Convergence Security: Cyber-Surveillance and the Biopolitical Production of Security

Sean Lawson
Department of Communication
University of Utah

Robert W. Gehl
Department of Communication
University of Utah

"We are also undergoing a phenomenon known as 'convergence'...This phenomenon means that the same networks and devices are processing a full range of data and support a full range of applications, from banking to social networking, from supply chain management to patient health records. This convergence adds much convenience, but it poses new security challenges across a swath of our government and economy."

~General James R. Clapper, Director of National Intelligence
(House Permanent Select Committee on Intelligence 2011, 27)

"I will argue here against the idea that convergence should be understood primarily as a technological process... Instead, convergence represents a cultural shift [...] Convergence occurs within the brains of individual consumers and through their social interactions with others."

~Henry Jenkins (Jenkins 2006, 3)

"The general public is often wholly unaware of how much of what we commonly call 'security' depends on the work of informal groups and volunteer networks."

~Alexander Klimburg (Klimburg 2009, 199)

Introduction

Since the end of the Cold War, several observers have noted the "widening" of the notion of security in Western nations (Buzan et. al 1998; Hardt & Negri 2004). In the face of a seemingly ever-expanding list of potential threats and vulnerabilities, the boundaries between internal and external security blur, the functions of military, law enforcement, and intelligence organizations overlap, and almost every aspect of daily life is subject to securitization (Bigo 2002). As the potential subjects and objects of threats to security have proliferated, so too have the potential arenas of conflict. Cyberspace has emerged as one of those arenas. It is not only a tool, terrain, and target of conflict for state actors, but also for non-state actors working on behalf of the state or for their own ends, thus illustrating the blurring of the boundary between traditional producers and "consumers" of security.

In this paper, we examine cases of self-organized, online volunteers in the United States that are devoted to countering what Deibert and Rohozinski (2010b) have identified as threats through or to cyberspace. These groups monitor and counter terrorist activities on the Internet, investigate and prevent cyberattacks, or patrol U.S. borders from the vantage point of cyberspace. Drawing from Hardt and Negri's description of the "global state of war," as well as the work of media studies scholars who have described the emergence of "convergence culture" and the "prosumer" as central to the "new economy," our paper posits the emergence of "convergence security." Just as new media technologies have been at the heart of the blurring boundaries between traditional producers and consumers of media products, so too are they at the heart of the blurring

boundaries between the traditional producers and consumers of security. Cyber-surveillance has emerged as a key avenue for citizen participation in the regime of seemingly ubiquitous surveillance that is at the heart of the production of security in Western societies. In the cases examined here, we see the emergence of an often uneasy relationship between the traditional and new producers of security that is fraught with ambivalence, ambiguity, and danger.

From the Global State of War to Convergence Security

Michael Hardt and Antonio Negri (2004, 6-7) have noted that war in the modern state system "was a limited state of exception" conducted between states with sovereign political authority, not by individuals or non-sovereign groups, However, the current state of affairs is one in which "the exception has become the rule" with the lines between war and peace, warrior and noncombatant, becoming increasingly blurry. The result is what they describe as a perpetual, indeterminate, interminable, and global state of war.

While the emergence of this global state of war was in evidence prior to the attacks of September 11, 2001 (Hardt & Negri 2004, 4), the "global war on terrorism" (GWOT) that resulted from those attacks has become the quintessential example of the phenomenon that they describe. The GWOT is a war against "abstract concepts," "sets of practices," and "indefinite, immaterial enemies" that "serve[s] to mobilize all social forces" in response to threats for which "there is little difference between outside and inside, between foreign conflicts and homeland security" (Hardt & Negri 2004, 14). One result has been a shift in focus from defense to security in Western nations. This involves a shift from emphasizing the defense of the political and territorial sovereignty of the state from external threats to emphasizing the need to secure all aspects of social, political, economic, and cultural life in the face of proliferating risks, vulnerabilities, and threats that transcend traditional boundaries. "This notion of security is a form of biopower, then, in the sense that it is charged with the task of producing and transforming social life at its most general and global level" (20).

Security-as-biopower works at all levels of society and results in a state of conflict that suffuses all of society, that is "indeterminate, both spatially and temporally," and which allows for the possibility that "all of humanity can in principle be united against an abstract concept or practice such as terrorism" (Hardt & Negri 2004, 14-15, 19). As war invades the normal functioning of everyday life, even mundane activities like washing one's hands or having up-to-date antivirus on one's computer become acts of "national security." In short, when war permeates all of society, which must be secured in its entirely on every possible front, then everyone is a potential "warrior."

Biopower, which Hardt and Negri (2004) see as "above society, transcendent, as a sovereign authority [that] imposes its order," is contrasted with "biopolitical production" (94). Biopolitical production is a networked, collaborative form of production based in openness, free flows of information, and sharing of common resources that is at the heart of the new economy (337). They point to the Internet-enabled labor of the open-source software movement as a prime example of biopolitical production. Biopolitical production, they argue, "tends itself to become political decision-making" and "makes democracy possible for the first time today" by "banish[ing] sovereignty [and biopower with it] from politics" (339-340).

