International Journal of Communication 6 (2012), 1965–1988 1932–8036/20120005

User-Generated Warfare: A Case of Converging Wartime Information Networks and Coproductive Regulation on YouTube

BRITTANY FIORE-SILFVAST[1]
University of Washington

User-generated content-sharing (UGC) platforms, such as YouTube, emerged as venues for competing wartime information and images among military, insurgent, and civilian user groups during the Iraq War. This article introduces user-generated warfare (UGW) as a theoretical concept to articulate this phenomenon and consider its implications for reshaping wartime information networks and flows outside of formal institutions. It is a variant of "netwar" that further locates this generative user activity within the sociotechnical infrastructure of the UGC platform. The present analysis examines an instance of UGW that highlights how user agency is configured through the coproduction of affordance and constraint via the YouTube platform and within a communicative context in which wartime user networks are converging outside formal channels.

During the early years of the Iraq War, user-generated content-sharing (UGC) sites emerged as venues for competing wartime information and images. Popular UGC sites like YouTube played host to a wide range of Iraq war videos, including propaganda and recruitment tools distributed by the U.S. military and insurgent networks, media coverage by mass media and citizen journalists, and combat footage produced by soldiers and often remediated or remixed by civilians. The conventional wartime media landscape expanded into cyberspace, adopting new platforms and user communities, prompting new strategies for waging war. Underlying this morphing landscape of wartime mediation was the simultaneous growth of easily available technologies of production, such as digital cameras and editing software and information and communication networking technologies, most notably UGC sites. These new media conditions further facilitated the development of not simply an information-based conflict within which "information generation, processing, and transmission become the fundamental sources of productivity and power" (Castells, 1996, p. 21), but one that also is increasingly organized through networks (Arquilla & Ronfeldt, 1997).

[1] The author would like to thank Professors Kirsten Foot and Manuel Castells, and the anonymous reviewers for their valuable comments and advice.

Brittany Fiore-Silfvast: fioreb@uw.edu
Date submitted: 2011–10–15

Warfare within the new networked information environment emerges within a sociotechnical gathering of Web platforms, platform providers, digital tools, and user communities. User-generated warfare (UGW) is a term introduced here to help articulate important ways that information-oriented conflict is waged in cyberspace via UGC platforms. UGW exemplifies Arquilla and Rondfeldt's (1997) network concept of information-based conflict, which emphasizes the networked organizational structure of its actors. Netwar is an emerging societal level mode of information-based conflict "involving measures short of warfare in which the protagonists use . . . network forms of organization, doctrine, strategy, and communication" (p. 277). While Arquilla and Ronfeldt (1997) warn that netwar is not just about the new technologies, they also note that users have ICT-expanded capabilities for taking a netwar approach to conflict. Further, the networked information environment enables a type of netwar that can be carried out entirely in an Internetted manner (p. 285). UGW can be characterized as a new variant of this Internet-based netwar in which the tactics between warring groups occur within a particular UGC platform, which provides a more refined lens through which to understand emerging patterns in netwar. Netwar can describe modes of conflict across a range of network designs and agendas, including transnational terrorist groups, criminal syndicates, ethnonationalist movements, and some activist networks (Arquilla & Ronfeldt, 1997). More specifically, UGW describes a mode of conflict among user networks of wartime actors, including the U.S. military, as well as nonstate actors such as insurgents and civilians. As users of a particular UGC platform, these wartime actors can participate in shaping the flows of wartime information outside of mass media institutions via their shared UGC platform. This phenomenon prompts the following guiding research questions: What are the implications of UGW for the production, distribution, and regulation of wartime information? How can UGW help us to better understand the network tactics and network organizational forms emerging across societal and military contexts?

UGW, as a theoretical concept, makes possible two analytic frames required to more carefully and productively makes sense of the implications potentiated by this variant of netwar. The first analytical frame locates the analysis of netwar more precisely within a specific UGC platform architecture and platform politics that influence user agency and the contours of the wartime media landscape. This moves the analysis of netwar beyond the relationship among network protagonists toward recognizing the contributions of the generative technology platform and its sociotechnical infrastructure in shaping the wartime media landscape, user agency, and thus the nature of network organizing that can take place. The second analytical frame redefines the wartime actors participating in information-oriented conflicts as *users* in relation to a specific platform. Under this broader identity, U.S. military, insurgents, and civilians, spanning geographies and ideologies, are all operating and acting within the same platform, using the same platform-based tools. Without traditional media institutions acting as gatekeepers in these platforms, the user's capacity to produce and influence wartime information flows and mediations expands in particular ways. Yet this expanded capacity to influence information flows is coproduced through the networked architecture and the corporate owner as a "patron" (Burgess & Green, 2008) of user participation. The distinctions between conventional notions of production and usage are blurred, resulting in a hybrid form of content production that has been termed elsewhere as "produsage" and "co-creation" (Bruns, 2008). To further complicate this view of content coproduction, van Dijck (2009) argues for the importance of users as "data providers" as well. Consequently, user agency is much more complex than are simple relationships of user or producer, as it must account for the multiplicity of human and nonhuman actors involved and the various roles that "produsers" may assume (Bruns, 2008; van Dijck, 2009).

To illustrate the phenomenon of UGW, this article examines its emergence within a particular case on the YouTube platform. YouTube is one of the most popular venues for UGC, but certainly only one of many possible venues for UGW. YouTube relies on what some scholars have called the "free," "volunteer," or "immaterial" labor (Postigo, 2003, 2009; Terranova, 2000) of users to both produce and regulate content. In UGW, wartime information flows are coproduced and coregulated via the YouTube platform. The information and communication flows become objects of symbolic power transforming the YouTube platform into a "place" to be dominated and defended—a cyberborder to secure. Information-oriented conflict does not require the warring user groups to occupy the same geographic place as combat operations would in conventional warfare contexts. Thus, the global-reaching YouTube platform is not a placeless "space of flows" (Castells, 2001); instead, these information flows interact with the traditional "space of places" (Castells, 2001) to create a new spatial structure constituted by networks connecting places. Increasingly, wartime operations depend on these spaces of information and communication flows. Consequently, Arquilla and Ronfeldt (2001) have predicted that "(p)sychological disruption may become as important a goal as physical destruction" (p. 2). As such, wartime actors are taking seriously their participation and volunteer labor on YouTube as important contributions to the war effort.

