SOCIAL MEDIA in CONFLICT

Comparing Military and Social-Movement Technocultures

Chris Hables Gray and Ángel J. Gordo

Abstract **There are important differences in how information technology is used in military and social-movement cultures. Militaries use social media in the Human Terrain model and security-police mode for quantifying and controlling social space, in order to meet low-intensity, counterinsurgency, and regime-maintenance goals (or for recruitment and public relations). For social-movement cultures, such as secular Egyptian revolutionaries, 15M (Los Indignados), and Idle No More, social media is an integral part of life; it is context. Unlike these horizontalist movements, military institutions are based on a hierarchical structure that precludes social media from becoming part of their organizational and decision-making culture. For them, social media constitute part of civil society, a commons both virtual and physical. The synergy between computer networks and decentralized social movements is clear when military, social-movement, and network theories and practices are compared. These differences are manifested in asymmetrical relationships to "veillance," alternative modes of producing social technologies (especially protocols), contrasting theories of power, and opposing conceptions of morality and efficacy. The differences are more than a matter of how the affordances of information technologies match with the different technocultures. Horizontalist social movements incorporate new information technologies into their praxis as self-control, while militaries seek to subsume them into the existing hierarchical control paradigms.**

Keywords **information war; information technologies; affordances; protocols; control**

Cultural Politics, Volume 10, Issue 3, © 2014 Duke University Press
DOI: 10.1215/17432197-2795645

Context: Proliferating Hybrids

Protocol is a solution to the problem of hierarchy. It is in many ways an historical advancement.
—Alexander Galloway, *Protocol*

The April 2013 bombing of the Boston Marathon revealed a great deal about social change and social media. The bombers seem to have recruited themselves through the interweb.[1] After their heinous act, they were identified through crowdsourced analysis of raw big data collected and processed by the US security bureaucracies. Boston was locked down as militarized police squads and armored cars searched for one wounded nineteen-year-old. Once found, he was observed by infrared from a helicopter and then a remote-controlled "robot" pulled back the tarp covering him.

This effective hybrid mobilization of hierarchical and distributed networks was mediated through mass and social media. In some ways, the process was what US military planners hoped the Human Terrain program and other information-based interventions would produce in Afghanistan and Iraq but never did. The US military doesn't have either the culture or the systems architecture necessary for these kinds of successes. For military cultures, heir to thousands of years of orders-from-the-top hierarchies, framed by patriarchal values and a focus on instrumentalist violence, participatory social change is impossible. Still, the US military and its allies have deepened their commitment to C^4I^2 (Command, Control, Communications, Computers, Intelligence, and Interoperability). This infocentric view of war is an integral quality of the current postmodern war system (Gray 1997). But there are many ways to put information at the center of one's worldview.

For armies, information is the power to accomplish specific missions: killing, wounding, capturing, degrading enemy systems, defending, supplying, and so on. A distributed network of semiautonomous interlinked nodes deploys information to enrich itself with connections, processes, possibilities. The flows between the nodes are flexible, and the information they deploy sustains but also reconfigures the network, making it flexible as well.

To understand these new dynamics between organizations, technologies, and politics is to accept the information revolution: "The relationship between humans and information has changed profoundly during the late 20th century; increased accessibility and an explosion in the quantity and quality of information made available to individuals requires new strategies and models to cope with these changes, which threaten to sweep away notions of identity and choice" (Macauley and Gordo-López 1995: 436). This crisis of meaning isn't going away; rather, it is deepening. The institutionalization of innovation established within the military (Van Creveld 1989) is also occurring within civilian technoscience. The perpetual revolution in military affairs that defines postmodern war is matched by a permanent revolution in information technology, producing, among other things, an ongoing revolution in revolutionary political change (Gray 2005).

Officially, the significant militaries of the world have embraced this new information system paradigm. All levels of war are pursued through an informatics lens, be it the artificial intelligence of an Aegis system on a warship or the quantified anthropology of the Human Terrain program to, among other tasks, acquire targeting intelligence for human–machine killer-drone teams. But, in practice, these "updated" militaries have not been able to renounce "force of fire" as the most

important force multiplier and accept that, in contemporary conflicts, information (in the richest sense of the term) is what wins wars (Gray 1997, 2005).