They also point to "post-Fordist," networked guerrilla movements like the Zapatistas as examples of biopolitical production (Hardt & Negri 2004, 81), which implies that practices of biopolitical production can be found in practices of conflict. But they only identify biopolitical practices of conflict among those groups that are resisting Western, neoliberal globalization and existing forms of politics based in sovereignty and war. They limit the work of security-as-biopower to the state. But the cases of convergence security examined below are examples of biopolitical production in service to state interests, or even the outsourcing of biopower to private actors.

To explore our cases, we will draw on convergence theory as developed in media studies. Henry Jenkins' theory of "convergence" is central to contemporary efforts to understand the production of media and entertainment content often identified as the "immaterial goods" most exemplary of the new economy and its collaborative, information and communication technology (ICT) enabled practices of biopolitical production. Convergence is about technological, organizational, and cultural changes (Jenkins 2006, 2-3). It involves producers and consumers both adapting to technological changes, which results in changes in and among traditional producer organizations, as well as changes in the relationship between traditional producers and consumers. Jenkins has predicted that while "we are [now] mostly using this collective power through our recreational life...soon we will be deploying those skills for more 'serious' purposes" like political and military affairs (4).

Convergence can already be seen in military affairs and the production of security. The effects of convergence within and among traditional producers of security can be seen in efforts to "transform" both the U.S. military via the adoption of "network-centric warfare" and the U.S. intelligence community via increased reliance upon open source information and collaborative work processes (Andrus 2007; Cebrowski & Garstka 1998; Lawson forthcoming; Steele 2001). Self-organizing, online volunteer groups like the ones examined below are examples of the changing relationships between producers and consumers of security. As with Jenkins' "convergence culture" or Toffler's "prosumer," we do not see the elimination or complete domination of one group by the other, but neither do we see the emergence of a space of completely open and equal participation (Bruns 2009; Jenkins 2006, 3). Instead, we see both top-down and bottom-up change that often leads to ambivalent, ambiguous, and sometimes contentious relationships among producers and consumers, with producers at once recognizing that they must rely upon the labor of consumers while simultaneously seeking to maintain control and consumers laboring out of a combination of passion, fear, patriotism, and frustration with producers, but nonetheless dependent upon the producers for the security that they ultimately seek (Jenkins 2006, 17-18, 20).

Countering Threats through Cyberspace

In the United States, surveillance has been at the heart of changes in traditional defense, as well as attempts to counter so-called "asymmetric" security threats. Guided by the principle that "what can be seen can be hit," battlefield surveillance was at the heart of the U.S. "revolution in military affairs" during the 1970s, 1980s, and 1990s (Tomes 2007). Two asymmetric threats in particular have caught the imaginations of those within the United States who have worked

consistently to increase government surveillance capabilities: the threats of terrorism and cyberattack (Harris 2010).

The idea that information-age conflict in general, and the fight against terrorism in particular, constitute a global "battle for hearts and minds" has been popular among U.S. defense and security professionals for at least a decade (Arquilla & Ronfeldt 1996, 1999). Various observers have worried about terrorist use of the Internet as a tool for fundraising, organizing, recruiting, and propaganda (Conway 2006; Lia 2005; Thomas 2003; Weimann 2005). It is in this spirit that Arquilla has urged the U.S. government to remove terrorist websites from the Internet (Arquilla 2009). Likewise, it is in this spirit that groups of self-organized, online volunteers engage in various types of online activities in support of the U.S. "war on terrorism," including intelligence gathering and counter-propaganda activities.

The work of Shannen Rossmiller and her group Phoenix Global Information Systems (formerly known as 7-Seas Global Intelligence) is the most notable example of intelligence-focused, volunteer cyber-counterterrorism. In response to the terrorist attacks of September 11, 2001, Rossmiller, a municipal judge from a small town in Montana, began trolling jihadist websites to learn more about those who had attacked the United States and what they might be planning next. In January 2003, Rossmiller joined forces with at least six other individuals whom she met in the online discussion forum, www.itshappening.com. They created a website and began calling themselves 7-Seas Global Intelligence. Members of 7-Seas live in the United States, Canada, Australia, and Singapore and include an economist, a physicist, a computer systems engineer, a corporate security consultant, and a private investigator (Mitchell 2004; Moore 2004; Roesler 2004).

Rossmiller and members of 7-Seas have used a number of techniques to gather intelligence about terrorists online. These have included creating multiple false personas complete with pictures and detailed life histories. To appear as convincing as possible to her targets, Rossmiller has learned Arabic, studied the Quran, and read Arabic literature. They also employ translation software, tools to map the IP addresses of the online jihadists with whom they interact, software to mask their own IP addresses and make it appear that they are located in the Middle East or South Asia, and even spyware that is remotely installed on the computers of some of those that they investigate (Carter 2004; Lubrano 2007; Moore 2004; Roesler 2004; Rossmiller 2007; States News Service 2009).

