E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One

Wendy H. Wong and Peter A. Brown

In recent years, WikiLeaks and Anonymous have made headlines distributing confidential information, defacing websites, and generating protest around political issues. Although many have dismissed these actors as terrorists, criminals, and troublemakers, we argue that such actors are emblematic of a new kind of political actor: extraordinary bandits (e-bandits) that engage in the politics of no one via anonymizing Internet technologies. Building on Hobsbawm's idea of the social bandit, we show how these actors fundamentally change the terms of global activism. First, as political actors, e-bandits are akin to Robin Hood, resisting the powers that be who threaten the desire to keep the Internet free, not through lobbying legislators, but by "taking" what has been deemed off limits. Second, e-banditry forces us to think about how technology changes "ordinary" transnational activism. Iconic images of street protests and massive marches often underlie the way we as scholars think about social movements and citizen action; they are ordinary ways we expect non-state actors to behave when they demand political change. E-bandits force us to understand political protest as virtual missives and actions, activity that leaves no physical traces but that has real-world consequences, as when home phone numbers and addresses of public officials are released. Finally, e-banditry is relatively open in terms of who participates, which contributes to the growing sense that activism has outgrown organizations as the way by which individuals connect. We illustrate our theory with the actions of two e-bandits, Anonymous and WikiLeaks.

On January 17, 2012, officials from the U.S. Federal Bureau of Investigation and Scotland Yard had a phone conversation that revolved around a strategy to take down the hacktivists[1] known as Anonymous, among other like-minded groups. Unfortunately for them, the very group they sought to investigate had compromised their e-mail systems. On February 1, Anonymous posted a recording of the conversation.[2] The ensuing embarrassment for both national-level investigative agencies also revealed key information about ongoing investigations. Similarly, in an internally-circulated 2008 classified Pentagon report, U.S. Army intelligence concluded that WikiLeaks "poses a significant 'operational security and information security' threat to military operations."[3] The report warned that the potential leaking of secret U.S. military documents on the WikiLeaks website could "influence operations against the U.S. Army by a variety of domestic and foreign actors."[4] Unfortunately for U.S. Army Intelligence, WikiLeaks procured the classified report about itself and subsequently leaked it on its website.[5]

Are they freedom-of-speech fighters or tech-savvy terrorists? Nongovernmental organizations (NGOs), social movements, or a new international criminal? We argue that WikiLeaks, Anonymous,[6] and other groups engaged in what has become described as hacktivism are "extraordinary bandits" (e-bandits), adapting Hobsbawm's iconic "social bandit" for the challenges of politics in the digital age.[7] E-bandits do not fit well in our existing analytical categories for a number of reasons. Introducing new terminology allows us to capture the essence of such actors in global politics while demonstrating the limits of existing tools from international relations (IR) and sociology. Using anonymizing technologies to create a transnational "politics of no one," e-bandits are principled actors[8] who capitalize on the Internet and other information technologies to lead disembodied, virtual attacks against physical targets in order to encourage political change. On the one hand, e-banditry is liberating—it allows whoever wants to join a movement to join, and "atypical" activists have joined political movements. It also allows for groups to impose physical costs without a physical presence. On the other hand, e-banditry by its very nature creates problems of

Wendy H. Wong is Associate Professor of Political Science and Director of the Trudeau Centre for Peace and Conflict Studies at the Munk School of Global Affairs, University of Toronto (wendyh.wong@utoronto.ca). Peter A. Brown is MA candidate in Political Science at the University of Toronto (pete.brown@mail.utoronto.ca). *The authors would like to thank David Welch; Mark Sedra; Ron Deibert; Todd Hall; Marcos Ancelovici; Stefania Milan; Stefan Kroll; Lilach Gilady; the participants of the Workshop for Transnational Linkages, Institutional Building, and the Reconfiguration of Rights and Justice Regimes; three anonymous reviewers; and especially Jeffrey Isaac for helpful comments. Brown's contribution to the research has been supported by the Social Science and Humanities Council of Canada.*

doi:10.1017/S1537592713002806

coherence, lack of directed action, and multiple and multiplying goals as participants join for their own purposes without revealing their identities, and therefore their interests. Our current understandings of the roles of transnational social movements and non-state actors in IR are just beginning to grasp the importance of the Internet, largely focusing on the role and responsibility of the state in digital governance.[9] By contrast, we intend to advance the thinking on how non-state actors can harness information technologies for political gains on a transnational level through engaging in a new politics of no one.

What e-bandits show us is that technology changes resistance. To date, many have considered the role of technology as a way to retool existing ways of participating in citizen movements. Instead of collecting signatures for petitions in parking lots, people can use digital signatures procured by mass e-mails. Groups can cut costs using listservs for a planned protest. Webpages serve as publicity vehicles for activists, and blogs democratize who can opine. Here, we argue that the anonymizing potential of the Internet challenges some of our fundamental assumptions of who can use technology, and for what ends. Prior to the Internet, protest occurred much in the "old way"—citizens gathering in public demonstrations, holding placards, and making speeches against state policy or corporate greed. Neither WikiLeaks nor Anonymous[10] necessarily employ these techniques in their methods of holding actors accountable and expressing discontent with policies or actions. Instead, both organizations hold others accountable in a way that does not reveal their own identities, and as such, the threat of their action is both a threat from nobody and potentially from everywhere at the same time. This "politics of no one," in which e-bandits make demands without revealing who they are, or who they speak for, affects the way that we conceive of contemporary forms of global citizen action.

The politics in which e-bandits engage are anything but business as usual in new technological clothing; the actions of e-bandits are extra-ordinary. First, as political actors, e-bandits are more akin to Robin Hood than the American Association for Retired Persons, politicking not through lobbying, but by "taking" what has been deemed off limits. Furthermore, Anonymous and WikiLeaks both explicitly see themselves as taking from the powerful to empower the disempowered with information and access to the political process. Second, e-banditry forces us to think about how technology changes "ordinary" transnational activism. Iconic images of street protests and massive marches often underlie the way we as scholars think about social movements and citizen action; they are ordinary ways we expect non-state actors to behave when they demand political change. E-bandits protest with virtual missives and actions, activity that leaves no physical traces but has real-world consequences, as when home phone numbers and addresses of public officials are released. Finally, e-banditry is relatively open in terms of who participates, which contributes to the growing sense that activism has outgrown organizations as the way by which individuals connect. To the extent that we can identify the "groupiness" of Anonymous or WikiLeaks, what one can say is that both organizations appeal to broader audiences than ordinary activist groups. As others have found, Anonymous' founding credo was anything but political,[11] and its actions continue to be precipitated and fueled by different kinds of activists than those attracted to other groups heavily reliant upon the Internet, such as Moveon.org. Participating in Anonymous' actions online is not an option for just anybody, as there are baseline technical knowledge requirements.[12] As a consequence, the anonymity under which e-bandits act provides us with a conceptual and theoretical challenge in terms of how we place these groups.

Here we first review the extant scholarship on transnational social movements, NGOs, and international criminal networks (ICNs) to demonstrate how each of these extensive literatures falls short in capturing the work of e-bandits. We then briefly introduce both Anonymous and WikiLeaks. Next we develop the concept of the e-bandit to show the importance of the politics of no one for IR and global activism. We will show how Anonymous and WikiLeaks epitomize e-banditry. We conclude with the implications of identifying e-bandits in politics and the future of a research agenda focused on the politics of no one.

Varieties of Transnationalism

IR has struggled since the 1970s to define political relationships outside of linkages between states, or between states and a catch-all category called "non-state actors."[13] We often have difficulty classifying and understanding the role and effect of such actors. To illustrate, at various times, critics have accused Anonymous of being a terrorist group, and some American politicians, including U.S. Vice President Joe Biden,[14] have painted WikiLeaks with the same brush.[15] We find this characterization inappropriate, given standing definitions of terrorism in political science, which emphasize violence against civilians,[16] implying (at least the threat of) physical injury or death, rather than property damage, virtual or actual. However, we do take the characterization of e-bandits as "international criminal organization"[17] seriously, as we see parallels between these two types of actors in the ICN literature. We also consider two other veins of research that shed light on the role of e-bandits—NGOs and transnational social movements—to illustrate that e-bandits challenge extant explanations for how non-state actors influence global politics.

NGOs and Transnational Social Movements

Often, social movements and NGOs can be thought of in complementary terms. NGOs can lead social movements, or they can transmit the desires of activists, or they can carry domestic disputes into the international arena and vice versa. Despite the fact that "social movements" capture the more amorphous types of activism that professionalized NGOs do not, many scholars have conceived of social movements as led by social movement organizations, with economic concerns.[18] Much of the difference, however, is scholarly discipline, with "social movements" being the territory of sociologists, and "transnational advocacy and NGOs" belonging to political scientists.[19] Scholars interested in transnationalism in both fields come from a particular political spectrum, often limiting analyses to the "good ones" of transnational politics, shunning the comparatively less attractive (i.e., more politically-conservative) organizations such as the National Rifle Association.[20]

Transnational activism received a massive amount of attention after the publication of *Activists beyond Borders,* [21] which gave those interested in the role of non-state actors in IR a common language and conceptual map. Using the idea of the boomerang pattern, Keck and Sikkink demonstrated the influence that networks wielded against norm-violating states. From that starting point, a research agenda emerged to examine networks for environmental[22] and human rights[23] causes. Scholars began thinking carefully about the role of non-state actors in different areas as well, such as security,[24] thereby linking the idea of transnational politics more generally to the extant literature on social networks.[25]

The actors within those transnational networks, however, have remained loosely conceptualized. Often, analysis privileges the role of NGOs or global civil society,[26] to bring about political change,[27] but transnational social movements have also received continued interest.[28] What NGOs are, however, is not always well defined; many scholars adapt a definition from the United Nations that NGOs are groups that are not established by intergovernmental agreement,[29] cannot use or advocate violence, be for-profit, or be a political party. They must be representative and promote the political purposes of the UN.

