 2012) and was thought to be related with Stuxnet (discovered in 2010), possibly as a non-destructive information-gathering tool (Zetter, 2011b). In February 2012, another form of malware known as "Mahdi" was discovered infecting computers in the Middle East. Although it has not been attributed to any particular organization, it is thought to be a cyber-espionage tool capable of extracting information from infected systems (Zetter, 2012). "Flame" was discovered in the Middle East in May 2012. It exploited the same security weak points in operating systems as Stuxnet.

[3] Several examples illustrate the consequences and costs. In April 2011, Sony's Playstation network was taken offline and user information (name, address, e-mail, birthday, login information and password) was stolen. At the time, Sony advised its customers to be aware of phishing and scam attacks (Kuchera, 2011a; 2011b). In December 2011, security firm Stratfor was attacked and user information was stolen (Friedman, 2012). Events such as the Arab Spring revolutions, the Japanese earthquake, Steve Jobs' and Amy Winehouse's deaths, and the 9/11 anniversary were used as opportunities for scamming, phishing, and spreading spam in 2011 (Symantec, 2012). Attacks on certificate authorities have also disrupted the digital world by undermining trust. Targets included Comodo, DigiNotar, GlobalSign and Digicert. The attack on the Dutch company DigiNotar in June 2011 exploited the breach of encryption keys to create false certificates. The loss of trust in its security certificates bankrupted the company by September 2011 (Symantec, 2012).

4. According to the security firm Symantec, in 2011, more than 5 billion malware attacks were blocked (up from 3 billion in 2010), with 5,989 new vulnerabilities and 403 million unique malware variants discovered, up from 286 million new variants in 2010 (Symantec, 2012).

5. "Targeted attacks use customized malware and refined targeted social engineering to gain unauthorized access to sensitive information … . Typically, criminals use targeted attacks to steal valuable information such as customer data for financial gain. Advanced persistent threats use targeted attacks as part of a longer-term campaign of espionage, typically targeting high value information or systems in government and industry." (Symantec, 2012, p. 14)

6. The "small world" effect in networks, along with their decentralized character and (almost) scale-free structure are among the main changes to power relations. On the other hand, distributed decentralized networks, like the Internet, are also prone to power law effects and hierarchization. This means that, on the Internet, 1) not all nodes in the network are equally important to its functioning (acting as "hubs"), and 2) adequate action can prioritize and target hubs according to the distribution of weights in the network and/or preferential connection, thereby bringing to the fore a strategic aspect of the topology of networked cyberspace.

7. An attack on August 15, 2012, infected "about 30,000 computers" (Saudi Aramco, 2012, p. 2) with malware and forced the company to take its website offline, although it did not confirm the full extent of the damage. A group calling itself "Cutting Sword of Justice" took credit for the occurrence (Fisher, 2012).

8. The idea of "noosphere" is attributed to Teilhard de Chardin and Vladimir Vernadsky. For de Chardin, the transformation of human cognition and consciousness is accelerated by technological progress and the complexification of social relations, eventually achieving a degree of awareness known as the "Omega Point," the culmination of macro-evolution towards higher forms of consciousness, aided by new, more sophisticated technological forms (de Chardin, 1964; 2003).

References

Abbate, Janet. (2012). L'histoire de l'Internet au prisme des STS. *Le Temps des medias, 18*(1), 170–180.

AFP. (2010). Terror, cyber warfare "biggest threats" in Britain. *Google News*. URL: http://www.google.com/hostednews/afp/article/ALeqM5gdyrkgPz6yAwLdCrZHqzjQSBjeRw?docId=CNG.aec298041bd87d0d6ae2ef88e13bcbcd.7e1 [March 10, 2013].

Anderson, Janna, & Rainie, Lee. (2014). *Net threats. Digital life in 2025*. Pew Research Center. URL: http://www.pewinternet.org/2014/07/03/net-threats/ [October 29, 2014].