While their initial goal was to predict future terrorist attacks, they soon shifted to gathering and analyzing information from terrorist websites, forums, and chat rooms, and then turning that information over to authorities (Carter 2004; Moore 2004). Rossmiller's efforts in particular have contributed to two high-profile arrests of would-be terrorists, including the 2004 case of Specialist Ryan Anderson, a Washington state National Guardsman who attempted to sell classified information about vulnerabilities of U.S. weapons systems to an al-Qa'ida member that he met online. That al-Qa'ida member was actually Rossmiller. Anderson is now in prison serving five consecutive life sentences, the harshest penalty yet dealt to an American in the war on terrorism (Rossmiller 2007). In another case, and again posing online as a member of al-Qa'ida, Rossmiller uncovered a plot by Pennsylvania resident and al-Qa'ida sympathizer, Michael Reynolds, to blow up several gas pipelines and oil refineries in the United States. Reynolds was convicted and is now serving fifty seven years in prison (Seper 2007). Rossmiller

is reported to have provided information to U.S. law enforcement or intelligence in as many as 240 other cases (Lubrano 2009), leading to the detention of dozens of suspects worldwide (Harden 2006) and even some arrests and deportations of terrorism suspects from the United States (Rossmiller 2007).

For all the success that Rossmiller and 7-Seas has had, there remains a great deal of ambivalence, ambiguity, and tension in their relationship with authorities. On the one hand, the volunteers are motivated in part by calls by authorities to be vigilant (Carter 2004; Rubinkam 2007). They believe authorities' claims about the seriousness of the threat of terrorism and want to help. One the other hand, they are also motivated by feelings that the government is either unable or unwilling to counter extremists' use of the Internet (Harden 2006; Lubrano 2009; Mitchell 2004; Rubinkam 2007). Similarly, while Rossmiller has received a great deal of praise and assistance from authorities--the FBI has compensated her for her expenses (Rubinkam 2007), provided her with Arabic translation services (Harden 2006), and provided her with security (Rubinkam 2007), a former Secretary of Commerce has said that she deserves a medal (Dempsey 2007), she has been consulted by the Defense Intelligence Agency (Contreras 2009), and she has been an invited speaker at an FBI cybersecurity conference (Lubrano 2009)—these agencies have also sometimes expressed concern or doubt about her work and the work of others like her (Carter 2004; Mitchell 2004; Roesler 2004). For her part, Rossmiller has at times complained that her work is being undervalued by authorities (Contreras 2009; Lubrano 2009) and has been clear to assert her independence from the state (Harden 2006; Lubrano 2007b).

But for all the tensions between authorities and volunteers, and for all that Rossmiller and 7-Seas have tried to distance themselves from the authorities, they nonetheless seek both approval and profit from the authorities. Both 7-Seas and later Phoenix Global Intelligence Systems have sought government contracts and intelligence and security consulting work for government clients (Carter 2004). In 2009, Rossmiller announced at an FBI-sponsored cybersecurity conference that she had formed a company and was seeking a partnership with a defense contractor to offer cyber-intelligence training and services to the government. She has been encouraged to do so by former CIA Director, James Woolsey (Lubrano 2009; States News Service 2009).

In the end, there are real reasons for tension and for concern. Both sides are right. The authorities likely cannot monitor and analyze that much Web content, making the work of the volunteers indispensable. However, the volunteers do not have the ability to physically arrest suspects or materially disrupt terrorist planning or operations in any significant way, making the capabilities of the state indispensable in achieving their goals. Additionally, there are clear difficulties in making the relationship work. Sometimes authorities and volunteers can work at cross purposes. If authorities rely too much on volunteers, or if the role of volunteers becomes formally institutionalized, then their main value can be compromised (Carter 2004). Finally, Michael Reynolds' defense strategy—i.e. claiming that he too was just trying to catch terrorists online like Rossmiller—also points to some of the potential difficulties in this new relationship between producers and consumers of security online (Lubrano 2007c).

Countering Threats to Cyberspace

Other groups have worked to counter threats to cyberspace. This includes efforts to investigate and analyze cyberattack incidents such as denial of service attacks and targeted use of malware.

Founded in August 2008 by former intelligence analyst Jeffrey Carr, Project Grey Goose was an experiment in online, volunteer, open source intelligence (OSINT) aimed at investigating possible Russian government involvement in the large-scale cyberattacks that hit the country of Georgia during the Russian military invasion earlier that month. On August 22, 2008, Carr used his blog to announce the project and to put out a call for volunteers. The final cadre of twelve that was listed in the group's October 2008 report was comprised primarily of current and former members of the intelligence community, academic researchers, and defense and security professionals (Project Grey Goose 2008). Contributors to a second Grey Goose report released in early 2009 largely fit the same demographic profile (Grey Logic 2009).