Despite the ambiguity in their definition, NGOs are credited as primary movers of transnational networks, in some cases serving as a kingmaker for local social movements and transnational issues,[30] with the ability to push some ideas on to the international agenda[31] and others off[32] across a variety of topics, including human rights, environmentalism, and security. NGOs have formed the backbone of many transnational movements, including the abolitionist movement of the nineteenth century, International Campaign to Ban Landmines, the network against the small arms trade, and the Multilateral Agreement on Investments.[33] International NGOs can affect domestic protest.[34] NGOs have made headway by creating alternative fora for activists across a variety of international issues,[35] and even influencing the processes of international environmental negotiations by transmitting information.[36] Furthermore, NGOs play a very important role in shaping the preferences of states on human rights in international law[37] and norms.[38]

Social movement scholars have demonstrated that activists build organizations and coalitions and try to change the way things work through inhibition, provocation, and information.[39] In short, social movements are "people with common purposes and solidarity who mount collective challenges to elites and authorities . . . [with] mobilization around particular norms."[40] Social movement organizations enable transnational participation, bringing nonlocal activists to different sites.[41] Activists' identities are reified and recreated through participation in social movements.[42] Some social movements have not been averse to breaking the law and private property, for instance, through civil disobedience techniques such as the Black Bloc.[43]

In spite of the usefulness of existing theory from sociology and IR, are WikiLeaks and Anonymous "merely" social movements or NGOs? These categories, as much as they describe many of the behaviors of e-bandits, seem to be missing some of the core raisons d'être, including a positive agenda for change. For instance, WikiLeaks argues that it is providing a more pure form of journalism, aimed at revealing the truth a coopted international media refuses to do, but without a positive agenda. Anonymous too lacks a coherent agenda, and is largely reactive, but its lack of agenda has more to do with its organizational structure (discussed later). One can imagine that e-bandits are engaged in a battle over information beyond political change, as they want to change the way information is distributed, but many of the demands have been "anti."

On another note, while Anonymous' role in the Occupy movements has been well-established[44] and WikiLeaks has become a legitimate source for news,[45] social movement and NGO scholars have not rushed to embrace such actors. Indeed, there is a reluctance to lump e-bandits in with do-gooders such as Amnesty International or World Vision. This may in part have to do with the current security climate, in a post-9/11 age where much information is kept secret. But it almost certainly also has to do with the fact that neither WikiLeaks nor Anonymous is engaged in purely legal activities and that some of its actions seem more destructive than acting in the name of principle, and yet they are not exactly criminal, as we will show.

International Criminal Networks

In examining ICNs,[46] scholars have sought to understand the "dark side"[47] of network forms of organization. ICNs are "dark networks—both illegal and covert",[48] and as such, they must "operate in the shadow of the law."[49] A criminal network is best defined as "a set of actors who are connected by ties which in some way or other support the commission of illegal acts."[50] The term ICNs is used broadly here to describe a myriad of illicit non-state actors that are oftentimes called by different names.

Since the 1980s, ICNs have been on the rise as a global security threat. Many governments now identify ICNs as top priorities in terms of domestic policing issues, and have dramatically increased budgets and personnel to combat them.[51] In the face of the expanding bureaucracy and policing measures meant to disrupt and eliminate ICNs, these groups adopt different network structures to solve the dilemma they inevitably face when managing their conflicting needs of both "concealment and coordination."[52] The resulting trade-offs between efficiency and security can differ depending on the motivations of a given set of network actors.[53] As Morselli et al. note, "not all criminal networks pursue the same objective. For example, drug trafficking or networks in criminal enterprise are designed for pecuniary profit. Others, such as terrorist networks, pursue ideological objectives."[54] The ends shape how networks approach the efficiency/security trade-off: criminal networks that pursue profit tend to prioritize efficiency over security, while many that pursue ideological ends tend to prioritize security over efficiency.[55]

ICNs are structured and survive based on relational ties between participants.[56] Criminal actors, who are willing to co-offend, typically do so based on notions of trust that are borne out of "criminally exploitable ties."[57] These ties are usually found in human bonds such as kinship, ethnicity, friendship, and prison associations, to name a few.[58] Trust relationships enhance the secrecy, and hence, the survivability of networks, helping them remain insular and clandestine.

Moreover, the resiliency of ICNs is, in part, based on access they gain to legitimate power channels through offers of money and other enticements that corrupt authorities and create space for their operations.[59]It is these "exchange relationships"[60] between ICNs and legitimate authorities that distinguish their activities from acts of simple banditry,[61] which is why they tend to thrive in failed states, or states that suffer from high levels of government corruption.[62] Online scammers, for example, take advantage of government corruption in Russia to pursue economic gains online, while terrorist networks like al-Qaeda take root in sovereignty-challenged states like Afghanistan in order to exercise their necessary organizational functions.[63]

Both WikiLeaks and Anonymous[64] closely resemble some of the key features of ICNs. They adopt network structures that facilitate access to new information for the benefit of learning and adaptation in the face of a powerful opposition that seeks to shut them down.[65] They overcome government attempts to disrupt their operations, by "[building] redundancy into their operations by exploiting the services of multiple peripheral nodes that perform the same task,"[66] and, like terror networks, they seek to circumvent or subvert formal state authority.[67] Additionally, both groups engage in criminal behavior. Anonymous members ("Anons"[68]) participate in both illegal distributed denial-of-service (DDoS) attacks, and in the theft and destruction of intellectual and private property, and WikiLeaks, at minimum, deals in the exchange and publishing of stolen materials.[69]

Nevertheless, e-bandits are quite distinct from other ICNs. Though e-bandits do commit crimes and engage in extreme forms of action, they do not deploy physical violence as a key tactic in their operations the way more traditional criminal organizations and terrorist groups do.[70] Moreover, e-bandits do not always operate according to the typical motivations of most ICNs. In keeping with their Robin Hood-like tendencies, neither WikiLeaks nor Anonymous operates for pecuniary profit,[71] and while they do act primarily toward ideological ends and political change, WikiLeaks aims toward an ambiguously stated goal of "maximum political impact,"[72] and a notable component of Anonymous' activities are done simply for the lulz,[73] and not for economic or political gain.

Furthermore, while some observers argue that ties of trust are a universal aspect of organized crime,[74] e-bandits intentionally operate in the absence of trust. Instead, e-bandits rely on the encryption technologies[75] and anonymizing procedures[76] of the Internet to hide their identities from both authorities and co-offenders. The online activities of e-bandits are not about using the Internet simply as a medium for communication and information exchange the way some terrorist groups do.[77] Instead, e-bandits use the Internet as their primary tool for both concealment and action; thereby in fact operating in opposition to traditional ICN reliance on trust and physical relationships. Lastly, e-bandits do not engage in exchange relationships with government authorities to gain access to legitimate power channels[78] through bribery or corruption. Following Kenney, this is what makes them less like organized criminals and more like bandits.[79]

Anonymous and WikiLeaks in Brief

Anonymous and WikiLeaks both share the key characteristics of e-bandits. Both of them rely heavily on the notion of anonymity in their work, whether in how it goes about soliciting information (WikiLeaks) or as its primary activism tactic (Anonymous). They are both also promulgators of the idea that citizens deserve more access to information that the powers that be hold in secret, thus their raisons d'être hinge on a Robin Hood ethic of empowering the disempowered. Both groups have been able to attack governments and corporations in ways that have much more wide-ranging implications than many other global social movements before them, from economic to security threats.[80] Finally, Anonymous in particular has harnessed the collective agency of a new population of activists, previously and perhaps still unengaged in traditional forms of politics, but finding community and identity with like-minded individuals worried about the encroachment of state and corporate control, with the loss of freedom online, akin to the way youth have congregated on using electronic petitions as a form of civic engagement.[81] The changes in governance of the Internet have also led to the rise of e-banditry as a form of protest that is not inherently political, but nonetheless has political, social, and economic implications.