A key feature of user participation in the networked media landscape is the growing trend for civilians to organize in networks to cooperatively act, as well as disrupt. Dispersed civilian users gain an ICT-expanded capability to employ a strategic and tactical netwar approach in cyberspace, coordinating efforts, collecting intelligence, and targeting audiences. Arquilla and Ronfeldt (1997) argue that while civil society will be strengthened with this trend and new social movements are likely to emerge, nonstate forces, such as terrorist groups, will also benefit. In recent history, the U.S. military has conducted wartime operations mostly far from the homefront, or "over there," but the "division between 'here' and 'there' matters little in the global battle to control the message and to stage the definitive media event, the definitive attack on the global network" (Raley, 2009, p. 69). As cyberspace emerged as another front of the Iraq war, some U.S. civilian users and user groups took it upon themselves to defend the YouTube platform against terrorists in cyberspace. These wartime efforts are instances of UGW. In the past, U.S. civilians have been limited by geographical distance and the high risk associated with challenging institutional media gatekeepers to coopt information and communication flows during wartime. At present they can access YouTube from the comfort of their own home and bypass the institutional media gatekeepers. Thus, while civilian participation in wartime is not new, what is notable is the new communicative context for participation that exists outside the institutional media channels and the networked architecture that amplifies the convergence of wartime information networks and flows. While UGW may bypass the institutional mass media gatekeepers, network architectures and corporate owners act as gatekeepers in different, more opaque ways (Rosen, 2008).

UGW is both enabled by what Zittrain (2008) terms "generative" technologies, and coproduced through the affordances and constraints of YouTube's platform. The generative technologies available on YouTube's platform afford users the ability to openly produce, disseminate, and innovate. However, these generative features are embedded in an architecture that is controlled and regulated by the sociotechnical infrastructure of the YouTube corporation (Google). As Gillespie (2010) reminds us, "these 'platforms' do have edges" (p. 358) that afford and constrain user-generated activity in various ways. YouTube's sociotechnical infrastructure, which consists of a variety of corporate policy decisions, community guidelines, Web architecture, and technical protocols, threatens the full generative capacity of the

technology platform. Situating UGW within the specific sociotechnical infrastructure of the YouTube platform allows for the recognition of the YouTube corporation as an important actor within a wider media landscape in which military, insurgent, media, and civilian user networks operate and compete. The YouTube corporation acts through the YouTube platform, which this analysis conceptualizes as a sociotechnical ensemble (Bijker, 1995). The platform then plays an important role in influencing the information flows and the distribution of user agency. Since user agency is coproduced by the particular sociotechnical infrastructure of the Web platform, UGW might look different as it manifests across different UGC platforms.

Regular observation of this emerging phenomenon from 2007–2009 precipitated more specific research questions to address the nature of coproduction in UGW. How do relationships of coproduction contribute to shaping the wartime media landscape on YouTube? How do those coproductive relationships influence the distribution of agency of wartime actors conducting netwar on YouTube? To address these research questions, this article illustrates and contextualizes these relationships in a particular case study that focuses on an instance of UGW in which a civilian user group—Operation YouTube Smackdown (OYS)—is conducting wartime activities on YouTube. OYS is a large, decentralized civilian user group, which attempts to collectively regulate "Internet terrorists" and terrorist supporters by regulating information flows and destroying their capacity to communicate and mobilize on the YouTube platform. As they mobilize against the "Internet terrorists" within the coproductive and convergent spaces of the YouTube platform, they realize that they must expand the target of their mobilization to include the YouTube corporation to pressure them to more strictly regulate what OYS would classify as terrorist-supporting content. This article reviews relevant scholarly discussions to develop a theoretical framing for the analysis of this instance of UGW.

Networks of War

Network structures are increasingly the form and organizational design adopted not only by the insurgent groups and the military but also by nonstate user communities, grassroots activist groups, and corporate or political campaigns (Bennett, 2003; Chadwick, 2007; Chadwick & Howard, 2009). While the Industrial Age favored state-run military hierarchies, the Information Age favors nonstate actors in social networks (Arquilla & Ronfeldt, 1997; Ronfeldt & Arquilla, 2001). As the industrial society shifts toward a network society, new frontiers and modes of warfare emerge, along with new spaces of flows for mediation and user engagement (Castells, 1996).

The U.S. military's shifting war machine has adopted new battlefields, weapons, network forms of organizing, and strategies of operations. Its recognition of the importance of virtual territories as spaces of information warfare transformed the way they conduct war. Donald Rumsfeld, former U.S. Secretary of Defense, warned in an address to the Council on Foreign Relations (2006), "Our enemies have skillfully adapted to fighting wars in today's media age, but for the most part we, our country, our government, has not adapted." In March 2007, a year after this address and four years into the war, the Department of Defense (DoD) established their presence on the YouTube battlefield by launching their own Multi-National-Forces-Iraq (MNFI) channel that regularly aired military-approved videos of the Iraq War. The MNFI channel was established to create a U.S. Web offensive against the negative propaganda circulating from the insurgents and the "enemies" in cyberspace (Jordan, 2007). The U.S. military then banned

access to social media sites, including YouTube, on DoD computers in Iraq, a policy shift that reflected the military's commitment to controlling these spaces in a time of war. These convergent media spaces threatened the military's ability to manage information in wartime. Within these new venues for war in cyberspace, the capacity of the U.S. military to operate is, in part, defined in relation to the platform itself. Thus, the future of the U.S. military's strategy is aimed at developing and employing military communications and surveillance capabilities to new venues of operations and converging media networks (Der Derian, 2009; Graham, 2010). A traditionally hierarchical institution must now adopt network centric strategies for deployment in cyberspace.

Long before the U.S. military, insurgent groups were utilizing the Internet for spreading propaganda, organizing attacks, recruiting, fundraising, training, and conducting psychological warfare (Anden-Papadopoulos, 2009; Weimann, 2006a). A scan of the Internet in early 2006 revealed more than 4,800 websites serving terrorists and their supporters (Weimann, 2006b, p. 624). With the capacity to reach multiple large audiences through user-generated operations, insurgents don't need to depend on traditional news media or other institutions to communicate. In many instances, Western news broadcasters had to rely on footage uploaded by insurgents for their own news coverage of an event because they had not been present (Dauber, 2009). Dauber articulates the view of terrorist attacks as media events themselves. As terrorists have become increasingly adept at synchronizing attacks on the ground with electronic jihad, many have suggested that the terrorist attacks are committed most importantly so that they may be filmed and distributed (ibid.). Similarly, Weimann and Winn (1994) conceptualize modern terrorism as a theater-of-terror in which terrorists communicate messages through the use of staged, choreographed violence. From this perspective, the "true target is not that which is blown up—that item, or those people—for that is merely a stage prop. What is really being targeted are those watching at home" (Dauber, 2009, p. v). The multiple iterations and viral trajectories of insurgent videos extend their reach across new sites and to new audiences, which can make the Internet an ideal organizing medium for terrorist groups (Weimann, 2006b, p. 624).

As the Iraq War became the centerpiece for a larger movement that George W. Bush called the Global War on Terror (GWOT), state and civilian actors were called on to defend and secure the homeland against terrorism. The GWOT is a war against an elusive, stateless enemy—a war on terrorism tactics. This preemptive mobilization of forces against potential threats meant that, in practice, there was "little difference between outside and inside, between foreign conflicts and homeland security" (Hardt & Negri, 2004, p. 14). Building on Hardt and Negri, Lawson and Gehl (2011) articulate the changing orientation from defense to security, 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" (p. 2). The pervasive nature of this movement calls on all state and nonstate actors to participate in the response to and the knowledge production about these potential threats. Thus, civilians become integral to securing the borders of the nation against terrorism. The borders that are easiest to reach for most civilians to counter terrorism are those in cyberspace.