The group has described their OSINT methodology as relying on "data mining" and "machine translation" of "foreign language forums and social media sites," technical analysis of "server-level data," "an examination of geopolitical events occurring around the time of the cyber attacks," and "a review of the [suspected] Nation State's military doctrine related to Information Warfare." They believe that the open source (i.e. non-classified) nature of their work is a distinct advantage, allowing them to work more quickly and with greater participation from international volunteers (Grey Logic 2009).

The two Grey Goose reports have had a substantial impact on shaping perceptions of Russia's involvement in the 2008 Georgia cyberattacks, as well as shaping public debate about the threat of cyberwar. Members and supporters of Project Grey Goose even believe that data that they turned over to authorities may have prevented some cyberattacks, as well caused the Kremlin "to reduce its support of various [hacker] groups" (Grey Logic 2009; Klimburg 2009, 200). Jeffrey Carr has become a sought-after expert on issues of cyberwar, resulting in his publication of the book *Inside Cyber Warfare* for O'Reilly Media in 2009 (Carr 2009). Carr's book is now on the Commander's recommended reading list for members of U.S. Strategic Command, the parent organization of the newly-formed U.S. Cyber Command.[1]

Once again, the case of Project Grey Goose indicates the ambivalence and ambiguities that often exist between producers and consumers of security. Like Rossmiller and others, Carr has argued that bureaucratic inefficiencies often prevent government from effectively countering "terrorism in cyberspace" (Carr 2007, 2008). One of those limitations, he argues, is that state actors do not yet understand the power of either the Internet, open sources of information, or collaborative processes of knowledge production (Carr 2008). Thus, governments have proven ill-equipped for countering terrorists online or meeting the challenge of cyberattacks (Carr 2009, xiii). He sees Project Grey Goose as exemplary of the value of applying the open source software development model to intelligence work and hopes that "it will prove that we do not have to wait for official channels to adopt innovative solutions" (Carr 2008).

Carr and his supporters identify Project Grey Goose as an example of what they call a "security trust network" (STN). Michael Sinkowitch, an executive at Fujitsu Australia who specializes in

[1]See http://www.stratcom.mil/reading_list/ (accessed 30 March 2011).

national security and intelligence, has defined STNs as "expert affiliations of interested organisations and individuals that can investigate and mitigate cybercrime threats" (Standing Committee on Communications 2009, p. 48). Alexander Klimburg, a fellow at the Austrian Institute for International Affairs and a contributor to Carr's 2009 book, defines them as the liberal, democratic, Western antithesis to Russian and Chinese "patriotic hackers." Where "patriotic hackers" are seen as beholden to or controlled by the state and composed of malicious actors with a dubious moral code, STNs are defined as free to "choose when and if" to support a government, as trustworthy and credible partners for government, and as "shar[ing] a common moral code" based in "doing the right thing" and "(generally) operating within the remits of the law" (Klimburg 2009, 200-201).

Carr, Sinkowitsch, and Klimburg all see STNs like Project Grey Goose as examples of the security-producing "informal groups and volunteer networks" that Klimburg speaks about in the epigraph to this paper. In the realm of cybersecurity in particular, Klimburg has claimed that most work is already being done by STNs and business with "government bringing up the rear" (Klimburg 2009, 199). He has claimed that STNs are particularly good at addressing the "attribution problem" in cybersecurity—i.e. figuring out the origin of a cyberattack, which is "a notoriously difficult task" (Klimburg 2009, 200). Sinkowitsch has gone so far as to claim that cybersecurity STNs are able to "defeat, or at the very least limit the damage of, these adversaries [i.e. cyberattackers of various sorts]" (Standing Committee on Communications 2009, 48).

But like the other cases of convergence security examined here, STNs too are ultimately dependent upon their relationship to the state. Even Sinkowitsch admits that "There is not much they [STNs] can do about stopping the threats" (Standing Committee on Communications 2009, 50). Though STNs are theoretically free to choose when and if they work with the state, in practice having an impact requires working with the state. Since the original call for volunteers for Project Grey Goose, Carr has solicited volunteers for a project he calls "Grey Balloons," which is an open-ended project to create a standing pool of volunteers that are ready and able to help the U.S. intelligence community with whatever challenges it might face (Conway 2010). Grey Balloons is a reflection of Carr's "hope that a bridge could be established connecting intelligence community professionals with independent volunteers with the necessary expertise" (Carr 2008). Finally, as in the case of Rossmiller and cyber-counterterrorism, there is profit to be made in assisting the state. In 2009, Project Grey Goose became Grey Logic, "a consultancy and information services provider to governments" (Grey Logic 2009). It is perhaps unsurprising then that Sinkowitsch and Klimburg have encouraged Western governments to promote and support the formation of STNs as a necessary component of their national cybersecurity strategies (Klimburg 2009, p. 202; Standing Committee on Communications 2009, 49).