Arquilla, John, & Ronfeldt, David F. (1999). *The emergence of noopolitik: Toward an American information strategy*. Santa Monica, CA: Rand Corporation.

Arquilla, John, & Ronfeldt, David F. (2001). *Networks and netwars: The future of terror, crime, and militancy* (2nd edition). Santa Monica, CA: Rand Corporation.

Barlow, John Perry. (1996). *A Declaration of the independence of cyberspace*. URL: https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration [March 10, 2013].

Barney, Darin. (2006). The morning after: Citizen engagement in technological society. *Techné: Research in Philosophy and Technology, 9*(3), 23–31.

Bartos, Otomar J., & Wehr, Paul. (2002). *Using conflict theory*. Cambridge, UK: Cambridge University Press.

Carr, Jeffrey. (2009). *Inside cyber warfare: Mapping the cyber underworld*. Sebastopol, CA: O'Reilly Media.

Castells, Manuel. (2004). *The power of identity*. Oxford, UK: Wiley-Blackwell.

Castells, Manuel. (2009). *Communication power*. Oxford, UK: Oxford University Press.

Cavelty, Myriam D. (2012). "The Militarisation of Cyberspace: Why Less May Be Better." In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict (CYCON)* (pp. 141–153). Talinn, Estonia: NATO CCD COE Publications.

Clarke, Richard A., & Knake, Robert. (2010). *Cyber war: The next threat to national security and what to do about it*. New York, NY: Harper Collins.

Clinton, Hillary Rodham. (2010). Remarks on Internet freedom. *U.S. Department of State - Diplomacy in Action*. URL: http://www.state.gov/secretary/rm/2010/01/135519.htm [March 10, 2013].

Coleman, E. Gabriella, & Golub, Alex. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory, 8*(3), 255–277.

Cornish, Paul, Livingstone, David, Clemente, Dave, & Yorke, Claire. (2010). *On cyber warfare: A Chatham House report*. London, UK: Chatham House.

Danchev, Dancho. (2008). Coordinated Russia vs Georgia cyber attack in progress. *ZDNet*. URL: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670 [March 10, 2013].

de Chardin, Pierre Teilhard de. (1964). *The future of man*. New York, NY: Harper & Row.

de Chardin, Pierre Teilhard de. (2003). *The human phenomenon*. Brighton, UK: Sussex Academic Press.

Deibert, Ronald J. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium-Journal of International Studies, 32*(3), 501–530.

Deibert, Ronald J., Palfrey, John G., Rohozinski, Rafal, & Zittrain, Jonathan. (Eds.). (2008). *Access denied: The practice and policy of global Internet filtering*. Cambridge, MA: The MIT Press.

Deibert, Ronald J., Palfrey, John G., Rohozinski, Rafal, & Zittrain, Jonathan. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: The MIT Press.

Deleuze, Gilles, & Guattari, Felix. (1987). *A thousand plateaus: Capitalism and schizophrenia*. Minneapolis, MN: University of Minnesota Press.

DeNardis, Laura. (2012). Hidden levers of Internet control: An Infrastructure-based theory of Internet governance. *Information Communication and Society, 15*(5), 720–38.

Denning, Dorothy E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In J. Arquilla & D.F. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Santa Monica, CA: Rand Corporation.

Dutton, William, Dopatka, Anna, Hills, Michael, Law, Ginette, & Nash, Victoria. (2010). *Freedom of connection-freedom of expression: The changing legal and regulatory ecology shaping the Internet*. Paris, France: UNESCO. URL: http://unesdoc.unesco.org/images/0019/001915/191594e.pdf [March 10, 2013].

Fisher, Dennis. (2012). Saudi Aramco confirms scope of malware attack. *Threatpost.com*. URL: http://threatpost.com/en_us/blogs/saudi-aramco-confirms-scope-malware-attack-082712 [March 10, 2013].

Foucault, Michel. (1979). *Discipline and punish*. London, UK: Prentice-Hall.