WikiLeaks

WikiLeaks is an organization that "solicits and publishes secrets and suppressed material from whistleblowers around the world."[82] Launched in 2006, it calls itself "an uncensorable system for untraceable mass document leaking."[83] Since its launch, it has published an extensive catalogue of secret documents—most of which seek to expose the dark underbelly of a variety of political and corporate issues.[84]

WikiLeaks' website provides whistleblowers with "a high security anonymous drop box fortified by cutting-edge cryptographic information technologies."[85] It uses a "modified version of the Tor Network,"[86] an online system that allows files to move across the Internet anonymously, with no way of determining where the file came from or where it is going.[87] Additionally, WikiLeaks routes all of its material through countries that have the strongest press freedom laws; it maintains servers in several different countries, and its material is hosted by hundreds of mirror sites, which makes removing its published content from the Internet virtually impossible.[88] By guaranteeing anonymity, WikiLeaks changes the way that whistle-blowing can be done both in terms of speed and the number of interlocutors necessary to release information. Encryption tools provide protection for the whistleblower and the ubiquity and usability of computers reduces the risk of discovery. Compared to the 1971 leaking of the Pentagon Papers, for example, when Daniel Ellsberg had to smuggle government secrets out of his office one volume at a time, and then copy them page by page, all the while risking detection, capture, and prosecution,[89] nowadays, almost anyone can submit material from almost anywhere, and leakers no longer need to rely on the oath of a journalist for assurances of their anonymity. WikiLeaks' ability to procure and publish secrets has caused the group to become a target of governments and corporations around the world. In addition to accusations of terrorism, the group's leader, Julian Assange, has become a wanted man; he is a target for capture, prosecution, and assassination.[90]

Anonymous[91]

The term "Anonymous" is a meme[92] that comes from online image boards. When someone posts or requests content online without signing their name to it, it is automatically assigned the name Anonymous.[93] Following from this, accurate characterizations of the "group" known as Anonymous are inherently difficult: "Anonymous is, like its name suggests, shrouded in some degree of deliberate mystery."[94] As such, descriptions of Anonymous lack precision. Anonymous can perhaps best be described as an Internet meme used by a transient and loosely affiliated collection of hackers, activists, trolls, and troublemakers who share two characteristics: they believe that the Internet should be a completely libertarian domain and they are willing to oppose and use disruptive tactics against those who seek to regulate cyberspace.

Anonymous has no permanent membership, no hierarchy or leadership, and no clear manifesto outlining its purpose or objectives.[95] Anonymous was born on the popular image boards known as 4chan—an online, image-based bulletin board where anyone can anonymously post comments and share images.[96] Content posted on 4chan is not searchable, and it disappears soon after posting, never to be found again.[97] In other words, participants, as well as content, are both anonymous and transient. Users of 4chan, and those who identify with the group Anonymous more generally, are often Internet trolls[98] searching for lulz. At its inception, Anonymous acted primarily with prankster-ish intentions.[99] Anonymous adopted a more politically-oriented ethos after trolling the church of Scientology in 2008.[100] When the church demanded the removal of an internal video that had been posted on various Internet sites, Anonymous organized a series of worldwide protests and launched a DDoS[101] attack against Scientology's website in the name of free speech.[102] Since that first political turn, Anonymous has protested many more times. It also supports groups (such as WikiLeaks) and movements (such as the uprisings in Tunisia in 2010–2011) that broadly fit its own freedom-based, anti-censorship underpinnings.

The Politics of No One

E-bandits such as WikiLeaks and Anonymous do not fit neatly into extant political categories, but they are also not sui generis. First, as we discuss below, Hobsbawm's work on social bandits demonstrates that liminal actors have always had a role in political protest. Second, hacktivists (and hackers more generally)[103] have always used technology to protest political and economic conditions.[104] Specifically, hacktivists have harnessed their energies into "three key areas: anti-censorship and freedom of speech, privacy, and Internet security."[105] Thus the key difference with e-banditry is that it harnesses both the anonymizing and economical capabilities of the Internet to link activists transnationally without revealing any real identities. Here we demonstrate how e-banditry challenges our conceptions and practices of politics in three different ways: "Robin Hood" activities, enabled via technology; using technology for virtual and anonymous protest; and changes in who can participate in political activism.

Contextualizing E-bandits—Why the Politics of No One is Different

Thinking about the role of the Internet in politics is a subject that scholars have wrestled with very seriously, as there are potentially far-reaching policy implications for democracy movements around the world.[106] A burgeoning literature explores how the Internet changes the way that individuals can act and interact politically, which can be roughly divided into the "Web 1.0" and "Web 2.0" periods.[107] Web 1.0 scholarship represents the first wave of interest in exploring the effects of the Internet and other digital media on participation and citizen experiences. Web 2.0, however, has opened up the door for thinking about how technology changes the nature of political participation and activism as Internet technologies and usages themselves proliferate.[108]

Our analysis fits firmly into this interest in how the Internet shifts the way that protest works[109] and why the Internet is important for civil society groups and NGOs.[110] Scholars working this vein have arrived at a number of interesting and somewhat oppositional conclusions. For one, not all agree that the Internet, or cyberspace more broadly, has necessarily all positive implications for change among non-state actors. While some have claimed the great transformative potential of cyberspace for activists fighting authoritarianism,[111] others have cautioned against the Internet as a tool for liberation,[112] or even the democracy of the Internet as a medium itself.[113] For non-state actors in particular, the encroachment of the state in terms of regulation and restriction poses problems for their abilities to use cyberspace as a tool, whether for dissent, protest, or mobilization.[114] Another perspective argues that it is the lack of state-led governance to date that has led to some of the quandaries we face regarding the regulation of the Internet today.[115] Bennett concludes that the Internet is a double-edged sword, creating opportunities for more lasting campaigns and building networks without pre-existing strong ties, but also creating decision-making and control problems.[116]

In the context of the contradictory implications of the Internet, one way to think about its effect is how it shapes the way that individuals can act. One set of arguments posits that citizens can now engage one another politically without turning to parties or interest groups,[117] using online petitions as a means to express political and social preferences.[118] The Internet may also change the way that we think about leadership in social movements,[119] certainly lowering the costs of organizing[120] and therefore depressing the threshold of who can create and sustain an activist group. However, Bimber et al. demonstrate that organizations themselves are not going away in the face of cyberspace.[121] Instead, extant organizations such as Moveon.org, AARP, and the American Legion utilize new communication modes to allow people to shape their experiences with political organizations more directly. Organizations are learning how to use the Internet in all sorts of ways beyond simple appeals to mass publics, as the Howard Dean U.S. presidential campaign demonstrated.[122] All of these investigations help us rethink how collective action as we know it works in the context of cyberspace.

We are interested in the effects of cyberspace on political action as well, but unlike previous work, we are concerned with a different political logic that is only enabled by the anonymizing capacity of the Internet. The politics of no one is only significant and important if the identity of the actors remains unknown. To date, the implicit assumption that underlies almost all of the different takes of the effect of the Internet on political organization is one of forming networks where none existed before, thereby enabling activists to interact on a far more regular or economical basis than ever before. The politics of no one, on the other hand, is not about creating communities and networks so much as it is about using anonymity as a tool for political action, and by its very definition therefore shirking the notion of community creation. It is about getting people involved without giving them faces, names, or even necessarily a position to defend. Rather, the politics of no one allows e-bandits to engage politically through cyberspace, and just as quickly disappear into the digital air.

Much of the extant theorization lays the groundwork for the politics of no one. The way that the Internet has developed to date has allowed for e-banditry, but changes in regulations and government practices may change these abilities. Nonetheless, the significance of the politics of no one should not be overlooked. Other "old" movements—such as the Zapatistas—incorporated the Internet into their repertoires to enable networking with like-minded groups or international actors.[123] For the most part, however, they were not "anonymous" because the movement's identity was known, and the "anonymous" Zapatista leader himself, Subcomandante Marcos, became iconic. For e-bandits, if they are successful, the identities of the very activists are shrouded, even if they engage in highly-publicized activities that drum up state backlash.[124] They truly engage in the politics of "no one," in that their views cannot be easily attributed to known individuals. Actors such as Anonymous and WikiLeaks have posed challenges to states, corporations, and other interested parties precisely because of the questions that their actions have raised. What are the possibilities opened for citizens with the advent of cyberspace? How can cyberspace constitute and define activism, rather than just being a tool of many that an organization uses to attract adherents, or an economical way for activists to stay in touch? All of the research to date on the politics of the Internet and the Internet in politics are enabling factors for the politics of no one. As we emphasize here, it is not the technology that makes e-banditry different, per se, but it is the *anonymity* that cyberspace enables that poses the greatest challenge for conceptualizing this kind of activism.