Finally, there are real reasons for concern when it comes to STNs. When questioned about the legal status of STNs and whether their work borders on vigilantism, Sinkowitsch claimed that there is no legal problem with what STNs do because they rely on information that is freely available on the Web; they are merely collecting and analyzing it in a different, more effective way (Standing Committee on Communications 2009, 53). But recent scandals over advertiser use of social media content (Angwin & Stecklow 2010), as well as the case of a defense contractor mining and analyzing social media content to smear supporters of WikiLeaks and political opponents of the U.S. Chamber of Commerce (Lipton & Savage 2011), indicate that there are

legitimate privacy and legal concerns when volunteers begin doing their own online intelligence work on behalf of the state or powerful corporate interests.

Patrolling National Borders in Cyberspace

Online, volunteer cyber-surveillance efforts have also been used to aid in the production of more traditional forms of security, such as defending territorial integrity by patrolling national borders. Since 9/11, the debate over immigration from the global South has been increasingly linked to the "War on Terror." Part of this linkage can be found in the actions and discourse of what are collectively called "Minutemen" groups. Minutemen groups are most known for their use of physical presence on the U.S.-Mexico border, especially in 2005, a presence spurred by organizers who wanted to draw attention to what they perceived to be the government's lack of intervention in illegal immigration (Seper 2005; J Walsh 2008). Although the Minutemen are not a government agency, their border-watching efforts were meant to supplement—and not replace—the physical intervention of the U.S. Border Patrol; thus the Minutemen appropriated part of the state's power of surveillance without impinging on the state's monopoly on the use of force (J Walsh 2008).

In addition, Minutemen groups have also deployed "Cyber Minutemen," extending surveillance onto the Web (Bonisteel 2006; Web users to "patrol" US border 2006; Jim Wood Guards Mexican Border From His Mission Viejo Home 2010). Using a mix of fiber-optic fencing, Web cameras, motion detectors, infrared sensors, and even aircraft (Glenn Spencer 2011), various Minutemen groups have posted images and live streams to a variety of Web sites.[2] This use of relatively inexpensive surveillance and Web technology is touted by Cyber Minutemen as a viable, high-tech, modern way for citizens to succeed where the state has ostensibly failed in stemming the flow of immigrants across the Mexican border. Jim Wood, founder of the now-defunct Border Fence Project, argues that citizen groups are more efficient and cost-effective than state efforts to secure the border (Campoy 2010). "The bottom line is this," he argues in a letter to supporters, "Despite bureaucratic refusals, delays and boondoggles, we civilians on the border can build a national Border Fence without them, repairing the old and erecting the new... Therefore, we as American citizens and patriots must stand up and do this ourselves."[3] Part of the efficiency arises from the use of distributed volunteers across the Web; volunteers from as far away as Australia have reportedly spotted illegal border crossings (Luscombe 2009). In this case, the convergence of state aims and privately deployed technologies echoes previous, new media "crowdsourcing" efforts such as Wikipedia and the NASA Clickworkers project (see Benkler 2006).

As in the other convergence security cases, Cyber Minutemen have enjoyed some support from the state, as well as from Internet entrepreneurs. Texas governor Rick Perry, the Texas Border Sheriff's Coalition, and private landowners joined Internet company BlueServo in a "public-private partnership" to distribute live feeds of the border to Web volunteers (Burnett 2009;

[2]For current Web border surveillance sites, see http://www.americanborderpatrol.com/ and http://www.texasborderwatch.com/caccount.php; this site, http://technopatriots.com/articles/border-camera-1/, had a camera but the camera is damaged; a now-defunct site is http://www.borderfenceproject.com; contact the authors for archived copies of material from this site.

[3]This letter appeared at http://www.borderfenceproject.com/letter.shtml; it is no longer online. Contact the authors for a copy.

Luscombe 2009). This public-private partnership is a for-profit endeavor. BlueServo claims, "Because www.BlueServo.net is an internet social network, in the future, BlueServo anticipates that high volume of traffic to its website will generate advertising revenue to defray the operations cost of the Virtual Community Watch to the Texas Border Sheriff's Coalition."[4] Thus, in keeping with convergence media business practices, BlueServo intends to meld the Cyber Minutemen desire to secure the border with the political economy of attention found in other Web 2.0 sites such as Facebook and YouTube. This entrepreneurial form of convergence border security has also been proposed by the Heritage Foundation (Carafano et al. 2006).

However, as with other convergence security groups, the Minutemen have had ambivalent, ambiguous, and tense relationships with the state. Although Texas Governor Perry and California Governor Arnold Schwarzenegger publicly endorsed the movement, George W. Bush referred to them as "vigilantes" (Argetsinger 2005). The Department of Homeland Security rejected a proposal to formally integrate volunteer citizen patrols into the Border Patrol (Gorman 2005).