At the same time, new media conditions are facilitating a "convergence" (Jenkins, 2006), not only between networks of media and cultural production but also between networks of war. In this convergent space of war, the same networks and technology are employed for different ends. Der Derian (2009) theorizes the convergent nature of war through a conceptual map of the Military-Industrial-Media-Entertainment-Network (MIME-NET) in which he demonstrates how what he terms "virtual warfare" is

produced, represented, and executed through the nodes and links of converging networks. The MIME-NET describes the information and technology feedback loops among the networked domains and the resulting convergence of the means of distinction among them. Examples of this feedback loop and convergence of domains include how simulations used to train pilots are used as special effects in Hollywood movies and the way military combat units are trained with video games played by teenagers (Der Derian, 2009). The MIME-NET maps a nodal infrastructure and flow of the virtual war machine, but what is undertheorized in this network map and also relevant to understanding the implications of UGW is the growing networks of online civilian users acting within this convergent space.

As self-organized online volunteer groups engage in online activities, such as intelligence gathering and counter-propaganda, they are supplementing the state's efforts to counter terrorism (Lawson & Gehl, 2011). Deibert and Rohozinski (2010) point to a similar phenomenon of "patriotic hackers" in Russia, China, and Iran who have the necessary technical expertise to generate knowledge, and respond to threats to their respective state, thus blurring the lines between citizen and state. Lawson and Gehl (2011) explore this phenomenon in the United States and call it an emerging form of "convergence security" in which online volunteer civilian networks are supplementing the work of security for the state. The case of the Cyber Minutemen, a group that monitors surveillance cameras positioned on the U.S.-Mexico border and reports crossings to the authorities without any official state authorization, is instructive here (Lawson & Gehl, 2011; Raley, 2009). The group considers itself an essential component in securing the nation's border zones where they find the state to be ineffective. In this case, state aims and private citizen-led surveillance converge to produce a new kind of coproductive security that changes relationships between the consumers and producers of security (Lawson & Gehl, 2011). Similarly, as an online volunteer civilian group, OYS is attempting to secure the cyberborders of YouTube against terrorists and exploit the changing relationships among users and platform providers.

Amplifying the Network as an Organizational Form

ICT-expanded capabilities of individuals influence the potential for cooperative production and collective action. It is important to focus not only on the ways that individuals are appropriating ICTs as tools in cooperative production and collective action but also on how, through ICT-enabled spaces, individuals generate new forms of communicating and organizing. ICTs and their enabled-network organizing possibilities are increasingly permeating the daily activities of most U.S. civilians, offering new mediated potential for civilian engagement and mobilization across political, economic, and social domains (Benkler, 2006; Castells, 1996, 2009; Ronfeldt & Arquilla, 2001). In this ICT-enabled space there is a blurring of public and private domains from which Bimber et al. (2005) argues that new forms and strategies for collective action emerge. It is also the blurring of horizontal and vertical (more hierarchical) networks that lead to more hybrid organizational types and flexible networks that can self-organize, bypassing the need for a formal organization (Bimber, Flanagin, & Stohl, 2005; Bimber, Stohl, & Flanagin, 2009). Similarly, Castells (2009) argues that a new modality of communication he calls "mass-self-communication" is emerging from the convergence of self-communication and mass communication. This modality allows individualized communication to reach mass audiences without having to go through formal organizations.

While Bimber et al. (2005) have theorized what this trend means for the relationship of the individual to collective action, other scholars have suggested that there are similar trends emerging in the relationship of the individual to cooperative production in the networked information economy (Benkler, 2006; Zittrain, 2008). Examining these organizational trends in the economic domain, Benkler (2006) argues that they are shifting modalities of information production towards a more cooperative, decentralized, nonproprietary production in which individuals have greater capacity to do more individually, cooperatively, and organizationally outside of the market sphere (p. 8). Cooperative production has also been observed as a core modality in smart mobs (Rheingold, 2003), crowd sourcing (Howe, 2006), and the operations of network armies (Hunter, 2002). The network army is particularly instructive in looking at the operations of OYS. This organizational form encourages distributed, collaborative sharing of information and resources without command and control structures and the coordination of individual actions toward a common goal. Instead of bosses or commanders, there may be influencers or coordinating leaders who emerge, but there is no formalized hierarchical system. Although these organizational formations existed before the Internet, current research emphasizes the ways in which the Internet and other ICTs can dramatically amplify both the power of networks and the speed at which they form (Hunter, 2002). As the present case study demonstrates, OYS operates as a network army, as it organizes individual actions toward a common goal through coordinating leaders and the networked collaborative sharing of information and resources.

YouTube as a Sociotechnical Ensemble

YouTube's media landscape is shaped by the user-driven and corporate activities of circulation and regulation that are coproduced via the YouTube platform. The YouTube platform can be conceptualized as a sociotechnical ensemble, including Web architecture, regulatory policy, reviewers, and generative features for coproduction and coregulation. For example, YouTube users coproduce regulation by flagging videos that they determine are inappropriate or violate its community guidelines. YouTube's staff then reviews the flagged videos to determine whether the content violates the community guidelines, which in turn would violate YouTube's Terms of Service and necessitate its removal from the site. The community guidelines constrain and afford what content the users and the corporate actors can regulate. YouTube's reviewers work as the front line for interpreting the community guidelines, making case-by-case decisions about whether to remove flagged videos, leave them up, or send them up through an internal hierarchy of reviewers for further consideration (Rosen, 2008). This "Decider Model" is not transparent and some would argue is inconsistent, which makes formally challenging it that much harder (Rosen, 2008). It situates the YouTube corporation as an intermediary between the law and the user, which affords maximum control in interpreting and applying these guidelines without incurring greater liability. As a patron, the platform provider has the power to set the conditions—whether they are technical, legal, or economic—under which users can participate. The YouTube corporation, in contraposition to the mass media institutions, claims that it is simply a facilitator and host for information sharing, offering an open and flat space for anyone to "broadcast" themselves. Thus, the kinds of interventions and choices these providers actually do make can be harder to see (Gillespie, 2010, p. 353). In the following case study, we must consider carefully the role of the YouTube platform and the corporation in coproducing both the wartime media landscape and the agency of wartime actors.

Methods

For this case study analysis, I chose to focus on the YouTube Web platform even though there are other means, even other Web platforms, through which insurgents distribute videos and information that could serve as potential sites for studying UGW. This YouTube war is importantly embedded in a larger Web-wide link context in which many more operations and facets of UGW activity exist.