Hearts and minds are not won by remote targeted killing. Yet that is what US strategy (not just tactics) has been reduced to in Afghanistan and Pakistan, in Iraq, and in Somalia. Cultural understanding has been reduced to masses of data on the Human Terrain. Social media is deployed for recruitment and propaganda, but with the exception of a few "sock puppets,"[2] the only innovative roles are for massive (sometimes even crowdsourced) surveillance and for the perfection of drones as a killing system.

Cyberspace has been the newest battlespace (Morello 2007) since the early 1990s, when the Zapatistas used the young Internet to mobilize civil society in order to keep the Mexican government from exterminating them. But it is hard to fit this battlespace into traditional military forms. Where it overlaps with older tactical and strategic areas (intelligence, sabotage, propaganda, logistics, weapons systems), information technology has been deployed efficiently, but in the sense that cyberspace changes war itself, the established militaries cannot adapt. They can craft concepts such as "information war," "cyber war," and "net war," but they cannot win these struggles. As Elaine Scarry (1987) proves in her masterful *The Body in Pain*, war is about changing human perceptions of reality through violence. The incredible power of new military technologies ended the possibility of total war, and decisive battle is impossible, as well, because social media is outpacing the ability of violence to change human perceptions of reality. It isn't just that war is an extension of politics, or even that, today, to paraphrase Michel Foucault's bon mot, politics often seems an extension of war, as in the Cold War and its little brother, the Terror War (Gray 1997, 2005); rather, it has become clear that "technology is politics by other means" because "social life is technologically mediated constantly and without interruption" (Sádaba and Gordo 2008: 10).

Violence is still powerful, of course. It can terrorize some people into agreement or silence, it can destroy people and render their perceptions of reality into nothingness, and it can enforce rules, even laws, that shape technologies (even social media) to the interests of the rich, the powerful, and the guilty. But this is negative power. The power to create new possibilities is something else. To explain why waves of protests, socially mediated by technology, are sweeping the world, while the most powerful armies grow weaker, requires a close analysis of contemporary social movements and militaries, as well as the codes and protocols of sociotechnical systems, including the latest social media: drones.

Technosocial Mediation

> Protocol is how control exists after distribution achieves hegemony as a formal diagram. It is etiquette for autonomous agents. It is the chivalry of the object.
> —Alexander Galloway, *Protocol*

The main function of computers is social. Even when they focus on big data, they do so in the service of selling to, monitoring, serving, killing, or in some way communicating with, and for, humans. But as computers have become ubiquitous, converging into one thick interweb, we have come to call the nodes and interfaces that are dedicated to one-to-one and one-to-many sociality *social media*, in contrast to the institutionalized broadcasts (to the many) of *mass media*. Mass media is often defined as "push" media, in that

it is pushed at us, while social media is accessed when we "pull" it by choice, with the option (because of interconnectivity) of contributing ourselves. As Manuel Castells (2009) has argued, this has produced a transformation of sociability itself.

Facebook, YouTube, Twitter, and other platforms have joined e-mails, blogs, and web pages as modes for the proliferation of social connectivity. As Esther Dyson (2012) points out, social media "changes the balance of power between individuals and institutions." Contemporary social movements don't just use social media; it is a crucial part of their milieu, their context. In some cases, the movements only exist through social media (e.g., Anonymous, WikiLeaks).