For their part, the Minutemen groups have not sought integration with the state. Rather, they have largely called for an increased police or military presence at the border; they tend to frame their activity as drawing attention to the perceived problem of illegal immigration, drug trafficking, and terrorism. In the main, the Minuteman movement has been strict with members about the use of violence; thus the Minutemen have been careful not to infringe on the state's monopoly on violence for fear of political and legal repercussions. A large Minuteman group, the Minutemen Civil Defense Corps (MCDC), disbanded in 2010 not long after a leader in that organization called for a "locked and loaded"—i.e., publicly armed—patrol of the border (Conery & Seper 2010). The "locked and loaded" muster was intended as a show of arms rather than an explicit call to violence. However, the proposed muster led to an enthusiastic response among members that the MCDC leadership interpreted as potentially violent, stoking fears within the organization that the MCDC would not be able to prevent members from using weapons on alleged illegal border crossers, thus echoing Bush's earlier fears of vigilantism (Bentley 2010). The leaders of the MCDC did not want to cross the border between civil society groups and state-sponsored military groups.

Ultimately, in the case of the Minutemen, their proposed virtual surveillance of the border was accepted by the state far easier than their proposed, *embodied* patrol of the border. While the MCDC disbanded in light of the potential use of force by members, BlueServo and its Web camera network remains active to this day. State officials who decry potential vigilantism at the border tend to ignore or tolerate the use of Web-based surveillance. Most state officials who want increased border security eschew Minutemen-style groups and opt instead for state-sanctioned groups such as the U.S. Border Patrol, the National Guard, or new bureaucratic formations such as the Department of Homeland Security.

Conclusion

We draw two key conclusions from these case studies. First, we see the value in applying media studies theories to security studies. Media studies is currently grappling with many of the transitions, ruptures, and continuities that digitization has wrought; likewise, scholars and

[4] Available at http://www.texasborderwatch.com/about.php, last accessed 28 March 2011.

policymakers alike have grappled with the implications of digitization for security. Synthesizing the two fields will produce new insights for those working in security studies. Second, at the level of politics, convergence security points to a fruitful critique of Hardt and Negri: the boundary between biopower and biopolitical production is not so neat as their work makes it seem. Further work in convergence security analysis will likely continue to blur that boundary; however, we also see convergence security as a means to continue Hardt and Negri's call for true democracy.

These case studies indicate that Jenkins's claim that convergence will apply in other areas beyond entertainment and media is borne out. General Clapper's statement (in the epigraph) indicates that the idea has made its way into the minds of influential professionals of security. Thus, applying convergence to understand changes in security affairs is necessary; moreover, the value of convergence points to other possible media studies theories that could be used in future security studies. Specifically, we should also consider applying the work of other media scholars like Mark Deuze's (2006, 2007) work on digital culture, Axel Bruns (2008) on "produsage," and Hector Postigo's (2003, 2009) and Tiziana Terranova's (2000) exploration of online volunteers and free labor. Media studies could further help us to understand the changes occurring within traditional security organizations, as well as between traditional producers and consumers of security.

Convergence security also undermines Hardt and Negri's perhaps too neat separation between biopower and biopolitical production; there is more continuity between the production of security and the production of other "immaterial goods" than once thought. In fact, it is possible to describe security itself as one of those immaterial goods created via biopolitical production. This has implications for the political project that Hardt and Negri map in *Multitude* and *Commonwealth*. While these findings do not entirely contradict or invalidate Hardt and Negri's belief that biopolitical production is "the social basis on which it is possible today to begin a project of the multitude" (95)—i.e. the project of creating real democracy—they do call our attention to the fact that the multitude can be appropriated to do the work of the state, and often quite happily so.

Further empirical and theoretical work is required to problematize the border between biopower and biopolitical production (and thus likely create a better map towards the democracy Hardt and Negri describe). For example, Deibert and Rohozinski (2010a, 2010b) point to the privatization and outsourcing of knowledge production about and response to threats to and through cyberspace, particularly among "patriotic hackers" in Russia, China, and Iran. We agree with their call for more research on this phenomenon, but we also note that it is not just adversaries of the U.S. that have such groups. The U.S. has "patriotic hackers" as well, and there are powerful policymakers calling for the U.S. government to do more to recruit and support these groups (Andreas 2010). Clearly, the courting and integration of biopolitical "patriotic hackers" into the auspices of the state is another, emerging form of convergence security.

All this said, Hardt and Negri's basic premise that the creative, affective, and immaterial labor of the multitude can lead to real democracy is not necessarily invalidated by convergence security; it is simply nuanced. For proponents of real democracy, the question becomes: how do we integrate the passions, desires, and skills of these groups into a more democratic polis?

References

Andres, R.B. & McNiel, P. (2010). Deterring Chinese Cyber Militias With Freedom Militias. NDU Press Blog, 27 April. Retrieved from http://ndupress.blogspot.com/2010/04/deterring-chinese-cyber-militias-with.html

Andrus, D.C. (2005). The Wiki and the Blog: Toward a Complex Adaptive Intelligence Community. *Studies in Intelligence* 49(3): 63-70.

Argetsinger, A. (2005). In Ariz., "Minutemen" Start Border Patrols; Volunteers Crusade to Stop Illegal Crossings. *Washington Post* (5 April 2005).