To fully capture and contextualize the spectrum of activities in this particular case, I employed multiple close readings over two-and-a-half years of the textual, visual, and relational (through links) evidence from the case that spanned across YouTube and the surrounding blogosphere. I view this evidence (texts, images, and links) as a network of coevolving Web artifacts that are inscribed dynamically with the communicative and operational activities of UGW. Engaging in what Foot and Schneider (2006) call "web archaeology," I excavated these Web artifacts and carefully observed them over time to make inferences about user practices and their implications for the broader, mediating and operating networks at war. After taking an inventory of the content, features, and links on what started as two primary sites out of which OYS operated, I then followed and tracked each new post or link, historically contextualizing it within the larger conversations and situating it within its relational link context. I recorded when and how the operations morphed or expanded in terms of features and aims and when sites of operations multiplied. This required writing copious observational notes and taking screen shots to capture changes and texts in their context. This longitudinal and multi-sited approach enabled the interpretation of these evolving textual, visual, and relational web artifacts within the sociohistorical context of the landscapes they inhabited and constituted. In this case study, the communication linking members of network armies was open and public, which made the circulating texts, images, and links reliable sources for learning about the formation and operation of a network army.

The case study illustrates an instance of UGW in which an online civilian user group, OYS, fight terrorists on YouTube, entering the convergent spaces of wartime mediation. After detailing the strategic and tactical operations of OYS, this case documents how the battle against "Internet terrorists" morphed into a struggle against the YouTube corporation for acting as a host to Internet terrorists.

Case Study: Operation YouTube Smackdown

OYS is a volunteer online civilian-user network that coordinates operations across multiple blogging communities to fight Internet terrorists on YouTube. Launched in July 2007, already four years into the Iraq War, OYS has steadily increased in size and influence since its inception. OYS began out of a conversation among conservative bloggers who were inspired by the potential for private citizens to fight the war through the Internet. The inspired blogger (and later OYS founding member) wrote:

> I read at PJM (Pajamas Media) that a lone blogger by the name of Rusty Shackleford has made it his personal business to shut down Taliban websites. This is a real fight, a people's war, a private citizen waging combat on his own! The Jawa Report vs. the Taliban, and guess who's winning? . . . A lone hacker is knocking out enemy

> communications from the privacy of his study. Twenty years ago this would have been science fiction![2]

The blogger called on his blogger friends to join the effort by volunteering to scour YouTube for footage from the "enemy" and flag it for YouTube's corporate staff to review and remove. After one of the bloggers volunteered his blog to serve as the coordinating site of operations, a handful of other bloggers began to connect their blogs and direct their readership to OYS.[3] It was there and then that the conservative bloggers and their readership began organizing themselves into a network army that would fight Internet terrorists on YouTube.

The OYS Mission

"Countering the Cyber-Jihad one video at a time" was one of the slogans OYS used to publicize their mission. On the initial OYS launch site, the group posted their mission publicly, calling on as many people as possible to join their "crusade" to fight the spread of terrorist propaganda on YouTube.[4] User Svinrod made the first attempt to enlist volunteers:

> Individually your participation might seem insignificant. But thousands of us united will crush this venue as an outlet for enemy propaganda. Our mission is to shut down the Jihadis on YouTube. Strike a blow for freedom. Copy this link and send a copy to everyone you know. Then go to YouTube and start your own personal crusade against terrorism. . .[5]

The group published instructions in "six easy steps," detailing how to sign into YouTube and flag a video. The task of removing an insurgent video was broken down into modular, easily accomplished steps that enabled users to contribute to the greater mission of OYS, whether it involved contributing five minutes every day or an hour only once. The decentralized cooperative organization harvested the power of the individual to accomplish small tasks that collectively contribute to achieving common goals. The OYS site provided a list on the side of the page listing the links to the videos that they were targeting and instructing users to go flag them on YouTube. This technique of mass coordinated flagging reflects the

---

All primary source digital objects of inquiry will be referenced as archived links with a transparent access date.

[2]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.smackdowncorps.org%2Fabout.html.&date=2010-06-10

[3]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.smackdowncorps.org%2Fabout.html.&date=2010-06-10

[4] http://www.webcitation.org/query?url=http%3A%2F%2Fmuninn-quotheraven.blogspot.com%2F2007%2F07%2Fyou-tube-smackdown.html&date=2010-06-10

[5] http://www.webcitation.org/query?url=http%3A%2F%2Fmuninn-quotheraven.blogspot.com%2F2007%2F07%2Fyou-tube-smackdown.html&date=2010-06-10

principles of swarming, which describe a "seemingly amorphous, but deliberately structured, coordinated, strategic way to strike from all directions at a particular point or points, by means of a sustainable pulsing of force and/or fire, close-in as well as from stand-off positions" (Ronfeldt & Arquilla, 2001, p. 12). In this case, the network army was not using fire, but rather the force of coordinated flagging efforts.

OYS's coordinated flagging is not only aimed at removing jihadist videos and affiliated accounts but also at policing the YouTube site to ensure that it will not encounter images and information that threaten OYS's agenda and values. Even with targeted coordinated flagging operations, OYS volunteers reported that many of the videos they had flagged on YouTube were not being taken down. Svinrod wrote:

> We object to YouTube making a profit hosting videos celebrating the death of Coalition Soldiers (and pretty much everyone else) while washing their own hands of any responsibility. We're out to smack those videos down, and maybe shake a little sense into YouTube in the process.[6]

This shows how members of OYS began to discursively construct the YouTube corporation as a new adversary. One OYS member explained that "Despite our best efforts, flagrant Terms-of-Service (TOS) abuses and calls for violent jihad remain on YouTube's servers. So essentially, not only are we fighting the islamo-fascists, we are fighting YouTube."[7] Their battle against the insurgent networks became a battle against the YouTube corporation for acting as a host to "terrorist supporting" videos, which OYS argued was equivalent to offering material support to the enemy in a time of war and therefore acting against executive orders. It became common for members to post a message addressing YouTube on their blog that included the video that OYS already tried flagging unsuccessfully, along with a description of each video frame that clearly violated YouTube's community guidelines. This direct address to the YouTube corporation revealed that this community was watching and keeping track of YouTube's corporate actions or inactions as much as it was the insurgents' activity.

Organizational Structure of Smackdown Corps

OYS began as a small decentralized network of bloggers engaging each of their respective readerships in collective flagging campaigns. In September 2008, a little over a year after the launch of OYS, its founding members decided that in order to manage and cultivate the growth of the effort, they needed a higher level of organization and coordination across factions.[8] They created Smackdown Corps

---

[6]http://www.webcitation.org/query?url=http%3A%2F%2Fmuninn-quotheraven.blogspot.com%2F2010%2F01%2Fwelcome-to-operation-youtube-smackdown.html&date=2010-05-28

[7]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.freerepublic.com%2Ffocus%2Ff-news%2F2374468%2Fposts&date=2010-05-28

[8]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.smackdowncorps.org%2Fabout.html&date=2010-05-28

(SC), which was a site that served to coordinate the 10 SC member hosting sites and over 25 SC supporter sites.[9] The 10 SC members that each had opened OYS operations on their own sites could be considered the coordinating leaders (Hunter, 2002) within the relatively flat organizational structure of the network army. The SC supporters are actors that may link to OYS operation sites, exhibit OYS graphics or logos, and participate regularly in OYS operations by flagging videos or gathering intelligence.