One of the closest analogues to e-banditry is the anarchist movement that became notable in the nineteenth century and persists today in the form of "anti" movements[125] that have engaged in sometimes violent confrontations with police and property in the form of the "black bloc."[126] As some have put it, anarchism is back, with a renewed focus on all forms of domination (beyond the state) and a de-emphasis on formal organization,[127] as punk bands and activists adopt the mantle of the iconic "circle-A."[128] Anarchists seek to build new kinds of communities focused around the notion of an "affinity group," with the idea being that larger groups act based on consensus and agreement from smaller groups.[129] In its current guise, anarchism finds its purpose in galvanizing groups that are frequently neglected by or are the victims of neoliberal excess and seeks to give those groups voice in global politics through direct action. Using techniques such as the black bloc, in which individuals dress in black and move as a group in order to express "a radical critique of the economic and political system,"[130] anarchists have blocked traffic, confronted police, and destroyed private property. The black bloc technique, similar to some of the disruptive techniques used by e-bandits discussed below, generates attention, perhaps disproportionately, for the perpetrators of such actions, but it is important to point out the tensions in making the comparison between e-banditry and black blocs. Participants in black blocs are anonymous until they are caught; e-bandits may never be caught if their digital footprints are covered by anonymizing technology. Black blocs are used by a sub-section of the protesters in an anarchist crowd; e-banditry is a tactic used by everyone participating in the politics of no one. Both black blocs and e-bandits, however, are engaged in resistance against power,[131] whether in the form of the state, corporation, or both. Moreover, e-bandits and anarchists have been able to counter negative media coverage through their own Internet-based outreach.[132]

E-bandits as Social Bandits

In his seminal work on banditry, Hobsbawm[133] introduces the concept of the social bandit to articulate how such actors have occupied the space between lords, states, and the peasantry throughout history by challenging the status quo and those who benefit from existing societal structures.[134] One type of social bandit, the noble robber ("Robin Hood"), is particularly applicable to thinking about e-bandits. Hobsbawm identifies the main characteristics of noble robbers, which can be summarized as righting injustices by taking from the rich to give to the poor; righteousness in that they are victims of injustice and pursue justice through noble and defensive means; and come from a community and therefore have its support, enduring as legendary figures.[135] E-bandits exhibit similar tendencies. First, they seek to redress threats to the freedom of the Internet, whether those threats come in the form of government restriction, surveillance, or regulation, or when corporations act in ways they deem unjust. In that sense, e-bandits take away from "the man," which is relatively wealthy in terms of power and resources, in order to empower ordinary people. By taking information, defacing websites, or otherwise using digital means to act against the powers that be, e-bandits effectively take from the rich through disabling commercial and government websites, and try at times to give back to the community, either in terms of revelation (releasing videos, previously unavailable materials), reporting, or providing previously unavailable tools (DDoS attacks).

Second, e-bandits use basic principles to justify their behavior. Even though Anonymous in particular emerged from individuals interested in "just the lulz," its first action against the Church of Scientology protested the censorship of videos containing actor Tom Cruise. WikiLeaks sees itself as an antidote to the complacency of modern mass media, releasing primary documents as a way for individuals to see the truth for themselves. E-bandits fit into the rough ethos of hacktivism, espousing an ethic of empowering those who are not privileged with knowledge while exposing the weaknesses of the powerful.

What makes them e-bandits, finally, is the method by which they achieve their goals, employing virtual and online techniques in the hacktivist style, which is defined most simply as "activism gone electronic."[136] The fundamental role the Internet plays in e-banditry distinguishes them as a community, which at once requires specialized skills, but also is inclusive and widens the doors for different kinds of individuals to become politically active and involved in a broader public interested in defending a set of principles. Some have seen the shifts enabled by the Internet as pivotal in changing how we think about social, political, and economic relationships.[137] Hacking, which forms the basis of e-banditry, is a skill set that not all people can become good at, and there is a specific way in which hackers go about demonstrating their prowess at manipulating code to gain access to blocked information.[138]

As one might expect, though, there is wide variation on what constitutes a hacktivist. Some, such as the founding members of the Cult of the Dead Cow (cDc), see hacktivism as "intended to refer to the development and use of technology to foster human rights and the open exchange of information."[139] These hacktivists view their work as liberating and in line with the broader human rights agenda promoting free speech and expression.[140] Others we might call hacktivists hijack websites and deface them, and launch DDoS attacks that shut down e-mail servers and websites.[141] Such tactics are key tools for Anonymous, but would not be embraced by cDc.

For our purposes, hacktivism differs from e-banditry in that e-bandits always operate anonymously but claim credit for their actions in the name of a social cause. By contrast, many early hackers wanted to leave no trace of their activities. E-bandits want their actions to be discovered, and in fact, purposefully make them well known and bombastic precisely for the purposes of generating support for the cause. They do not, however, want their identities to be known. E-bandits also engage in illegal, extra-legal, and legal activities that result in negative or at least costly outcomes for their targets, thus distinguishing them from some hacktivists who simply want to post videos on behalf of a cause.

Thus, we see e-bandits as forming a distinct subgroup among hacktivists, pursuing a distinct kind of activism enabled by the anonymizing technologies of the Internet, which at once lends a common identity to those who participate, but at the same time making it difficult for others (and e-bandits themselves) to identify them as specific individuals. The critical component that distinguishes e-banditry from other social movements or even hacktivists is the *disembodiment* of activism. This decoupling of resistance and physical presence is central to the politics of no one, as technology enables anonymity that does not require individuals to physically gather for a show of strength or support. For e-bandits, the technology allows for their actions, and they in turn embody the most crucial elements of the technology. WikiLeaks' anonymous drop box, for instance, provides potential whistleblowers with a measure of assurance that their identities will not be revealed in exchange for sharing potentially explosive information. "No one" is there to drop off the documents or pick them up. The threats posed by e-bandits are not about physical destruction or trespass, but virtual transgressions, such as disrupting website traffic, stealing information stored in digital databases, or broadcasting secrets in easily-replicable digitized form. Thus, the anonymous and disembodied nature of e-banditry forms the core of the politics of no one.

Anonymous and WikiLeaks as E-Bandits

We have argued that e-banditry has changed the way that non-state actors can pursue political ends. Technology has come to define the way that politics is expressed, not merely serving as a means by which other political actions are taken. Both Anonymous and WikiLeaks embody e-banditry, and furthermore, inspire new ways of thinking about democracy and citizen activism.

Robin Hood?

Both WikiLeaks and Anonymous see themselves as providing a public service for mass consumption, revealing controversial materials without the same ethical concerns of the mainstream media or launching online attacks against governments and corporations with little regard for the law. Both view their actions as "taking it to the man"—fighting corporate greed, government corruption, and journalistic restrictions through technology—somewhat akin to Robin Hood stealing from the rich to give to the poor. In this case, both Anonymous and WikiLeaks steal and redistribute information.

Assange has emphasized that Wikileaks' "mission is to expose injustice."[142] It targets both highly oppressive regimes and immoral behavior on the part of governments and corporations in the West with the ultimate goal of being part of a social movement that can "bring down many administrations."[143] WikiLeaks has collaborated with several traditional media outlets such as *The Guardian* and *The New York Times,* [144] giving both of them, as well as their entire readership, access to stolen information they would otherwise not have obtained. WikiLeaks shared stolen data with these other media outlets in order to increase the amount of political impact the material would have, and to share in the labor of dealing with such a large trove of documents—thereby ensuring a broad proliferation of the material.[145] Upon the release of the material, WikiLeaks published its own un-redacted version on its website for readers to see the source documents in their entirety.[146] In this way, WikiLeaks was able to occupy a unique position by simultaneously being source, publisher, and political activist.

Anonymous more explicitly breaks law in its pursuit of principles, and in defense of the disempowered it deems to have been wronged by the powers that be. In December 2011, Anonymous hacked the servers of an intelligence firm known as Stratfor.[147] Anonymous stole the company's client list along with the credit card information of many of its members, and also procured millions of internal e-mails, which are said to show the monitoring of activists by private corporations, secret payments to government officials, and insider trading.[148] The hack was said to be in retaliation for the arrest and imprisonment of Bradley Manning, the U.S. Army intelligence officer accused of leaking classified information to WikiLeaks.[149] Anonymous shared the e-mails with WikiLeaks, thus allowing the information contained in them to reach a broad public, and in Robin Hood-like fashion, it used the stolen credit card information to make several charitable donations.[150]

Anonymous also acts defensively for itself and its perceived allies, such as WikiLeaks. In February 2011, HBGary Federal[151] CEO Aaron Barr claimed to have unearthed intimate details about the hierarchy and identities of some Anons,[152] and he threatened to turn this information over to the FBI.[153] In response, Anonymous hacked into the company's servers, defaced its website, destroyed and stole data, seized its Facebook and Twitter accounts, and lifted thousands of internal e-mails that were subsequently published openly on the Internet.[154] One of the stolen files turned out to contain material outlining a plot by HBGary Federal to disrupt and discredit WikiLeaks and its many supporters through threats, exploitation, and fraud.[155]

The hacking of both HBGary Federal and Stratfor were particularly novel for several reasons. First, the obtained information was not leaked by an aggrieved insider, rather, it was gathered by a group of outsiders that was able to use technology to infiltrate the system and expose secret information. Second, Anonymous was not limited to traditional forms of protest when Barr issued his threats against the group. Instead, it was able to immediately threaten and retaliate—striking back at an adversary while willfully breaking some laws along the way. Lastly, these attacks were largely reactionary in nature and perpetrated against people who were deemed by Anons to "deserve it"; in other words, Anonymous was motivated by a sense of injustice,[156] and these anonymous, disembodied attacks had real-world consequences for those who were hacked.

Moreover, Anonymous endeavors to expose corporate malfeasance through the activities of Anonymous Analytics (AA). AA employs "unique skill sets to expose companies that practice poor corporate governance and are involved in large-scale fraudulent activities."[157] One observer has characterized the group as research vigilantes who are "the WikiLeaks of the business world, bent on uncovering corporate wrongdoing."[158] The operation has already levied allegations of corporate wrongdoing against several prominent corporations. The allegations accuse the targeted corporations of misrepresenting corporate achievements to advertisers, providing falsified financial statements, and defrauding investors.[159] The research done by AA is beginning to achieve a level of broad legitimacy. As an example, Moody's Investor Service recently used an AA report against the company Choada as a reason to downgrade its credit rating.[160]

In terms of the Robin Hood-like qualities of both groups, both have skirted the legal/illegal divide, engaging in activities that both circumvent and outright break laws protecting intellectual property and privacy, yet they do so, they claim, in the name of higher principles and at great risk to their own survival. Observers have noted the willingness of WikiLeaks' staff to face life in prison, or even possible execution, in order to release information it deems vital to the public interest.[161] Anonymous, especially, has claimed that it is not worried about running afoul of the law based on its own sense of ethics.[162] Both groups take enormous risks in the name of principles they believe in, fighting on behalf of others who can't fight for themselves. Anons have come to the online defense of rape victims, oppressed groups, targets of government censorship, student protestors, and even the grieving families of murdered children.[163] Legitimate or not, what seems most apparent, is the Robin Hood-esque aspirations of both of these groups to fight on the behalf of the disempowered, to break the stranglehold of information, and to broaden access to political power.