Because the first digital social media to fundamentally change society have been virtual, we forget that much human sociality is physical. To extend that physicality through technology is still social. Since drones, teleoperated or remotely piloted vehicles, are extensions of the user physically, they, too, are social media. Lev Grossman explains: "A drone isn't just a tool; when you use it you see and act through it—you inhabit it. It expands the reach of your body and senses in much the same way the internet expands your mind. The net extends our virtual presence; drones extend our physical presence . . . one of a handful of genuinely transformative technologies to emerge in the last 10 years" (2013: 28). Drone technology isn't just a tool, a machine with a program. Similar to other social media, it constitutes a relationship between humans and machines. But while Facebook and the like are natural-to-use extensions of our friendships and working relationships, drones are disturbing. Grossman notes: "There is something uncanny about drones. . . . It's roughly analogous to interacting with an anonymous contributor on a blog. You're dealing with someone who is both present and absent, who has decided that what they say or do will have consequences for you but not for them. Drones bring that asymmetrical dynamic out into the real world: a drone is the physical avatar of the virtual presence of a real person" (2013: 31). As drones proliferate in type and influence throughout culture, in the same way that social media has, we'll need to differentiate their extension of physicality from the projection of personality that is "traditional" social media.

Both drone and interweb technology have military origins. But as the Internet was distributed, it grew out-of-control, so the Pentagon handed it off to the National Science Foundation, which couldn't control it, either. Meanwhile, the military had to create their own MILNET (Military Network). Drones have stayed closer to their military origins. The Royal Air Force perfected target drones after World War I when a radio-controlled flight system, out of a Fairey scout 111 manned aircraft ("Queen"), was put into a De Havilland Gipsy Moth. Later, an improved target aircraft was called "Queen Bee." At this point, the term *drone* was first used (Jarnot 2012: 6). Clearly, the reference was, in part, to drone bees, but with an added implication of impotence, as drones can't sting and targets can't shoot back.

But drones can kill now. This has led to an extensive academic, and even popular, debate around the ethics of "killer robots," but, obviously, drones are not robots, just extraordinary human extensions. Extraordinary but ineffective. Drones are the latest military information technology breakthrough that fails to deliver strategic success. This is the pattern of postmodern war.

Drones and the Human Terrain

By design, protocols such as the Internet Protocol cannot be centralized.
—Alexander Galloway, *Protocol*

The central contradiction of postmodern war is that the most powerful weapons cannot be used. This contradiction produced the strange "conflicted" world of the Cold War and its successor, the Terror War. The first great military product of the computer age was the hydrogen bomb. Then came the "electronic battlefield" of Vietnam, which ended in a US defeat despite the computerization of everything from targeting to body counts (Gray 1997). The Soviet military lost in Afghanistan even as it embraced the same principles as the US military, which repeated the story there and in Iraq (Gray 2005).

Yet, while the approach failed and is losing the Pakistan war before it even starts, information technoscience has been taken to new levels with the rise of the drones (now used more than "manned" aircraft) and the quest for "total battlefield awareness," as in the Human Terrain program. Military drones have become a central part of the current hybrid (digital and embodied) battlespace, even though their military efficacy is suspect. They also raise significant political and ethical issues, as exemplified by President Obama's claim that they can be used to execute US citizens. Military exploitation of social media seems equally problematic.

There are the sock puppet programs, part of the unironically named Operation Earnest Voice (OEV). The US military has bought "false online personalities" for fifty operators ("online persona management"). General James Mattis told the US Senate that OEV "supports all activities associated with degrading the enemy narrative, including web engagement and web-based product distribution capabilities." Jeff Jarvis, who broke the story, says "Washington shows the morals of a clumsy spammer" (Jarvis 2011).

Defense giant Raytheon used what it has called "extreme-scale analytics" to create RIOT (Rapid Information Overlay Technology), which mines social media to predict behavior. A great tool for marketers, it also was used in 2010, according to Ryan Gallaher, "to help build a national security system capable of analyzing 'trillions of entities' from cyberspace," not just for searching, but also "as a means of monitoring and control." It allows for constructing a digital doppelgänger of someone, including social, economic, and political information, as well as a map of their key locations (Gallaher 2013). These technologies mobilize information and algorithms for control from above, much like the Human Terrain program does—although the latter collects information through anthropologists, since the Afghans and Iraqis aren't so established in social media. But, while these programs mine distributed networks for data, the use of the data is centralized.