Friedman, George. (2012). The hack on Stratfor. URL: http://www.stratfor.com/weekly/hack-stratfor [March 10, 2013].

Fuchs, Christian. (2005). The Internet as a self-organizing socio-technological system. *Cybernetics & Human Knowing, 12*(3), 37–81.

Greenberg, Andy. (2012a). Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees). *Forbes*. URL: http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ [March 10, 2013].

Greenberg, Andy. (2012b). Shopping for zero-days: A price list for hackers' secret software exploits. *Forbes*. URL: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/ [March 10, 2013].

Greenwald, Glenn. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Metropolitan Books/Henry Holt.

Hardt, Michael, & Negri, Antonio. (2004). *Multitude: War and democracy in the age of empire*. New York, NY: The Penguin Press.

Karatzogianni, Athina. (2006). *The politics of cyberconflict*. London, UK: Routledge.

Karatzogianni, Athina (Ed.). (2008). *Cyber-conflict and global politics*. London, UK: Routledge.

Karatzogianni, Athina, & Robinson, Andrew. (2010). *Power, resistance and conflict in the contemporary world: Social movements, networks and hierarchies*. London, UK: Routledge.

Kuchera, Ben. (2011a). PSN down due to "external intrusion," no news on fix, credit card security. *Ars Technica*. URL: http://arstechnica.com/gaming/news/2011/04/playstation-network-still-down-due-to-external-intrusion.ars [March 10, 2013].

Kuchera, Ben. (2011b). Sony admits utter PSN failure: Your personal data has been stolen. *Ars Technica*. URL: http://arstechnica.com/gaming/news/2011/04/sony-admits-utter-psn-failure-your-personal-data-has-been-stolen.ars [March 10, 2013].

Landler, Mark, & Markoff, John. (2007, May 29). Digital fears emerge after data siege in Estonia. *The New York Times*. URL: http://www.nytimes.com/2007/05/29/technology/29estonia.html [March 10, 2013].

Latour, Bruno. (1993). *We have never been modern*. Cambridge, MA: Harvard University Press.

Lawson, Sean. (2013). Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics, 10*(1), 86–103.

Libicki, Martin C. (2009). C*yberdeterrence and cyberwar*. Santa Monica/Arlington/Pittsburgh: Rand Corporation.

Liles, Samuel, Rogers, Marcus, Dietz, J. Eric, & Larson, Dean. (2012). Applying traditional military principles to cyber warfare. In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *2012 4th International Conference on Cyber Conflict (CYCON)* (pp. 169–180). Talinn, Estonia: NATO CCD COE Publications.

Marinos, Louis, & Sfafianakis, Andreas. (2013). *ENISA threat landscape – Responding to the evolving threat environment*. Heraklion, Greece: European Network and Information Security Agency. URL: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape [March 10, 2013].

Markoff, John. (2010, February 5). Google asks spy agency for help with inquiry into cyberattacks. *The New York Times*. http://www.nytimes.com/2010/02/05/science/05google.html [March 10, 2013].

Massit-Folléa, Françoise. (2012). La gouvernance de l'Internet. Une internationalisation inachevée. *Le Temps des medias, 18*(1), 29–40.

Mendel, Toby, Puddephatt, Andrew, Wagner, Ben, Hawtin, Dixie, & Torres, Natalia. (2012). *Global survey on Internet privacy and freedom of expression*. UNESCO series on Internet freedom. Paris, France: UNESCO. URL: http://www.unesco.org/ulis/cgi-bin/ulis.pl?catno=218273 [March 10, 2013].

Morozov, Evgeny. (2011). *The net delusion: The dark side of internet freedom*. Philadelphia, PA: PublicAffairs.

Mueller, Milton. (2004). *Ruling the root: Internet governance and the taming of cyberspace*. Cambridge, MA: The MIT Press.

Mueller, Milton. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: The MIT Press.