Technology

New communication technologies and the Internet are at the heart of e-banditry. These technologies have altered the terms by which transnational political participation occurs, forcing open the boundaries of what constitutes "activism." E-bandits use Internet technologies to deploy anonymity as a means to steal and gather information, attack adversaries, and capture political power. In other words, as Nye argues, "technology is putting into the hands of deviant individuals and groups destructive powers that were once reserved primarily for governments.[164]

WikiLeaks has been described as an "advocacy group for sources,"[165] one that provides assurances of anonymity for anyone who comes forward through its online drop box. The drop box is a critical technological development in information gathering,[166] since the anonymity afforded by WikiLeaks' encryption tools has the potential to motivate people to share secret information when they might not otherwise be inclined to do so for fear of reprisals.[167] The most famous case to date has been that of U.S. Army Intelligence analyst Bradley Manning.[168]

WikiLeaks has acquired and published a myriad of secret documents as part of a broader effort to "[give] people the information they need."[169] In 2010, it released a classified U.S. military video titled "Collateral Murder." The video, which received over 10 million views on YouTube alone, shows U.S. military personnel opening fire on a group of Iraqi civilians.[170] WikiLeaks followed that by releasing a trove of secret military files that document the U.S.-led wars in Iraq and Afghanistan. These "War Logs" paint an unflattering picture of both wars, and reveal the un-reporting of civilian deaths, the capturing and killing of opposition leaders without trial, the acquisition of surface-to-air missiles by the Taliban, and the increasing use of drones to hunt Taliban targets by remote control.[171] In addition, WikiLeaks released a massive classified file containing secret diplomatic cable between the US and many of its enemies and allies. The cables contain detailed accounts of such things as corruption by foreign regimes, undercover arms shipments, and human trafficking.[172]

Although e-banditry generally requires technical sophistication, Anonymous' operations provide a means for nonspecialists to use technology to participate in political action.[173] Some of Anonymous' most basic tactics, such a DDoS attacks, are easy to participate in, and are often described as a "digital sit-in."[174] In terms of transnational activism, DDoS attacks are transformative, because by simply sitting in front of a computer screen, anyone can anonymously[175] engage in a virtual protest that has real-world effects, thereby bypassing the traditional requirement of a physical gathering to demonstrate support. Other Anons carry out riskier, more advanced activities such as the building and maintaining of infrastructure, providing technological assistance, facilitating anonymity, law-breaking, information gathering, and other types of labor that furthers the group's political objectives.[176] Furthermore, some Anons employ botnets[177] to wreak havoc against state and corporate targets online. Botnet controllers simultaneously harness the power of thousands of hijacked computers (often without any of the computers owners being aware) that have the online capacity to take down the websites of governments and major corporations.[178] These online attacks have costly real-world effects, and are often done in retaliation against targets that Anons deem to be corrupt or unjust.[179]

Technology shapes the way that these groups engage in political action. The cloak of anonymity inhibits discovery, facilitates information exchange, and encourages participation, thereby changing the way that we think about political protest. In this light then, technological evolution has spawned new ways to participate in direct action without having to physically gather; the Internet provides the means for the anonymous and disembodied politics of no one.

Changing Participation

Anonymous is radically democratic in its structure. There are no leaders, anyone can join, and members are located almost everywhere in the world.[180] Anons meet in Internet Relay Chats[181] (IRCs) where anyone can bring forward issues, discuss strategy, or propose attacks with the aim of furthering broad political objectives.[182] Each Anon is motivated by his or her own political issues, and can pick and choose which operations they wish to participate in.[183] Many of those who take part in the group's operations act in the name of principled causes, and by a desire to fight for "something."[184] In this way, Anonymous' structures are akin to affinity groups among anarchists.

This democratic structure, however, can cut both ways. In one sense, the open and leaderless nature of Anonymous makes it susceptible to problems of incoherence and a lack of directed action. Sometimes Anons are interested in "hacking as a form of protest,"[185] other times however, Anons are subject to internal strife and in-fighting. Indeed, some former participants have become vigilantes who seek to expose and bring down other Anons.[186] Nonetheless, the transient and radically democratic nature of these types of hacktivist groups makes it very difficult for authorities to disrupt their activities. Leaderless[187] groups that have flat decision-making strategies and fluid membership make it near impossible for authorities to use "kingpin strategies"[188] to take them down. It might be said then, that along with anonymity, the fluid and democratic nature of hacktivist groups contributes to their resiliency and survival.

Beyond reporting, WikiLeaks works to create democratic links between activists with shared political values. The group recently launched its own online social networking platform.[189] The platform is intended to allow like-minded individuals to anonymously join with others who share similar principles and who wish to fight for common causes.[190] The "Friends of WikiLeaks" (FoWL) site is built upon similar characteristics as the whistleblowing website. Encryption ensures anonymity to users and the site claims to be beyond surveillance or compromise.[191] Users can sign up using anonymous information, and then communicate with like-minded activists worldwide in languages of their own choosing.[192] FoWL allows users to decide for themselves how best to organize their contacts and operations, and users are encouraged to bring forward issues of their choosing for discussion and action.[193] In short, the anonymity afforded by both FoWL and WikiLeaks' drop box allows ordinary citizens, political outsiders, and atypical activists to engage in political activism.

Conclusion

In recent years, we have been confronted with the role of social media in citizen protests and overthrows of unpopular and repressive governments in the Middle East. Much virtual ink has been spilled describing the capability of the Internet to make people matter,[194] rendering once-invincible autocrats such as Hosni Mubarak vulnerable to the demands of ordinary people. These analyses, however trenchant, reflect an old mode of thinking about activism as enabled by communications technologies. Technology is yet another tool for activists to employ; Middle Eastern protesters used social media to tap into one another's extant political interests and unify demands. Transnational supporters showed their solidarity via virtual links to events on the ground, broadcasting footage and passing the message on to Western audiences. Importantly, these political demands existed prior to social networking technologies.[195]

It is not enough to simply attribute positive qualities to the Internet for its mobilizing potential. In fact, there are potential pitfalls, and perhaps even some negative, or at least uncomfortable consequences. We have presented an alternative way to conceive of technology and how its anonymizing capability creates the conditions for the politics of no one. E-bandits challenge our current conceptions of transnational activism in three important ways. The first is that e-bandits engage in an explicit resistance to power through technological means, and are largely able to attack powerful targets through techniques that shield their identities as they engage in questionable kinds of activities (à la Robin Hood). The second is that the anonymizing potential of the Internet enables different kinds of social protest to emerge. Instead of physical protest as a show of strength, activists can gather online, sometimes advertently, sometimes inadvertently, and express their political preferences through leaking information and attacking servers. Virtual protest, as we demonstrate, often creates physical externalities. Finally, e-banditry expands the boundaries of who can become a political activist. Rather than technology as a tool among many for activists to choose from, communication technology in the case of Anonymous, WikiLeaks, and groups similar to them have found activism because of technology. Communication technologies, therefore, underlie and define groups, and are the only tool with which these groups might wield political influence. The "who" behind protests, whether they are professional activists, non-citizens, or kids with high-level computer skills, matters less if the means by which protest happens are both anonymous and disabling, thereby demanding attention from policymakers or business executives. In this sense, therefore, we can view Anonymous and WikiLeaks as emblematic of transnational, democratic movements, largely un-directed by a centralized viewpoint, dependent on its participants to define its goals.

We think this last plank of the theory of e-banditry holds plenty of promise for a future research agenda. The tension that has arisen in recent years over the "representativeness" of NGOs and other transnational movements is directly affected by Internet technologies. Professionalization of the non-profit advocacy sector has made it harder for those without resources to break in; the potential unleashed by the Internet for non-professionals to engage in activism and impose consequences on their targets is something worth exploring further. Not only is this important for transnational advocacy, but also for thinking about the potential of radical democracy within our current institutions, as we see with the growing number of Pirate Parties in Europe and beyond. What are the challenges posed by the politics of no one to our conceptions of democracy, both globally and domestically?

Secondly, the ever-evolving nature of WikiLeaks and Anonymous makes us wonder whether they are enduring or ephemeral. Do e-bandits arise in times of turbulence and uncertainly to question the status quo, revealing its inconsistencies? Or are these actors here to stay, changing forever the landscape of what it means to be a transnational actor, and indeed, how activism can occur without a physical gathering of protestors? Can the whistleblowing, the unleashing of private information, and the temporary destruction of websites substitute for occupation of city streets and public places? Anonymous and WikiLeaks already collaborate on projects.[196] In recent events, the link between the two has become increasingly explicit as the two groups work in concert to enact political goals. Where Anonymous can gather information, WikiLeaks can disseminate it—as illustrated by WikiLeaks' recent release of millions of internal documents from the private intelligence firm Stratfor that were allegedly obtained by Anonymous.[197] These actions, along with some of their other structures described here, seem to indicate that the two groups have plans to stay.