Why this inability to fully mobilize in distributed networks? Because military culture is committed to hierarchy. Decentralized networks can work in military culture, as al Qaeda (the Base) has demonstrated. But truly distributing power (to judge and originate ideas) cannot coexist with military chains of command. The controversy surrounding Bradley Manning is a fine example. Manning disobeyed orders and sent massive amounts of information to WikiLeaks, the antithesis of MILNET, from which Manning mined the information. That information was collected through observing from above—surveillance—but was transformed by the alchemy of

WikiLeaks to observation from below—sousveillance. As Steve Mann (2013) has shown, in coining the term *sousveillance*, and by revealing the importance of our technologically proliferating gazes, "veillance" is now a fundamental aspect of contemporary culture. Sousveillance threatens informational monopolies.

After the Vietnam War syndrome was recognized, the US military began to make the case that the domestic information economy was the most important "front" of all (Gray 1997). As a result, the US government has felt compelled to pursue social engineering of an authoritarian kind, as in President Obama's "unprecedented war" on whistleblowers (Van Buren 2012). At the beginning of 2013, the Pentagon announced it was expanding its Cyber Command fivefold, adding four thousand people (Greenwald 2013). This initiative fits well with the recent expansion of social-media monitoring (and other big-data collecting and analyzing) by the National Security Agency (NSA). The NSA (led by General Keith Alexander, who also heads Cyber Command) not only built a domestic network of regional centers and domestic listening posts but is also building the world's most powerful spy center in Utah (Bamford 2012). In a *Washington Post* editorial advocating this expansion, Vice Admiral Mike McConnell (former Director of National Intelligence) argued that the United States needs "to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic, military and legal options—and we must be able to do this in milliseconds. More specifically, we need to reengineer the Internet to make attribution, geolocation, intelligence analysis and impact assessment—who did it, from where, why and what was the result—more manageable" (McConnell 2010). Of course, easier said than done. Many active users have a different vision than Admiral McConnell has, not just for the interweb but for society.

Socially Mediated Movements

> It is through protocol that one must guide one's efforts, not against it.
> —Alexander Galloway, *Protocol*

Founded through Facebook by four women in Canada, Idle No More became a worldwide movement in two months (Bernd 2013). It "has been driven by social media, a place where anyone can participate in discussion and follow news if they have an Internet connection or smartphone" (Donkin 2013). Idle No More is only the latest movement to use digital technology integrally. In many ways, labels such as Arab Spring, Occupy, Los Indignados, and Idle No More don't mark new movements so much as current incarnations of ongoing resistance cultures that social media is revitalizing in new and more potent ways.

The spark that started the Arab Spring was the protest suicide of Mohamed Bouazizi, a Tunisian street vendor the police forced out of business for insufficient bribery. His sacrifice sparked a conflagration. Social media played an important role in shaping the understandings (the fuel) of the Tunisian revolutionaries, and it was even more important as revolution spread to Egypt (catalyzed by the police murder of a blogger) and beyond.

Early on, Anonymous launched Operation Tunisia. It included denial-of-service attacks on government websites and a care packet, in Arabic and French, on identity concealment for cyber dissidents. A Greasemonkey script was written to "help Tunisians evade an extensive phishing

campaign carried out by the government" (Ryan 2011). Anonymous was not alone. Among the important cybergroups catalyzing the Arab Spring are Avaaz, Telecomix, Witness, Herdict, OpenNet Initiative, and the Open Mesh Project.

The ongoing Egyptian revolution is a good model for the role of social media in extreme social change. While it came together, in part, through Facebook and other social technologies, it only succeeded because of its strength in the streets and its sophistication about technology. For example, while eighty-five thousand people signed up on Facebook for the January 25 protests that began the revolution, the actual organizing for that day was by word of mouth, because the protesters had learned that the Egyptian military had purchased, from the German military, a full "cracking" package that allowed total access to e-mails, web pages, Facebook accounts, and Twitter feeds (Salah 2011). So, in the days leading up to January 25, false information was planted across the interweb.