Angwin, J. & Stecklow, S. (2010). 'Scrapers' Dig Deep for Data on the Web. *Wall Street Journal*, 12 October. Retrieved from http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html

Arquilla J. (2009). How to Lose a Cyberwar: Why is America Still Letting Online Jihadists Run Amok? *Foreign Policy*, 12 December. Retrieved from http://www.foreignpolicy.com/articles/2009/12/11/how_to_lose_a_cyberwar

Arquilla J. & Ronfeldt, D. (1996). *The Advent of Netwar*. Santa Monica, CA: RAND.

_____. (1999). *The Emergence of Noopolitik: Towards an American Information Strategy*. Santa Monica: RAND.

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven CT: Yale University Press.

Bentley, L. (2010). Minuteman Civil Defense Corps cancels muster, announces dissolution. *Sonoran News*. Retrieved from http://www.sonorannews.com/archives/2010/100331/ftpgMinuteman.html

Bigo, D. (2002). Security and Immigration: Toward a Critique of the Governmentality of Unease. *Alternatives: Global, Local, Political* 27(1): 63-92.

Bonisteel, S. (2006). Minuteman Project Brings High-Tech Security to Arizona Border. *Fox News*. Retrieved from http://www.foxnews.com/story/0,2933,225799,00.html

Bruns, A. (2008). *Blogs, Wikipedia, Second Life, and beyond. From production to produsage.* New York: Peter Lang.

Burnett, J. (2009). A New Way To Patrol The Texas Border: Virtually. *National Public Radio*. Retrieved from http://www.npr.org/templates/transcript/transcript.php?storyId=101050132

Buzan, B., Wæver, O. & Wilde, J.D. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner Pub.

Campoy, A. (2010). *Fence Frustrates Minutemen, Too.* wsj.com (19 March 2010). Retrieved from http://online.wsj.com/article/SB10001424052748703523204575129902304382316.html

Carafano, J. et. al. (2006). Better, Faster, and Cheaper Border Security. *Heritage Foundation.* Retrieved from http://www.heritage.org/Research/Reports/2006/09/Better-Faster-and-Cheaper-Border-Security

Carr, J. (2007). Terror Web 2.0: The Net-Centric Operations of Terrorist Groups Today. *Threats Watch*, 19 June. Retrieved from http://analysis.threatswatch.org/2007/06/terror-web-20/

_____. (2008). Given Enough Eyeballs, All Threats Are Shallow. *CTLab*, 5 September. Retrieved from http://www.terraplexic.org/review/2008/9/5/given-enough-eyeballs-all-threats-are-shallow.html.

_____. (2009). Inside Cyber Warfare: Mapping the Cyber Underworld. Sebastopol, CA: O'Reilly Media.

Carter, M. (2004). Citizens use internet to spy on, thwart terrorists. *Seattle Times*. 18 June.
Cebrowski, A,K. & Garstka, J.J. (1998). Network-Centric Warfare: Its Origin and Future. *Proceedings of the U.S. Naval Institute* 124(1): 28-35.
Conery, B. & Seper, J. (2010). Volunteer force of Mexico border watchers disbands. *Washington Times*. Retrieved from http://www.washingtontimes.com/news/2010/mar/30/volunteer-force-of-mexico-border-watchers-disbands/
Contreras, G. (2009). Hearing Today At Bamc for Hasan. *San Antonio Express-News*, 21 November, p. 1A.
Conway, D. (2010). Volunteer to Help the Intelligence Community. *Zero Intelligence Agents*, 11 January. Retrieved from http://www.drewconway.com/zia/?p=1744
Conway, M. (2006). Terrorist 'Use'of the Internet and Fighting Back. *Information and Security* 19: 9-30.
Deibert, R & Rohozinski, R. (2010a). Cyber Wars. Index on Censorship, 23 March. Retrieved from http://www.indexoncensorship.org/2010/03/cyber-wars-technology/
_____. (2010b). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology* 4: 15-32.
Dempsey, J. (2007). Biz zeroes in on real-life terrorist hunter. *Variety*. 23 July. 19.
Deuze, M. (2006). Participation, remediation, bricolage: Considering principal components of a digital culture. *Information Society* 22(2): 63–75.
_____. (2007). Convergence culture in the creative industries. *International Journal of Cultural Studies* 10(2): 243.
'Glenn Spencer'. (2011). *Southern Poverty Law Center*. Retrieved from http://www.splcenter.org/get-informed/intelligence-files/profiles/glenn-spencer
Gorman, A. (2005). No Plans for Citizen Border Patrols Seen. *Los Angeles Times*. Retrieved from http://articles.latimes.com/2005/jul/22/local/me-border22
Grey Logic. (2009). *Project Grey Goose Phase Ii Report: The Evolving State of Cyber Warfare*. Grey Logic.
Harden, B. (2006). In Montana, casting a web for terrorists. *TechNews*. 4 June.
Hardt, M & Negri, A. (2004). *Multitude: War and Democracy in the Age of Empire*. New York: The Penguin Press.
Harris, S. (2010). T*he Watchers: The Rise of America's Surveillance State*. New York: Penguin Press.
House Permanent Select Committee on Intelligence. (2011). *Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence*. United States House of Representatives, 10 February.
Jenkins, H. (2006). *Convergence Culture: Where Old and New Media Collide*. New York: New York University Press.
'Jim Wood Guards Mexican Border From His Mission Viejo Home'. (2010). *Mission Viejo Dispatch*. Retrieved from http://missionviejodispatch.com/people/jim-wood-guards-border-from-mission-viejo/
Klimburg, A. (2009). Whole-of-Nation Cyber Security. In Carr J (eds) *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media, 199-202.
Lawson, S. (forthcoming). Surfing on the Edge of Chaos: Nonlinear Science and the Emergence of a Doctrine of Preventive War in the United States. *Social Studies of Science*.
Lia, B. (2005). Al-Qaeda Online: Understanding Jihadist Internet Infrastructure. *Janes Intelligence Review*, 2 December.