Finally, from an organizational perspective, future research can examine further some of the questions that have arisen in IR regarding the study of NGOs. As e-bandits move to more "legitimate" means of attaining and distributing information, we can examine their actions using tools from extant debates about the credibility of NGOs.[198] Thus, theories and research on transnational advocacy networks, in which autonomous NGOs, activists, and other like-minded actors seek out one another in order to attain collective global goals, remains highly relevant to both academic and policy circles. E-bandits both force us to think about our assumptions about transnational politics, and they also reinforce the importance of looking carefully at the non-state actors in networks.

Notes

[1] Those who practice hacktivism, which is defined as "the application of information technologies . . . to political action"; Ludlow 2010, 26.

[2] Albanesius 2012.

[3] Hodson 2010.

[4] Ibid.

[5] Ibid.

[6] Although they are independent, WikiLeaks and Anonymous are nonetheless linked. In recent collaboration, WikiLeaks released 500 million internal documents from a private intelligence firm called Stratfor. The data had been procured by Anonymous. It is unclear, however, whether this relationship is enduring; see Stryker 2012.

[7] The "digital age" denotes the proliferation of information technologies in the contemporary era. "Cyberspace" is most often conceived as the Internet, but also encompasses the broader spectrum of global digital electronic communications; see Deibert 2012. In this article, we use cyberspace and the Internet interchangeably, unless otherwise noted.

[8] Sikkink 1993.

[9] See Goldsmith and Wu 2006; Deibert et al. 2008, 2010, 2011; Zittrain 2008; Hughes 2010; Palfrey 2010.

[10] Anonymous members do, on occasion, protest in more traditional ways; see Olson 2012a, 81–86. This is not, however, the primary means by which they advocate.

[11] Halpin 2012.

[12] Coleman 2011a. These skills, however, are not always necessary for the modal participant in an Anonymous action, as seen later.

[13] Huntington 1973, Keohane and Nye 1974, Lipschutz 1992, Wapner 1995, Keck and Sikkink 1998.

[14] Grier 2010.

[15] McCullagh 2010.

[16] E.g., Lake 2002.

17 “Marc Garneau on Privilege.”
18 McCarthy and Zald 1973, 1975, 1977; Jenkins 1983; Jenkins and Eckert 1986; Burstein and Linton 2002; more recently Smith and Wiest 2005.
19 Klotz 2002.
20 Rieff 1999; Bob 2012.
21 Keck and Sikkink 1998.
22 Khagram, Riker, and Sikkink 2002.
23 Risse, Ropp, and Sikkink 1999.
24 Montgomery 2005.
25 Kahler 2009; Hafner-Burton, Kahler, and Montgomery 2009.
26 See Clark, Friedman, and Hochstetler 1998 for a discussion of the role of NGOs in global civil society.
27 Lipset 1994; Mathews 1997; Rieff 1999.
28 Tarrow 1994; Gill 2000; Bandy and Smith 2005.
29 Ahmed and Potter 2006, 8.
30 Bob 2005, 2012; Carpenter 2011.
31 Wong 2012.
32 Carpenter 2010.
33 Deibert 2000; Rutherford 2000; Williams, Goose, and Wareham 2008; Shawki 2011; Wong 2011
34 Murdie and Bhasin 2010.
35 Clark, Friedman, and Hochstetler 1998.
36 Betsill and Corell 2001.
37 Neumayer 2005; Hafner-Burton and Tsutsui 2007.
38 Price 1998.
39 E.g., Tarrow 1994, 2005; McAdam, McCarthy, and Zald 1996; Keck and Sikkink 1998; Khagram, Riker, and Sikkink 2002; Bandy and Smith 2005.
40 Klotz 2002, 57.
41 Fisher et al. 2005.
42 Melucci 1996; Polletta and Jasper 2001; Snow 2001.
43 See Dupuis-Deri 2010b.
44 Captain 2011.
45 Thus, releasing its news hoax was seen as a bad move by man;. Greenberg 2012b.
46 For example: “criminal networks” (Morselli, Giguère, and Petit 2007), “illicit entrepreneurs” (Kenney 2009), “clandestine transnational actors” (Andreas 2003), “dark networks” (Raab and Milward 2003), and “radical transnational groups” (Adamson 2005).
47 Kenney 2009.
48 Raab and Milward 2003, 419–420.
49 Ibid.
50 von Lampe and Johansen 2004,167.
51 Andreas 2003.
52 Kenney 2009, 82.
53 Morselli, Giguère, and Petit 2007, 145.
54 Ibid, 145.
55 Ibid, 143–145.
56 McIllwain 1999.
57 von Lampe 2003, 10.
58 von Lampe 2003, 11, McIllwain 1999, 308.
59 Kenney 2009, 88.
60 Ibid.
61 Ibid.
62 Kahler 2009, 116; Viano 2003, 170–172.
63 Kahler 2009, 116; Richmond 2012.
64 Some Anons believe that police groups view them as an organized criminal group. See Olson 2012a, 364.
65 Kenney 2007, 1–24.
66 Kenney 2009, 85.
67 Kahler 2009, 116; Rosen 2010.
68 The term “Anons” is borrowed from Coleman 2011c.
69 Some observers contend that WikiLeaks may actively participate in potentially illegal activities in order to acquire the documents it leaks; see Zetter 2010.
70 McIllwain 1999, 308–309; Adamson 2005.
71 Both groups do receive donations. Illegal profit is not, however, the primary motive of either group. See Zetter 2011 and Olson 2012a, 264–265, 304–306.
72 As quoted in Harnden 2010.
73 Lulz is “a pluralization and bastardization of laugh out loud (lol). Lulz denotes the pleasures of trolling, but the lulz is not exclusive to trolling. The lulz can also refer more generally to lighthearted and amusing jokes, images, and pranks.” Coleman 2011b.
74 von Lampe 2003, 22.
75 All online submissions to WikiLeaks are heavily encrypted. See “About WikiLeaks.”
76 Anons hide their identities even within the Anonymous network; see Olson 2012a, 122, 255–256.
77 Kenney 2010.
78 WikiLeaks has collaborated with Icelandic parliamentarians on drafting free-speech legislation and on document leaking. These rare collaborations, however, were licit and voluntary. For more see Mackey 2010 and Khatchadourian 2010.
79 Kenney 2009, 88.
80 An example: when Bank of America saw its stock drop over 3 percent based on the threat that WikiLeaks was in possession of a 5GB hard drive from one of its executives and was set to release it; see Memmott 2010.
81 Earl and Schussman 2008.
82 “Julian Assange, The Man Behind Wikileaks.”
83 As quoted in Misselwitz 2011.
84 Ibid.; Domscheit-Berg 2011, xi-xiv.
85 “About WikiLeaks.”
86 Khatchadourian 2010.
87 Bagh 2010.
88 Sutter 2010, Misselwitz 2011, Somaiya 2010.
89 Cooper and Roberts 2011.

90 Burns and Somaiya 2010 and "Julian Assange, The Man Behind WikiLeaks."

91 Because anyone can use the moniker "Anonymous" (Coleman 2011b), in this article we use "Anonymous" and "Anons" to refer to anyone that self-identifies as such. We also use these terms to refer to anyone who behaves in accordance with the general tendencies of "Anonymous," such as LulzSec, Antisec, Knightsec, or others.

92 "A meme is basically an idea that is easily transferable." Memes are created when a "large group of users come to identify with a particular image or slogan," as a catch-phrase might be; Crenshaw 2013.

93 Ibid.

94 Coleman 2011b.

95 Walker 2011.

96 See 4Chan website (www.4chan.org, Accessed March 31, 2013).

97 Grigoriadis 2011.

98 Trolls are cyberpranksters who engage in playful and unpredictable behavior online meant to provoke and humiliate others; see Coleman 2011b.

99 Coleman 2011a.

100 Ibid.

101 Distributed denial-of-service (DDoS) attacks occur when "a multitude of computers [are] coordinated to overwhelm a site with so much data that it [is] temporarily knocked offline"; Olson 2012a, 9.

102 Coleman 2011a.

103 See Levy 2010 for more details about hackers since the 1950s and the hacker ethic more generally.

104 Chiefly, the hacker ethic might be distilled as two basic ideas: "(1) all information should be free; (2) mistrust authority and promote decentralization"; Ludlow 2010, 25.

105 Deibert 2003, 528.

106 For instance, with the recent debates over the role of social media in democratizing the Arab world; Howard and Hussain 2011; Lynch 2011.