By the time the revolutionaries had seized Tahrir (Cairo's heart) and the Egyptian government blocked Egypt's telecommunications, it was too late. The shutdown only provoked people to go out in the streets to see their friends and to find out what was going on. Just as important, Al Jazeera TV, which could not be cut off, was showing such atrocities as the Battle of the Camels.

Los Indignados in Spain began crystalizing in February 2011 when the group No les Votes formed online to urge abstention on a law to tax culture and defend corporate copyrights. The national initiative Revolución Ciudadana Espontánea also began then. Its principles included peaceful street protests, rejecting the two-party system through participatory democracy, governance by assembly, and unity around human rights and a decent life ("*una protesta de tod@s por todo*"). The very similar Estado del Malestar also started in February.

This wave of new collectives, groups, movements, metamovements, and other initiatives took place both physically and virtually. The most important was the Plataforma de Coordinación de Grupos Pro-Movilización Ciudadana, which brought together Anonymous, ADESORG (Asociación Nacional de Desempleados), Ponte en Pie, Juventud en Acción, and others to organize a demonstration in Madrid against voting for the Socialist party. Then it called for major demonstrations across Spain for May 15, under the slogan *"¡Democracia Real Ya!"*

Social media is integral to this organizing. Coordinating collectives emerged in different cities linked mainly through Facebook. At the grassroots, institutions such as Medialabs (temporarily autonomous spaces) and Autonomous Social Centres (from the autonomous and squatting movements), like Tabacalera, Patio Maravillas, and Casablanca in Madrid and Kukutza in País Vasco, played a major role. Besides the N-1 social network, the main technodimension of the movement is the 15hack platform, an open-code space (Moreno-Caballud 2013).

A full mapping of these new political-technical developments is impossible because, in a sort of Heisenberg Uncertainty Principle of political change, noticing and using them promulgates more of them. Connections between the technical and the political are clear at a deeper level, in shared ideas of the commons (Benkler 2006; Holmes 2007; Estalella, Rocha, and Lafuente 2013), open-source distributed network processes, rhizomes, DIY/DIT (do-it-yourself/do-it-together) citizenship (Boler 2008), augmediated

participation (Bauwens 2012), maktivism (Mann 2014), and veillance (Mann 2013). In many respects, it comes down to nonhierarchical governance (Internet protocols, crowdsourcing, the mass meetings of the Arab Spring, Los Indignados, and Occupy) and in shared groups and techs (Anonymous, WikiLeaks, Ushahidi, and Open Mesh, among many others). As Paul Mason notes: "Once information networks become social, the implications are massive: truth can now travel faster than lies, and all propaganda becomes instantly flammable. . . . Whereas the basic form of, say, a Leninist party, a guerrilla army or even a ghetto riot has not changed in a century, once you use social networks the organizational format of revolt goes into constant flux" (Mason 2012). The form is not separate from the process or the results. Certain networks lend themselves to some processes better than others. Why this is turns out to be very important.

Affordances, Protocols, and Control

Protocol is a circuit, not a sentence.
—Alexander Galloway, *Protocol*

The concept of affordances used in discussions of human-computer interaction derives from the fields of both psychology and design. While there are nuances to both perspectives, as well as others (Soegaard 2010), we use *affordances* here in the sense that objects (including complex networks that are hybrids of the virtual and the physical) ontologically are easier to use in some ways than others by specific users (individuals, groups, or subcultures) because of the options they "afford."

Different affordances in information technologies (in architecture, code, and protocols) match with different technocultures because of their epistemologies. Is knowledge the result of tradition, elites, and formalisms? Or is it the result of innovation, collectivity, and dynamic processes? How one answers this question has clear political implications as well. Contemporary horizontalist social movements incorporate new social technologies into their praxis, in order to change society, while militaries seek to conserve the current system.

Human culture has structures. Information, energy, and matter flow through human society along established lines. But it is messy. Marriage and property and power rules and rituals are sustained only through human acceptance. Information flows through formal computer networks, as well, but even though they grow, and grow together, and change continually, they are sustained by more than belief. They are instantiated in machines and code and organized by protocols.