Lipton, E. & Savage, C. (2011). Hackers Reveal Offers to Spy on Corporate Rivals. *New York Times*, 11 February. Retrieved from http://www.nytimes.com/2011/02/12/us/politics/12hackers.html?_r=2

Lubrano, A. (2007a). An unexpected patriot terrorist hunter. *Philadelphia Inquirer*, 22 July. Retrieved from http://www.philly.com/inquirer/local/20070722_Terrorist_Hunter.html?viewAll=y

_____. (2007b). The online search that never ends. *The Philadelphia Inquirer*. 26 July. A01.

_____. (2007c). Web sleuth testifies in terror trial: A montana woman related how she ensnared a PA Man accused of plotting to blow up the trans-alaska pipeline. *The Philadelphia Inquirer*, 10 July. B01.

_____. (2009). Web-based terrorist hunter to teach. *The Philadelphia Inquirer*, 9 January. A03.

Luscombe, R. (2009). Patrol watches Texas-Mexico border-from pub in Australia. *The Guardian*. Retrieved from http://www.guardian.co.uk/world/2009/mar/23/texas-mexico-patrol-webcam-australia

Mitchell, M. (2004). Cyber sleuths patrol the web for signs of terrorism. *Associated Press*, 26 June.

Moore, E. (2004). Mother of 3 hunts terrorists at night: Montana judge, 6 others use web to snare suspects. *The Houston Chronicle*, 12 July. A1.

Postigo, H. (2003). Emerging Sources of Labor on the Internet: The Case of America Online Volunteers. *International Review of Social History* 48(S11): 205-223.

_____. (2009). America Online volunteers: Lessons from an early co-production community. *International Journal of Cultural Studies* 12(5): 451-469.

Project Grey Goose. (2008). *Project Grey Goose Phase I Report: Russia/Georgia Cyber War - Findings and Analysis.* Project Grey Goose.

Roesler, R. (2004). Terrorist hunters get mixed welcome; little- known civilian group in spotlight. *Spokesman Review*, 15 May. B1.

Rossmiller, S. (2007). My Cyber Counter-Jihad: How a Montana Woman Broke New Counterterrorism Ground. *Middle East Quarterly*, Summer: 43-48.

Rubinkam, M. (2007). Former Montana Judge Goes Undercover At Night on Web to Hunt Terrorists. *Associated Press*, 19 July.

Seper, J. (2007). Pipeline Plotter, Seeking Al Qaeda Funding, Convicted; Given Maximum of 57 1/2 Years After Jury Deliberated Short Time. *Washington Times*, 14 July, p. A02.

_____. (2005). 'Minutemen pronounce border vigil a success'. Washington Times. Retrieved from http://www.washingtontimes.com/news/2005/apr/19/20050419-121839-2468r/

States News Service. (2009). Suburban Counterterrorist Works From Home to Thwart Jihad. *States News Service*, 9 January.

Steele, R.D. (2001). *On Intelligence: Spies and Secrecy in an Open World.* OSS International Press.

Terranova, T. (2000). Free Labor: Producing Culture for the Digital Economy. *Social Text* 18(2): 33-58.

Thomas, T.L. (2003). Al Qaeda and the Internet: The Danger of "Cyberplanning." *Parameters* 33(1): 112-124.

Tomes, R.R. (2007). *U.S. Defense Strategy From Vietnam to Operation Iraqi Freedom: Military Innovation and the New American Way of War, 1973-2003*. London: Routledge.

Walsh, J. (2008). Community, surveillance and border control: The case of the minuteman project. *Sociology of Crime, Law and Deviance* 10: 11–34.

Web users to "patrol" US border. (2006). *BBC*, 2 June 2006. Retrieved from http://news.bbc.co.uk/2/hi/americas/5040372.stm

Weimann, G. (2005). How Modern Terrorism Uses the Internet. J*ournal of International Security Affairs*, Spring(8).