Beyond flagging videos, SC provided other ways to contribute and offered a set of tools that could be mobilized to these ends. Participants contributed by designing graphics, incorporating graphics and feeds on their sites, and using multiple modes of communication for publicity. For instance, multiple YouTube videos and channels were devoted to supporting OYS through publicity or by offering information about how to flag a jihadist video. Another way OYS users contributed to the effort was by gathering intelligence on the "Internet terrorist" network using the "Terrorist Logo ID" PDF of jihad symbols and flags posted under "Smackdown Tools" on the SC site to identify and report jihad videos back to SC.[10] The SC site also linked to Google Translator, which was cued to apply to Arabic text found on YouTube to try to decipher in English what users were saying and whether there were jihadist intentions.

Emerging from the mobilization of these tools across OYS's distributed communities was a coordinated movement to collect intelligence about the enemy, which paralleled the operations of military intelligence and may have at points even overlapped. From the timeline of events (Figure 1), it is clear that the surge of U.S. military effort to take seriously the Internet as a battleground—by launching the MNFI YouTube channel to combat insurgent propaganda and shifting policies to control the use of social media sites by soldiers—occurred only a few months prior to the launch of OYS. Operating alongside (but not formally with) the U.S. military on YouTube, this correspondence in time suggests that OYS attempted to fill the void of a virtual counterpart to the militia on the ground in fighting Internet terrorists by acting to supplement these state activities.

[9]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.smackdowncorps.org%2Findex.html&date=2010-05-29

[10]http://www.webcitation.org/query?url=http%3A%2F%2Fwww1.nefafoundation.org%2Fmiscellaneous%2Fnefainsurgencychart0308.pdf&date=2010-05-28

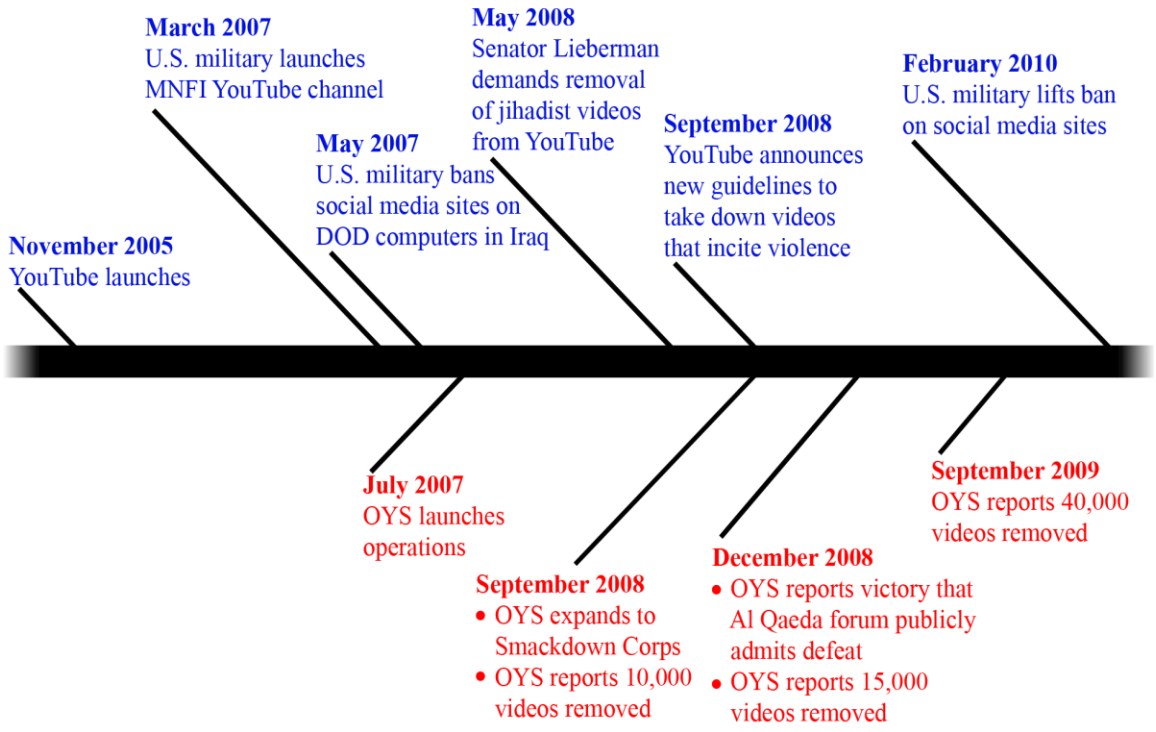

Figure 1. Timeline of OYS (red), YouTube, U.S. military, and state (blue) events.

The Rhetoric of War

Digging into the blogging forums and user comments of OYS, it becomes clear that the rhetoric employed throughout blurs the lines between the U.S. military's war effort on the ground in Iraq and their YouTube War. Kat, an OYS participant, believed that the actions she performed in this YouTube War were influencing the operations of Iraq War. She was participating in the virtual execution of the war via the generative mechanisms of YouTube's Web platform. Kat described the importance of joining "an Internet army whose function is clandestine warfare against such blatant use of public space to further terrorist propaganda, recruit fighters and provide direct material support to such organizations."[11] From this view, each user could participate in effectively destroying the virtual existence of the "enemy" on YouTube. Kat explained how her actions on the YouTube platform operated on the battlefield.

[11]http://www.webcitation.org/query?url=http%3A%2F%2Fthemiddleground.blogspot.com%2F2007%2F08%2Finformation-war-internet-videos-and.html&date=2010-05-28

> I have taken up virtual arms to assist in decreasing that number [of insurgent videos], even if it is by one since one suicide bomber can kill hundreds of people with one bomb. . . . We have but to organize and dedicate ourselves to the battle. Remembering that their defeat is not in their total or instantaneous destruction but in the harassment and continual interdiction of their abilities. Remember that all efforts are worthy if even one life is saved.[12]

Kat's rhetoric reveals her equation of the impact of virtual combat and the combat on the ground in Iraq. She correlates the presence of a video of a suicide bomber with the actual killing of hundreds of people. Furthermore, she links her efforts to remove videos in which U.S. soldiers are harmed with the saving of lives. For Kat, "it is a battle . . . for a space that has been generally left to the terrorists."[13] OYS supporters perceive the YouTube platform as a contested battle space that offers citizens a way to participate and make a difference on this battlefront.

OYS branded its war effort with icons, slogans, and graphics as different military units might do in the form of patches and posters. OYS has its own graphic (Figure 2) that participants are encouraged to circulate to their readership to publicize its efforts and identify supporters. A different graphic is used to designate membership in the SC (Figure 3). Through the circulation of digital insignia, OYS brands their cause, which functions to establish public communications and recruit users. In May 2008, OYS "unveiled their latest weapon in the fight against YouTube terrorists"—Jihadi SMACKDOWN of the day, an RSS feed that runs a banner with a link to a new jihadi video that needs flagging each day to make it even easier for members to participate in OYS.[14] By September 2008, they added an associated Twitter feed that provides links to videos to flag. "Stop Internet Terrorists," one of the SC members, hosted a graphic of Uncle Sam pointing out toward the reader to invite them to join the fight against Internet terrorists. The backdrop is the New York City skyline with the World Trade Center still standing and the American flag waving behind him (Figure 4). This message implies that you—the civilian sitting at your computer screen—can fight Internet terrorists along with the military. In adopting some of the military's organizational and symbolic terms and imagery to brand their war effort, OYS is further blurring the lines between military and civilian domains.