MILNET is formal and hierarchical. This is true of most intranets (internal networks), although some are decentralized. A decentralized network does not have one hierarchy; it has multiple trees or other forms linked together in a metahierarchy. A distributed network has no top, no center. It may contain smaller hierarchical nodes, but its overall form is of a mesh. This is the worldwide interweb. Facilitated by open committees of experts who set the intercommunication standards, the interweb has evoked a widely shared ethos, articulated in the 1997 "One Planet, One Net" manifesto of Computer Professionals for Social Responsibility (CPSR). It declared that "there is only one net" that should be available to all, and we are its stewards, not owners. No "individuals, organizations, or governments should dominate," and it "should reflect human diversity, not homogenize it" (CPSR 1997). People have a right to communicate and to privacy.

These values don't come from hardware or software. They are political

principles. In 1973, Colin Ward published *Anarchy in Action*, where he argued that liberation emerged from principles such as "spontaneous order" and "harmony through complexity" (Ward 1973). The next year, Ted Nelson's *Computer Lib/Dream Machines* came out, claiming that computers could foster similar principles in society. Since then, there has been a proliferation of principles, processes, and even products that link antiauthoritarian social movements and cutting-edge computing.

Kevin Kelly (1995) echoes Ward when explaining how systems out of external control (weather, economies) regulate themselves. They are distributed with autonomous subunits and high connectivity. But distributed systems are not automatically democratic.In *Code*, Lawrence Lessig (1999) points out that the Internet is not immune to corruption and even to appropriations that would change it from an open to a closed system. Lessig argues that a state is necessary to keep the web free through "self-conscious control."[3] But collective consciousness doesn't require states, just community. It can be built into the code, in terms of the law Lessig prioritizes and, more importantly, in the protocols (technical rules and standards) of the systems, as Alexander Galloway (2004) contends. The basic processes of self-control in systems (feedback, self-reference, homeostasis, checks and balances, distributed power) are the most scalable, the most prolific, and the best creators of new emergent properties.

Insightful as Galloway is, he errs by misunderstanding control. His claim that "the Internet is the most highly controlled mass media hitherto known" (2004: 243) is true enough, but only because the control is homeostatic; it is self-governance. Lessig's view includes "content" as a major factor in a network, while Galloway proudly "makes no allowances for special anthropomorphic uses of data" (Galloway 2004: 40). This is a major gap in understanding the potential of hybrid distributed systems, for humans decide how they are used. This can be done consciously (open-source) with the creation of protocols that serve specific values.

Although, to be fair, as governance, this process is unusual for humans (but not for bees). It isn't "self" control, but collective control, in the truest sense, which means that often individuals don't get their way. Such distributed systems won't necessarily make the best decisions, but they might. Group decisions are usually better than hierarchical choices, and they are indeed "dangerous" to the powers that be (Galloway 2004: 16).

Our anthrocentric choices about data use are crucial, after all. But those choices are not the only ones. The most important choice is of epistemology: open or closed? Closed epistemologies don't mesh well with open systems; closed systems provoke responses from open epistemologies. The spread of surveillance produced a wave of sousveillance that, far from abating, is becoming ubiquitous (Mann 2013). The same dynamic will shape extension (drone) technoscience. The Federal Aviation Administration predicts that by 2020 there will be thirty thousand civilian drones in the United States (Uberti 2012). It is quite possible that there will be ten times that number. Extensions from "above" will be met with those from below, leading to a society that is saturated by extended physicality, as we now live immersed in veillance and social media.

The traffic goes both ways. As networks are used, they evolve in particular directions. Thomas Hughes (1983) shows how large sociotechnical networks (think power grids) reach a tipping point of technological momentum where one form becomes hegemonic over the others. This

isn't necessarily a worldwide phenomenon. Hughes looked at Soviet and North American power grids that did develop different protocols. But, in the case of the interweb, it will be fundamentally one form: one net for one planet.