107 Bimber 2012.

108 Ibid., 115.

109 Earl 2010.

110 Deibert 2000; Earl and Kimport 2011; Bimber, Flanagin, and Stohl 2012.

111 Shirky 2008; Howard 2010, 2011.

112 Morozov 2011.

113 Hindman 2009.

114 Deibert et al. 2008, 2010, 2011.

115 Zittrain 2008.

116 Bennett 2003.

117 Zukin et al. 2006.

118 Earl and Schussman 2008.

119 Earl 2007.

120 Earl and Kimport 2011.

121 Bimber, Flanagin, and Stohl 2012.

122 Hindman 2005.

123 See Bob 2005; Langman 2005.

124 Denning 2001.

125 Rupert 2006.

126 Dupuis-Deri 2010b; Shantz 2011.

127 Gordon 2007.

128 Williams 2007.

129 Graeber 2002, Dupuis-Deri 2010a.

130 Dupuis-Deri 2010b.

131 Shantz 2011, 54–5.

132 Owens and Palmer 2003.

133 Coleman 2011a makes links to Hobsbawm, but in our mind, for very different purposes.

134 Hobsbawm 2000, 7. See also Andreas 2013 for a take on smugglers in U.S. history.

135 See Hobsbawm 2000, 46–62.

136 Jordan and Taylor 2004, 1.

137 Benkler 2006; Castells 2007; Shirky 2008.

138 Levy 2010.

139 Delio 2004.

140 For example, in an interview Oxblood Ruffin, who is a member of cDc, characterizes hacktivism as "[using] technology to improve human rights. It also employs nonviolent tactics." Allnutt 2011.

141 Denning 2008.

142 Khatchadourian 2010.

143 As quoted in Khatchadourian 2010.

144 Keller 2011 (accessed July 31, 2012).

145 "Julian Assange, The Man Behind WikiLeaks."

146 Keller 2011.

147 Stratfor website (http://www.stratfor.com/, Accessed September 3, 2013).

148 Greenberg 2012a.

149 Perlroth 201.

150 Ibid.

151 HB Gary website http://www.hbgary.com/ (Accessed September 3, 2013).

152 Coleman 2011a.

153 Freeman 2012.

154 Olson 2012a, 3–25.

155 Masnick 2011.

156 Olson 2012a, 24–25.

157 See "Anonymous Analytics."

158 Bacani 2011.

159 Olson 2012b; La Roche 2011; McMillan 2011.

160 Bacani 2011.

161 Greenwald 2012.

162 Isikoff 2011.

163 Lennard 2012a; Lennard 2012b; Lennard 2012c; Leonard 2012.

164 Nye 2011, 120.

165 Khatchadourian 2010.

166 *The Wall Street Journal,* has attempted to duplicate and utilize the WikiLeaks model; see Foremski 2011.

167 Keller 2011.

168 Manning is currently facing charges related to the leaked files. It was not, however, Wikileaks who compromised his anonymity. Manning allegedly confessed to Adrian Lamo, who subsequently reported him to authorities; See Nakashima 2010.

169 "Julian Assange, The Man Behind WikiLeaks."

170 Domscheit-Berg 2011,162.

171 Davies and Leigh 2010.

172 Leigh 2010.

173 Olson 2012a, 131; Crenshaw 2013.

174 Coleman 2011c.

175 Anonymous has previously had trouble with its DDoS application known as Low-Orbit Ion Cannon (LOIC), in terms of ensuring online anonymity for users. Subsequently, Anons have developed alternative versions of LOIC that use the anonymizing procedures of the TOR network (described earlier); see Olson 2012a, 125–129.

176 Olson 2012a; Coleman 2011b.

177 "Botnets" are "large networks of 'zombie' computers usually controlled by a single person who [gives] them commands from a private IRC channel"; Olson 2012a, 74.

178 Olson 2012a, 74–75, 111–124.

179 Ibid.

180 Coleman 2010.

181 "An IRC Tutorial."

182 Coleman 2010.

183 Crenshaw 2013.

184 Coleman 2010.

185 Olson 2012a, 244.

186 Ibid., 205–217.

187 Though Assange is WikiLeaks' leader, the advocacy activities of the group result from the willingness of independent sources to leak secret material through appropriately encrypted servers. Indeed, Assange himself has made it clear that the activities of WikiLeaks would continue without him. For more see "Julian Assange, The Man Behind WikiLeaks."

188 Kenney 2005, 73–74.

189 See "Friends of Wikileaks."

190 Ibid.

191 See "About Friends of WikiLeaks."

192 Ibid.

193 "Friends of WikiLeaks Membership."

194 For two views on this subject, see Howard and Hussain 2011; Morozov 2011.

195 Anonymous, among other groups, worked to restore Internet connections when the Egyptian goverment cut off service during Arab Spring.

196 Greenberg 2012a.

197 Stryker 2012.

198 Gourevitch, Lake, and Stein 2012.

References

4Chan website *http://www.4chan.org/* (Accessed September 3, 2013).

"About Friends of WikiLeaks." https://wlfriends.org/about (Accessed March 31, 2013).

"About WikiLeaks." http://wikileaks.org/About.html (Accessed September 3, 2013).

Adamson, Fiona B. 2005. "Globalisation, Transnational Political Mobilisation, and Networks of Violence." *Cambridge Review of International Affairs* 18(1): 31–49.

Ahmed, Shamima, and David Potter. 2006. *NGOs in International Politics.* Bloomfield, CT: Kumarian Press.

Albanesius, Chloe. 2012. "Anonymous Leaks FBI, Scotland Yard Call About Hackers." *PCMAG,* February 3; accessed February 14, 2012.

Allnutt, Luke. 2011. "Old-School Hacker Oxblood Ruffin Discusses Anonymous and the Future of Hacktivism." *RadioFreeEurope/RadioLiberty.* June 8; accessed January 24, 2013.

Andreas, Peter. 2003. "Redrawing the Line: Borders and Security in the Twenty-first Century." *International Security* 28(2): 78–111.

———. 2013. *Smuggler Nation: How Illicit Trade Made America.* New York: Oxford University Press.

"An IRC Tutorial." http://irchelp.org/irchelp/irctutorial.html#intro (Accessed September 3, 2013).

"Anonymous Analytics." http://www.anonanalytics.com/ (Accessed September 3, 2013).

Bacani, Cesar. 2011. "Are You Safe from the Research Vigilantes?" *CFO Innovation ASIA,* October 12; accessed July 31, 2012.

Bagh, Carl. 2010. "How WikiLeaks Uses Technology to Protect Anonymity of Whistle-blowers." *International Business Times,* November 29; accessed March 25, 2012.

Bandy, Joe, and Jackie Smith, eds. 2005. *Coalitions across Borders: Transnational Protest and the Neoliberal Order.* Lanham, MD: Rowman and Littlefield.

Benkler, Yochai. 2006. *The Wealthy of Networks: How Social Production Transforms Markets and Freedom.* New Haven and London: Yale University Press.

Bennett, W. Lance. 2003. "Communicating Global Activism: Strengths and Vulnerabilities of Networked Politics." *Information, Communication, and Society* 6(2): 143–68.

Betsill, Michele M., and Elisabeth Corell. 2001. "NGO Influence in International Environmental Negotiations: A Framework for Analysis." *Global Environmental Politics* 1(4): 65–85.

Bimber, Bruce. 2012. "Digital Media and Citizenship." In *The SAGE Handbook of Political Communication,* ed. Holli A Semetko and Margaret Scammell. London: SAGE Publications, Ltd.

Bimber, Bruce, Andrew J. Flanagin, and Cynthia Stohl. 2012. *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change.* New York: Cambridge University Press.

Bob, Clifford. 2005. *The Marketing of Rebellion: Insurgents, Media, and International Activism.* New York: Cambridge University Press.

———. 2012. *The Global Right Wing and the Clash of World Politics.* New York: Cambridge University Press.

Burns, John F., and Ravi Somaiya. 2010. "WikiLeaks Founder on the Run, Trailed by Notoriety." *New York Times,* October 23; accessed March 26, 2012.

Burstein, Paul, and April Linton. 2002. "The Impact of Political Parties, Interest Groups, and Social Movement Organizations on Public Policy: Some Recent Evidence and Theoretical Concerns." *Social Forces* 81(2): 380–408.

Captain, Sean. 2011. "The Real Role of Anonymous in Occupy Wall Street." *Fast Company,* October; 17; accessed January 24. 2013.

Carpenter, R. Charli. 2010. *Forgetting Children Born of War: Setting the Human Rights Agenda in Bosnia and Beyond.* New York: Columbia University Press.

———. 2011. "Vetting the Advocacy Agenda: Network Centrality and the Paradox of Weapons Norms." *International Organization* 65(1): 69–102.

Castells, Manuel. 2007. "Communication, Power, and Counter-power in the Network Society." *International Journal of Communication* 1: 238–66.

Clark, Ann Marie, Elisabeth J. Friedman, and Kathryn Hochstetler. 1998. "The Sovereign Limits of Global Civil Society: A Comparison of NGO Participation in UN World Conferences on the Environment, Human Rights, and Women." *World Politics* 51(1): 1–35.

Coleman, Gabriella. 2010. "What It's Like to Participate in Anonymous' Actions." *The Atlantic,* December 10; accessed July 31, 2012.

———. 2011a. "Hacker Politics and Publics." *Public Culture* 23(3): 511–16.

———. 2011b. "Anonymous: From the Lulz to Collective Action." *MediaCommons,* April 6; accessed March 25, 2012.

———. 2011c "The Ethics of Digital Direct Action." *Al Jazeera English,* September 1; accessed July 31, 2012.

———. 2012a. "Our Weirdness Is Free." *Triple Canopy,* January 13; accessed Mach 30, 2012.