---

[12]http://www.webcitation.org/query?url=http%3A%2F%2Fthemiddleground.blogspot.com%2F2007%2F08%2Finformation-war-internet-videos-and.html&date=2010-05-28

[13]http://www.webcitation.org/query?url=http%3A%2F%2Fthemiddleground.blogspot.com%2F2007%2F08%2Finformation-war-internet-videos-and.html&date=2010-05-28

[14]http://www.webcitation.org/query?url=http%3A%2F%2Fmuninn-quotheraven.blogspot.com%2F2008%2F05%2Funleashing-new-weapon-against-cyber.html&date=2010-05-28

Figure 2. OYS's insignia.

Figure 3. SC's insignia.

Figure 4. Header graphic for "Stop Internet Terrorists."

The primary way that OYS evaluates its influence on the YouTube battlefield is by tallying the number of its flagged videos and accounts that disappear from the YouTube platform. For example, OYS reported 40,000 terrorist-supporting videos removed in September 2009. OYS kept track and tallied these "smackdowns," as a military commander might have tracked and tallied the destruction of enemy groups or sites. SC members created graphics that depict their achievements, including one showing the total number of video smackdowns (Figure 5), another representing each successful account suspension, using a noose with an *S* inside for smackdown, and another representing every 25 smacked-down videos, using a larger bomber, again with an *S* inside (Figures 6 and 7).[15] These symbols and statistics were a source of pride and motivation for participants and created milestones of achievement for the network army. As data visualizations they were enrolled to technically and symbolically challenge both the Internet terrorists and YouTube.

[15]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.freerepublic.com%2Ffocus%2Ff-news%2F2142695%2Fposts&date=2010-05-30

Figure 5. OYS graphic showing the tally of videos removed.

Figure 6. Graphic for a suspended account; the "S" means Smackdown.

Figure 7. Graphic for 25 videos smacked down; the "S" means Smackdown.

Another way that OYS evaluates their influence is through the public communication and negotiation among competing network armies. The battles of a network army only conclude when one side or the other announces publicly that it has given up (Hunter, 2002, p. 82). OYS claimed a victory of this kind in December 2008, when a member of an Al Qaeda terrorist forum called Al Falojah admitted that it had been defeated on YouTube by OYS (Figure 1). After discovering this posting by using Google Translator to decode the Arabic on the forum, one of the SC members posted the partial translation and celebrated what they called a "victory" for OYS.

Evaluating Video Smackdowns

With YouTube as an intermediary, there is no documented link between the tactics of OYS and the removal of these videos other than what OYS has tracked themselves. It is difficult to fully ascertain the nature of OYS's influence in shaping these wartime information flows across convergent domains on YouTube. OYS employs wartime rhetoric to evaluate and represent their progress in fighting Internet terrorists. These self-evaluative claims linking the removal of insurgent videos from the YouTube platform to disrupting insurgent wartime operations must be qualified and contextualized by considering the meanings and functionalities of the videos that insurgents are disseminating. Insurgent groups are using the Web to reach multiple audiences with videos that have more than one rhetorical purpose (Dauber, 2009). Dauber develops a typology of videos produced by the "modern day terrorist" (p. 26), which contains seven categories and suggests their associated functionalities.[16] The seven categories of videos are: (a) heavily produced, (b) hostage, (c) statement, (d) tribute, (e) internal training and instructional, (f) last will and testament, and (g) operational (ibid.). The functionalities associated with these videos include propaganda, recruiting, fundraising, media attention, amplifying the psychological and political impacts of an operation, making threats, claiming responsibility for attacks, training, honoring those who died for the cause, and cultivating sympathy across broad audiences (ibid.). While it is not in the scope of this study to perform an in-depth analysis of each flagged video, it is possible, using this typology, to determine the general range of functions of these videos that may be disrupted or impaired when they are removed.

Although OYS doesn't use the refined language that Dauber (2009) uses, they do explicitly call for the flagging of particular types of videos that fall within the categories that Dauber presents. OYS calls for the flagging of "actionable" videos, which they characterize as containing "graphic violence," "sniper/Juba videos," "bomb-making footage," or "executions."[17] OYS and supporting sites also call for the flagging of "IED videos," "hate speech" (toward Coalition soldiers),[18] "martyr videos,"[19] "terrorism

[16] This is based, in part, on the typology in Ben Venzke, "Jihadi Master Video Guide, JMVG) Vol. 1.1" May 18, 2006, Intel Center, Alexandria, VA. Available at *www.intelcenter.com/JMVG-V1-1.pdf*

[17]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.smackdowncorps.com%2Fsubmit.html&date=2011-02-21

[18]http://www.webcitation.org/query?url=http%3A%2F%2Fmuninn-quotheraven.blogspot.com%2F2007%2F07%2Farguing-principle.html&date=2011-02-22

speeches," or "videos of American soldiers and innocent Iraqis being killed."[20] These categories are not mutually exclusive and they do not represent an exhaustive list of all the types of videos that OYS aims to remove. However, they do represent the range of video categories that OYS explicitly encourages participants to flag. This range of flagging categories corresponds to all seven video categories in Dauber's (2009) typology. If OYS's video flagging categories correspond with those of Dauber, then when the videos in these categories are flagged, it is likely that their removal will impact the associated functionalities that correspond to the particular categories of videos being removed. It is possible that insurgent operations were disrupted momentarily before they migrated to a new platform to continue their operations elsewhere. However, given that YouTube provides a very broad audience, as compared to targeted forums, it is probable that the functionalities of videos aimed at broader audiences will be relatively more impaired than will others. These categories of videos aimed at broader audiences include those that are heavily produced, statement, and operational, which are also the videos that are the most multipurposed in their functionality (Dauber, 2009). When videos are flagged under these categories, there is no guarantee that they will be removed. YouTube's reviewers only decide to remove the video if it violates the community guidelines. Thus, there are many videos that fulfill the criteria for both OYS's flagging categories and Dauber's categories, but that fail to meet the criteria for removal by the YouTube reviewing staff.