Notes

1. The term *interweb* refers to the convergence of the Internet, the web, and mobile social media.
2. The term *sock puppets* refers to invented online fake personas used for false-flag recruitments or for spreading propaganda and disinformation.
3. Lawrence Lessig put *Code* online for crowdsourced editing. The result, *Code: 2.0*, is more balanced.

References

Bamford, James. 2012. "The NSA Is Building the Country's Biggest Spy Center." *Wired*, March 15, www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/.

Bauwens, Michael. 2012. " 'Occupy' as a Business Model: The Emerging Open-Source Civilization." *Al Jazeera*, March 9, www.aljazeera.com/indepth/opinion/2012/03/2012361233474499.html.

Benkler, Yochai. 2006. *The Wealth of Networks*. New Haven, CT: Yale University Press.

Bernd, Candice. 2013. "Idle No More: From Grassroots to Global Movement." *Truthout*, January 29, truth-out.org/news/item/14165-idle-no-more-from-grassroots-to-global-movement.

Boler, Megan, ed. 2008. *Digital Media and Democracy*. Cambridge, MA: MIT Press.

Castells, Manuel. 2009. *Communication Power*. Oxford: Oxford University Press.

CPSR (Computer Professionals for Social Responsibility). 1997 "One Planet, One Net," *The CPSR Newsletter* 15 (4), cpsr.org/prevsite/publications/newsletters/issues/2001/Summer/nsb.html/view.

Donkin, Karissa. 2013. "Social Media Helps Drive Idle No More Movement." *Toronto Star*, January 11, www.thestar.com/news/canada/2013/01/11/social_media_helps_drive_idle_no_more_movement.html.

Dyson, Esther. 2012. "The Rise of the Attention Economy." *Al Jazeera*, December 28, www.aljazeera.com/indepth/opinion/2012/12/201212271132754429.html.

Estalella, Adolfo, Jara Rocha, and Antonio Lafuente, eds. 2013. "Laboratorios de procomún" ("Laboratories of the Commons"). Special issue, *Teknokultura* 10 (1), www.teknokultura.net/index.php/tk/issue/view/5.

Gallaher, Ryan. 2013. "Software That Tracks People on Social Media Created by Defense Firm." *Guardian*, February 10, www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence.

Galloway, Alexander. 2004. *Protocol*. Cambridge, MA: MIT Press.

Gray, Chris Hables. 1997. *Postmodern War*. New York: Guilford, www.chrishablesgray.org/postmodernwar/index.html.

Gray, Chris Hables. 2005. *Peace, War, and Computers*. New York: Routledge.

Greenwald, Glenn. 2013. "Pentagon's New Massive Expansion of 'Cyber-Security' Unit Is About Everything Except Defense." *Guardian*, January 28, www.guardian.co.uk/commentisfree/2013/jan/28/pentagon-cyber-security-expansion-stuxnet.

Grossman, Lev. 2013. "Drone Home." *Time*, February 11, 26–33.

Holmes, Brian. 2007. "The Revenge of the Concept: Artistic Exchanges, Networked Resistance." In *Art and Social Change: A Critical Reader*, edited by Will Bradley and Charles Esche, 350–68. London: Tate.

Hughes, Thomas. 1983. *Networks of Power*. Baltimore: Johns Hopkins University Press.

Jarnot, Charles. 2012. "History." In *Introduction to Unmanned Aircraft Systems*, edited by Richard K. Barnhart, Stephen B. Hottman, Douglas M. Marshall, and Eric Shappee, 1–16. New York: CRC Press.

Jarvis, Jeff. 2011. "Revealed: US Spy Operation That Manipulates Social Media: Military's 'Sock Puppet' Software Creates False Online Identities to Spread Pro-American Propaganda." *Guardian*, March 17, www.guardian.co.uk/technology/2011/mar/17/us-spy-operation-social-networks.

Kelly, Kevin. 1995. *Out of Control*. New York: Basic Books.

Lessig, Lawrence. 1999. *Code and Other Laws of Cyberspace*. New York: Basic Books. *Code 2.0* is available at www.socialtext.net/codev2/.