Reporters Without Borders. (2012). *Internet enemies report 2012*. URL: http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf [November 13, 2012].

Reporters Without Borders. (2013). *Enemies of the internet 2013 report – Special edition: Surveillance*. URL: http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf [April 4, 2013].

Reporters Without Borders. (2014). *Enemies of the internet 2014 report*. URL: http://12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf [May 13, 2014].

Rid, Thomas. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.

Sanger, David E. (2012, June 1). Obama ordered wave of cyberattacks against Iran. *The New York Times*, sec. World/Middle East. URL: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [March 12, 2013].

Saudi Aramco. (2012). *Saudi Aramco restores network services*. URL: http://www.saudiaramco.com/en/home.html#news%257C%252Fen%252Fhome%252Fnews%252Flatest-news%252F2012%252Fsaudi-aramco-restores-network.baseajax.html [March 14, 2013].

Singel, Ryan. (2010). Cyberwar hype intended to destroy the open Internet. *Threat level*. URL: http://www.wired.com/threatlevel/2010/03/cyber-war-hype/ [March 12, 2013].

Singer, Peter W., & Friedman, Allan. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford, UK: Oxford University Press.

Sommer, Peter, & Brown, Ian. (2011). *Reducing systemic cybersecurity risk*. Report number: IFP/WKP/FGS(2011)3. Future Global Shocks. London, UK: OECD/IFP.

Symantec. (2012). *Internet security threat report – 2011 trends*. URL: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf [March 12, 2013].

Taddeo, Mariarosaria. (2012a). An analysis for a just cyber warfare. *Cyber Conflict (CYCON), 2012 4th International Conference on Cyber Conflict*, June 5–8, 2012. Conference proceedings (pp. 1–10). Tallinn, Estonia.

Taddeo, Mariarosaria. (2012b). Information warfare: A philosophical perspective. *Philosophy & Technology, 25*(1), 105–120.

Taylor, Paul. (1999). *Hackers: Crime in the digital sublime*. London, UK: Routledge.

The Department of Commerce Internet Policy Task Force. (2011). Cybersecurity, innovation and the Internet economy. *U.S. Department of Commerce*. URL: http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf [March 12, 2013].

The White House. (2009). *Cyberspace policy review: Assuring a trusted and resilient information and communications infrastructure*. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [March 12, 2013].

The White House & National Security Council. (2011). *The comprehensive national cybersecurity initiative*. URL: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative [March 12, 2013].

Toffler, Alvin. (1989). *The third wave*. New York, NY: Bantam Books.

Toffler, Alvin. (1991). *Powershift: Knowledge, wealth, and power at the edge of the 21st century*. New York, NY: Bantam Books.

Vegh, Sandor. (2003). Classifying forms of online activism. The case of cyberprotests against the World Bank. In M. McCaughey & M.D. Ayers (Eds.), *Cyberactivism: Online activism in theory and practice* (pp. 71–95). New York, NY: Routledge.

Winner, Langdon. (1978). *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, MA: The MIT Press.

Winner, Langdon. (2005). Technological euphoria and contemporary citizenship. *Techné: Journal of the Society for Philosophy and Technology, 9*(1), 124–134.

Wu, Tim. (2012). *The master switch: The rise and fall of information empires*. New York, NY: Alfred A. Knopf.

Zetter, Kim. (2011a). DHS fears a modified Stuxnet could attack U.S. infrastructure. *Threat Level*. URL: http://www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks/ [March 12, 2013].

Zetter, Kim. (2011b). Son of Stuxnet found in the wild on systems in Europe. *Threat Level*. URL: http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/ [March 12, 2013].

Zetter, Kim. (2012). Mahdi, the Messiah, found infecting systems in Iran, Israel. *Threat Level*. URL: http://www.wired.com/threatlevel/2012/07/mahdi/ [March 12, 2013].

Zittrain, Jonathan. (2009). *The future of the Internet: And how to stop it*. London, UK: Penguin Books Limited.