Challenging the YouTube Model

This case highlights OYS's shift from targeting Internet terrorists to challenging the YouTube corporation. In attempting to hold the YouTube corporation accountable for its actions, OYS is challenging the sociotechnical protocols that govern the space they aim to defend. OYS claimed success in focusing attention and influencing YouTube's corporate policies. In May 2008, a time when OYS was aggressively challenging YouTube, Senator Lieberman demanded that the company remove the dozens of "jihadist" videos from the site (Rosen, 2008). YouTube maintained that they examine flagged videos and remove the ones that violate their community guidelines. Many of the videos that concerned Lieberman did not violate their community guidelines and were not removed (YouTube Team, 2008). In the exchanges that followed, YouTube defended itself against Lieberman's request by asserting its commitment to uphold free speech. However, in September 2008, shortly after the exchanges, YouTube announced new guidelines prohibiting videos "intended to incite violence" (Rosen, 2008) as noted in Figure 1.[21] This adjustment in the community guidelines allowed YouTube's reviewers to remove more of the jihadist videos without

---

[19]http://www.webcitation.org/query?url=http%3A%2F%2Fcreepingsharia.wordpress.com%2F2009%2F06%2F12%2Fhelp-fight-the-cyber-jihad-join-the-jihadi-smackdown-corps%2F&date=2011-02-22

[20]http://www.webcitation.org/query?url=http%3A%2F%2Fwww.facebook.com%2Fgroup.php%3Fgid%3D4108104233%26v%3Dinfo&date=2011-02-22

[21] Compare YouTube's community guidelines.

http://web.archive.org/web/20080611231521/http://www.youtube.com/t/community_guidelines

http://www.webcitation.org/query?url=http%3A%2F%2Fwww.youtube.com%2Ft%2Fcommunity_guidelines%3Fhl%3Den&date=2010-05-29

violating those community guidelines and encouraged users to flag videos that met the criteria. OYS was coacting with the state to try to influence YouTube to change its policies to ensure it was not supporting terrorist activity. It is difficult to know how YouTube actually made the decision and therefore difficult to evaluate how much influence OYS or Senator Lieberman had on the outcome. Still, it is evident that both played a role in bringing these issues to YouTube's attention and thus were part of the coproduction of new regulation around these issues.

Conclusions

YouTube users are experiencing the ease of access to the means of participation and the potential for real-time engagement across dispersed wartime networks that seem to render geography irrelevant. In the case of OYS, a decentralized network of civilians bypassed the traditional mass media and state institutions to more immediately and directly engage in the convergent spaces of wartime mediation. OYS was operating outside the bounds of the U.S. military, media, or any other state-authorized activity. The cyber counter terrorism efforts were not unlike those of the Cyber Minutemen employed to secure national borders, cyber-borders against terrorists. Frustrated by the lack of vigilance and monitoring on the YouTube front by the state or by Google, they decided to take matters into their own hands. In their effort to eliminate Internet terrorists, their operations supplemented state and military aims. OYS's strategy and tactics reshaped conventional boundaries between offense and defense, civilian and military, state and society, as well as between user and platform provider (Arquilla & Ronfeldt, 2001, p. 14).

The YouTube platform provided a communicative context in which the technical and symbolic means of coproduction are convergent. OYS operated on both symbolic and technical levels to re-engineer not only the information flows but also the mediating and governing protocols of the YouTube platform. Yet YouTube's powerful role as gatekeeper reveals a relationship between user and platform provider in which the user, while able to exploit and challenge certain aspects of the platform architecture and policy, is still constrained by their dependency on YouTube as the provider of the platform. Tracing the associated Web of OYS demonstrated some of the affordances and constraints of the YouTube platform as a venue for UGW and the contributions of particular coproductive relationships. YouTube's corporate operations have challenges of unwieldy volumes of videos to monitor, competing ideas about the interpretation of community guidelines, and the potential for users to repost the video in different locations, in different languages, and with different user names. Positioned as the intermediary decision maker, the YouTube corporation ultimately has the power to interpret and apply its own community guidelines, which may differ from its users' contested visions for a proper public space. It is clear that UGC is not fully in the hands of the users, but rather it is coproduced via corporate-owned platforms whose contours must be examined in light of the sociotechnical relationships among the corporate actors, terms of service, community guidelines, and the Web architecture.

User agency, as defined in relationship to the platform as a sociotechnical ensemble, also plays a significant role in shaping the information flows of UGW. As illustrated through the tracing of OYS tactics, individual users collectively mobilized the generative features of coproductive regulation and the network organizational form as the instrumental means to reshaping and defending the wartime information flows on YouTube. YouTube's model relies heavily on users, spanning geographies and ideologies, to coproduce

regulation via YouTube's platform features. Thus, the potential for the user-generated contribution to counterbalance and regulate all the UGC uploaded to the site depends in large part on the levels of participation from the users. The degree of user participation varies greatly across the growing YouTube user population, with a majority of users only engaging on the level of passive viewing (Madden, 2007). This means that there is significant unrealized potential for user participation to more effectively enforce the community guidelines. The limitations of coproduced regulation emerge as the user community and YouTube fall short of fully and consistently enforcing these community guidelines for every video posted.

The evidence suggests that the relative efficacy of OYS in getting terrorist-supporting videos removed may have partially thwarted the aims of the insurgent groups by impairing the functionalities of their videos on YouTube or forcing them to migrate to other platforms. While insurgents may choose to migrate to other video sharing and social media platforms, such as Web forums, Liveleak, Facebook, and Twitter (Dauber, 2009, p. 4), the YouTube platform offers the insurgents a uniquely broad audience, which is the target audience for particular categories of videos (Dauber, 2009). Since YouTube is only one venue for wartime actors to exercise their networking power to win people's minds, more work needs to be done to further contextualize the tactics observed in this case study within the wider Web of information operations. To know more about how the functionalities of the removed videos were impaired or disrupted, future researchers should study the migration patterns of Internet terrorists to other platforms and track the circulation of videos beyond the YouTube platform. Studying the interactions and practices on the Internet is inherently partial, as the researcher can see only what is made public or presented online. There are offline components, private online interactions, and interactions on different platforms that could be relevant to the phenomena studied here, but that this article is not able to address. For the purposes of this research, it was sufficient to limit myself to observing the phenomena on the Web and through Web-based communication around YouTube. As with most Internet research, challenges emerge when trying to represent a case or analyze specific practices in the context of the constantly evolving and dynamic network landscape. This may limit the application and credibility of a research claim to a specific moment in time.

The U.S. military, civilian, and insurgent groups are taking seriously their presence on YouTube as an important part of how war is conducted in the information age. As UGW emerges on YouTube, it needs to be investigated not solely as mediations of war but also as actions and operations of war (Keenan, 2002). The YouTube platform itself becomes a territory that wartime actors seek to dominate and defend, providing adjunct spaces to the Iraq War and the GWOT that need to be studied further as such. As civilian, military, media, entertainment, and insurgent networks engage on the same Web platform, using the same tools and tactics for different ends, it becomes all the more challenging to distinguish among these means. UGW helps to locate these convergences in a particular space by making visible the coproductive relationships between users, platforms, and the platform provider.

As a sociotechnical ensemble, the YouTube platform affords and constrains user-generated network activity in particular ways that become the basis for the tactics employed in UGW. This suggests a trend in platform-based netwars that might look very different from each other depending on the sociotechnical ensemble governing the platform, such as the owner's policies, protocols for enforcing their policies in these situations, and the affordances and constraints of the Web architecture. For example, when Facebook was notified that they were hosting the material of a jihadist group, the page was shut down immediately (Mowbray, 2008), which differs from how Google handled similar situations. It is

possible that the irrelevant geography that has allowed for the convergence of military, insurgent, media, and civilian operations on the same Web platform may become relevant again in the form of platform contours, in which platform owners become visible actors and the sociotechnical infrastructure of a given platform begins to distinguish one conflict from another.