Macauley, William, and Ángel Gordo-López. 1995. "From Cognitive Psychologies to Mythologies." In *The Cyborg Handbook*, edited by Chris Hables Gray, Steven Mentor, and Heidi Figueroa-Sarriera, 433–44. New York: Routledge.

Mann, Steve. 2013. "Veillance." Paper presented at the IEEE International Symposium on Technology and Society (ISTAS), Toronto, June 27–29.

Mann, Steven. 2014. "Maktivism: Authentic Making for Technology in the Service of Humanity." In *DIY Citizenship: Critical Making and Social Media*, edited by Matt Ratto and Megan Boler, 29–52. Cambridge, MA: MIT Press.

Mason, Paul. 2012. "Global Unrest: How the Revolution Went Viral." *Guardian*, January 3, www.guardian.co.uk/world/2012/jan/03/how-the-revolution-went-viral.

McConnell, Mike. 2010. "Mike McConnell on How to Win the Cyber-War We're Losing." *Washington Post*, February 28, www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html?sid=ST2010031901063.

Morello, Henry. 2007. "e-(re)volution: Zapatistas and the Emancipatory Internet." *A Contracorriente* 4 (2): 54–76, www.ncsu.edu/project/acontracorriente/winter_07/Morello.pdf.

Moreno-Caballud, Luis. 2013. "Desbordamientos culturales en torno al 15-M" ("The 15-M Movement in Its Cultural Context"). *Teknokultura* 10 (1), www.teknokultura.net/index.php/tk/article/view/79.

Nelson, Ted. 1974. *Computer Lib/Dream Machines*. San Mateo, CA: Hugo's Book Service, www.digibarn.com/collections/books/computer-lib/.

Ragan, Steve. 2011. "Tunisian Government Harvesting Usernames and Passwords." *Tech Herald*, January 4, www.thetechherald.com/articles/Tunisian-government-harvesting-usernames-and-passwords/12429/.

Ryan, Yasine. 2011. "The Tragic Life of a Street Vendor." *Al Jazeera*, January 20, www.aljazeera.com/indepth/features/2011/01/201111684242518839.html.

Sádaba, Igor, and Ángel Gordo. 2008. "El Tecnología es política por otros medios" ("Technology Is Politics by Other Means"). In *Cultura digital y movimientos sociales* (*Digital Culture and Social Movements*), edited by Igor Sádaba and Ángel Gordo, 9–22. Madrid: Cararata.

Salah, Ahmed. 2011. Unpublished interview with Chris Hables Gray, October 3.

Scarry, Elaine. 1987. *The Body in Pain*. Oxford: Oxford University Press.

Soegaard, Mads. 2010. "Affordances," www.interactiondesign.org/encyclopedia/affordances.html.

Uberti, David. 2012. "Rise of the Machines: Domestic Drones Take Off." *Medill National Security Zone*, April 3, nationalsecurityzone.org/site/rise-of-the-machines-domestic-drones-take-off/.

Van Buren, Peter. 2012. "Obama's Unprecedented War on Whistleblowers." *Salon*, February 9, www.salon.com/2012/02/09/obamas_unprecedented_war_on_whistleblowers/.

Van Creveld, Martin. 1989. *Technology and War*. New York: Free Press.

Ward, Colin. 1973. *Anarchy in Action*. London: Freedom Press.

Ángel J. Gordo is a lecturer of sociology at the Universidad Complutense de Madrid. He is a member of the research group Cibersomosaguas and coeditor of *Teknokultura: Revista de cultura digital y movimientos sociales*. His research interests include technology and social change, social mobility, material culture, and qualitative critical methodology.

Chris Hables Gray lectures at the University of California, Santa Cruz, in the cultural studies of science and technology and is Vice President for Organizing for UC-AFT, which represents all lecturers and librarians in the University of California. He was lead editor of *The Cyborg Handbook* (1995) and is the author of *Postmodern War* (1997), *Cyborg Citizen* (2002), and *Peace, War, and Computers* (2005). He is a member of the research groups Syndicate for Initiative and Cibersomosaguas.