References

Anden-Papadopoulos, K. (2009). U.S. soldiers imaging the Iraq War on YouTube. *Popular Communication*, *7*(1), 17–27.

Arquilla, J., & Ronfeldt, D. F. (1997). The advent of netwar. In J. Arquilla & D. F. Ronfeldt (Eds.), *In Athena's camp: Preparing for conflict in the information age* (pp. 275–294). Santa Monica, CA: Rand.

Arquilla, J., & Ronfeldt, D. F. (2001). The advent of netwar (revisited). In J. Arquilla & D. F. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 1–25). Santa Monica, CA: Rand.

Benkler, Y. (2006). *The wealth of networks*. New Haven, CT: Yale University Press.

Bennett, W. (2003). Communicating global activism. *Information, Communication & Society*, *6*(2), 143–168.

Bijker, W. E. (1995). *Of bicycles, bakelites, and bulbs: Toward a theory of sociotechnical change*. Cambridge, MA: MIT Press.

Bimber, B., Flanagin, A. J., & Stohl, C. (2005). Reconceptualizing collective action in the contemporary media environment. *Communication Theory*, *15*(4), 365–388.

Bimber, B., Stohl, C., & Flanagin, A. J. (2009). Technological change and the shifting nature of political organization. In A. Chadwick & P. N. Howard (Eds.), *Routledge Handbook of Internet Politics* (pp. 72–85). London: Routledge.

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

Burgess, J. E., & Green, J. B. (2008). *Agency and controversy in the YouTube community.* Paper presented at the Association of Internet Researchers (AoIR) Conference, IT University of Copenhagen, Denmark.

Castells, M. (1996). *The rise of the network society*. Cambridge, MA: Blackwell Publishers.

Castells, M. (2001). Informationalism and the network society. In P. Himanen (Ed.), *The hacker ethic, and the spirit of the information age* (pp. 155–178). New York: Random House.

Castells, M. (2009). *Communication power*. New York: Oxford University Press.

Chadwick, A. (2007). Digital network repertoires and organizational hybridity. *Political Communication*, *24*(3), 283–301.

Chadwick, A., & Howard, P. (Eds.).(2009). *Routledge handbook of Internet politics*. London: Routledge.

Dauber, C. E. (2009, November 16). YouTube war: Fighting in a world of cameras in every cell phone and photoshop on every computer. Retrieved from http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?PubID=951

Deibert, R., & Rohozinski, R. (2010). Liberation vs. control:The future of cyberspace. *J. Democr. Journal of Democracy*, *21*(4), 43–57.

Der Derian, J. (2009). *Virtuous war: Mapping the military-industrial-media-entertainment network*. New York: Routledge.

Foot, K. A., & Schneider, S. M. (2006). *Web campaigning*. Cambridge, MA: MIT Press.

Gillespie, T. (2010). The politics of platforms. *New Media & Society*, *12*(3), 347–364. doi: 10.1177/1461444809342738

Graham, S. (2010). Combat zones that see: Urban warfare and U.S. military technology. In F. MacDonald, R. Hughes, & K. Dodds (Eds.), *Observant states: Geopolitics and visual culture*, pp. 199–223. London: I. B. Tauris.

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

Howe, J. (2006). The rise of crowdsourcing. *Wired*, *14*(6). Retrieved from http://www.wired.com/wired/archive/14.06/crowds.html

Hunter, R. (2002). *World without secrets: Business, crime, and privacy in the age of ubiquitous computing*. New York: J. Wiley.

Jenkins, H. (2006). *Convergence culture: Where old and new media collide*. New York: New York University Press.

Jordan, E. (2007). U.S. dominates new front in Iraq War: YouTube. *Iraq Slogger*. Retrieved from http://www.iraqslogger.com

Keenan, T. (2002). Publicity and indifference: Media, surveillance, humanitarian intervention. In T. Y. Levin, U. Frohne, P. Weibel, & K. Zentrum. für Kunst und Medientechnologie (Eds.), *Rhetorics of Surveillance from Bentham to Big Brother* (pp. 544–561). Karlsruhe, Germany; Cambridge, MA: ZKM Center for Art and Media; MIT Press.

Lawson, S., & Gehl, R. W. (2011). *Convergence security: Cyber-surveillance and the biopolitical production of security* Paper presented at the Cyber-Surveillance in Everyday Life, An International Workshop, University of Toronto, Canada.

Madden, M. (2007). Online video. *Pew Internet and American Life Project*. Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Online_Video_2007.pdf.pdf

Mowbray, J. (2008). Jihadist group trying to invade Facebook gets shutdown. *Fox News*. Retrieved from http://www.foxnews.com/story/0,2933,470385,00.html

Postigo, H. (2003). Emerging sources of labor on the Internet: The case of America online volunteers. *International Review of Social History*, *48*(Supplement), 205–223.

Postigo, H. (2009). America online volunteers. *International Journal of Cultural Studies*, *12*(5), 451–469.

Raley, R. (2009). *Tactical media*. Minneapolis: University of Minnesota Press.

Rheingold, H. (2003). *Smart mobs: The next social revolution*. Cambridge, MA: Perseus Publishing.

Ronfeldt, D., & Arquilla, J. (2001). Networks, netwars and the fight for the future. *First Monday*, *6*(10). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/889/798

Rosen, J. (2008, November 30). Google's gatekeepers. *The New York Times Magazine*, Retrieved from http://www.nytimes.com/2008/11/30/magazine/30google-t.html?pagewanted=all

Rumsfeld, D. (2006). New realities in the media age: A conversation with Donald Rumsfeld. *Council on Foreign Relations*. Retrieved from http://www.cfr.org/publication/9900

YouTube Team (2008). Dialogue with Sen. Lieberman on terrorism videos. *Broadcasting ourselves: The YouTube blog*. Retrieved from http://googlepublicpolicy.blogspot.com/2008/05/dialogue-with-sen-lieberman-on.html

Terranova, T. (2000). Free labor: Producing culture for the digital economy. *Social Text*, *18*(2), 33–58.

van Dijck, J. (2009). Users like you? Theorizing agency in user-generated content. *Media Culture Society*, *31*(1), 41–58. doi: 10.1177/0163443708098245

Weimann, G. (2006a). *Terror on the Internet: The new arena, the new challenges*. Washington, DC: United States Institute of Peace Press.

Weimann, G. (2006b). Virtual disputes: The use of the Internet for terrorist debates. *Studies in Conflict and Terrorism*, *29*(7), 623–639.

Weimann, G., & Winn, C. (1994). *The theater of terror: Mass media and international terrorism*. New York: Longman.

Zittrain, J. (2008). *The future of the Internet and how to stop it*. New Haven, CT: Yale University Press.