———. 2012b. "Am I Anonymous?" *Limn,* accessed July 31, 2012.

Cooper, Michael, and Sam Roberts. 2011. "After 40 Years, the Complete Pentagon Papers." *Nytimes.com,* June 7; accessed March 25, 2012.

Crenshaw, Adrian. 2013. "Crude, Inconsistent Threat: Understanding Anonymous." *Irongeek.com;* accessed January 28, 2013.

Davies, Nick, and David Leigh. 2010. "Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation." *The Guardian,* July 25;. accessed July 31, 2012.

Deibert, Ronald J. 2000. "International Plug 'n Play? Citizen Activism, the Internet, and Global Public Policy." *International Studies Perspectives* 1: 255–72.

———. 2003. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace." *Millennium—Journal of International Studies* 32(3): 501–30.

———. 2012. "Cybersecurity: The New Frontier." *Foreign Policy* Topic 4: 45–58.

Deibert, Ronald J., John Palfrey, Rafal Rohozinski, and Jonathan L. Zittrain, eds. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, MA: MIT Press.

———. 2010. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Cambridge, MA: MIT Press.

———. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Delio, Michelle. 2004. "Hacktivism and How It Got Here." *Wired;* accessed July 14, 2004.

Denning, Dorothy E. 2001. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy,* ed. John Arquilla and David F. Ronfeldt. Santa Monica, CA: RAND.

———. 2008. "Cyberwarriors: Activists and Terrorists Turn to Cyberspace." *Harvard International Review* 23(2): 70–75.

Domscheit-Berg, Daniel. 2011. *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website.* Toronto: Doubleday Canada, Limited.

Dupuis-Deri, Francis. 2010a. "Anarchism and the Politics of Affinity Groups." *Anarchist Studies* 18(1): 40–61.

———. 2010b. "The Black Blocs Ten Years after Seattle." *Journal for the Study of Radicalism* 4(2): 45–82.

Earl, Jennifer. 2007. "Leading Tasks in a Leaderless Movement: The Case of Strategic Voting." *American Behavioral Scientist* 50(10): 1327–49.

———. 2010. "The Dynamics of Protest-Related Difussion on the Web." *Information, Communication, and Society* 13(2): 209–25.

Earl, Jennifer, and Katrina Kimport. 2011. *Digitally Enabled Social Change: Activism in the Internet Age.* Cambridge, MA: MIT Press.

Earl, Jennifer, and Alan Schussman. 2008. "Contesting Cultural Control: Youth Culture and Online Petitioning." In *Civil Life Online: Learning How Digital Media Can Engage Youth,* ed. W. Lance Bennett. Cambridge, MA: MIT Press.

Fisher, Dana R., Kevin Stanley, David Berman, and Gina Neff. 2005. "How Do Organizations Matter? Mobilization and Support for Participants at Five Globalization Protests." *Social Problems* 52(1): 102–21.

Foremski, Tom. 2011. "*Wall Street Journal* Wants Your Leaks—Launches 'SafeHouse'" *ZDNet,* May 5; accessed July 31, 2012.

Freeman, Allen. 2012. "Who Is Anonymous? How the *Wall Street Journal* and the NSA Got It Wrong." *Null Byte,* accessed April 2, 2012.

"Friends of WikiLeaks." https://wlfriends.org (Accessed March 31, 2013).

"Friends of WikiLeaks Membership" https://wlfriends.org/membership (Accessed March 31, 2013.)

Gill, Stephen. 2000. "Toward a Postmodern Prince? The Battle in Seattle as a Moment in the New Politics of Globalisation." *Millennium* 29(1): 131–40.

Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World.* New York: Oxford University Press.

Gordon, Uri. 2007. "Anarchism Reloaded." *Journal of Political Ideologies* 12(1): 29–48.

Gourevitch, Peter A., David A. Lake, and Janice Gross Stein, eds. 2012. *The Credibility of Transnational NGOs: When Virtue Is Not Enough.* New York: Cambridge University Press.

Graeber, David. 2002. "The New Anarchists." *New Left Review* 13: 61–73.

Greenberg, Andy. 2012a. "WikiLeaks Tightens Ties To Anonymous In Leak Of Stratfor Emails." *Forbes,* February 27; accessed April 2,. 2012.

———. 2012b. "How WikiLeaks' *New York Times* Hoax Diluted Truth-Telling With Trolling." *Forbes,* July 30; accessed January 24, 2013.

Greenwald, Glenn. 2012. "Attacks on RT and Assange Reveal Much about the Critics." *Salon.com,* April 18,; accessed July 31, 2012.

Grier, Peter. 2010. "WikiLeaks Chief Julian Assange: 'Terrorist' or Journalist?" *The Christian Science Monitor,* December 20; accessed July 9, 2012.

Grigoriadis, Vanessa. 2011. "4chan's Chaos Theory." *Vanity Fair,* April; March 30, 2012.

Hafner-Burton, Emilie M., and Kiyoteru Tsutsui. 2007. "Justice Lost! The Failure of International Human Rights Law To Matter Where Needed Most." *Journal of Peace Research* 44(4): 407–25.

Hafner-Burton, Emilie M., Miles Kahler, and Alexander H. Montgomery. 2009. "Network Analysis for International Relations." *International Organization* 63(3): 559–92.

Halpin, Harry. 2012. "The Philosophy of Anonymous: Ontological Politics without Identity." *Radical Philosophy* 176: 19–28.

Harnden, Toby. 2010. "Julian Assange's Arrest Warrant: A Diversion from the Truth?" *The Telegraph,* August 22; accessed July 31, 2012.

HB Gary website http://www.hbgary.com/ (Accessed September 3, 2013).

Hindman, Matthew. 2005. "The Real Lessons of Howard Dean: Reflections on the First Digital Campaign." *Perspectives on Politics* 3(1): 121–28.

———. 2009. *The Myth of Digital Democracy.* Princeton, NJ: Princeton University Press.

Hobsbawm, Eric. 2000. *Bandits.* New York: The New Press.

Hodson, Steven. 2010. "Has WikiLeaks Finally Bitten off a Secret Too Big?" *The Inquisitr,* 24 March 24; March 25, 2012.

Howard, Philip N. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam.* New York: Oxford University Press.

———. 2011. "Reply to Evgeny Morozov's Review of *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam.*" *Perspectives on Politics* 9(4): 900.

Howard, Philip N., and Muzammil M. Hussain. 2011. "The Role of Digital Media." *Journal of Democracy* 22(3): 35–48.

Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs* 86(2): 523–41.

Huntington, Samuel P. 1973. "Transnational Organization in World Politics." *World Politics* 25(3): 333–68.

Isikoff, Michael. 2011. "Hacker Group Vows 'cyberwar' on US Government, Business." *Msnbc.com,* March 8; accessed March 30, 2012.

Jenkins, J. Craig. 1983. "Resource Mobilization Theory and the Study of Social Movements." *Annual Review of Sociology* 9: 527–53.

Jenkins, J. Craig, and Craig M. Eckert. 1986. "Channeling Black Insurgency: Elite Patronage and Professional Social Movement Organizations in the Development of the Black Movement." *American Sociological Review* 51(6): 812–29.

Jordan, Tim, and Paul A. Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause.* New York: Routledge.

"Julian Assange, The Man Behind Wikileaks." http://www.cbsnews.com/8301-18560_162-7286686.html (Accessed January 29, 2013).

Kahler, Miles, ed. 2009. *Networked Politics: Agency, Power, and Governance.* Ithaca, NY: Cornell University Press.

Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists beyond Borders.* Ithaca, NY: Cornell University Press.

Keller, Bill. 2011. "Dealing with Assange and the WikiLeaks Secrets." *New York Times,* January 30; accessed July 31, 2012.

Kenney, Michael. 2005. "Drug Traffickers, Terrorist Networks, and Ill-Fated Government Strategies." In

New Threats and New Actors in International Security, ed. Elke Krahmann. New York: Palgrave Macmillan.

———. 2007. *From Pablo to Osama: Trafficking and Terrorist Networks, Government Bureaucracies, and Competitive Adaptation.* University Park, PA: Pennsylvania State University Press.

———. 2009. "Turning to the 'Dark Side': Coordination, Exchange, and Learning in Criminal Networks." In *Networked Politics: Agency, Power, and Governance,* ed. Miles Kahler. Ithaca, NY: Cornell University Press.

———. 2010. "Beyond the Internet: Metis, Techne, and the Limitations of Online Artifacts for Islamist Terrorists." *Terrorism and Political Violence* 22(2): 177–97.

Keohane, Robert O., and Joseph S. Nye. 1974. "Transgovernmental Relations and International Organizations." *World Politics* 27(1): 39–62.

Khagram, Sanjeev, James V. Riker, and Kathryn Sikkink, eds. 2002. *Restructuring World Politics.* Minneapolis: University of Minnesota Press.

Khatchadourian, Raffi. 2010. "No Secrets." Newyorker.com, June 7; accessed March 25. 2012.

Klotz, Audie. 2002. "Transnational Activism and Global Transformations: The Anti-Apartheid and Abolitionist Experiences." *European Journal of International Relations* 8(1): 49–76.

Lake, David A. 2002. "Rational Extremism: Understanding Terrorism in the Twenty-first Century." *Dialogue-IO* 1(1): 15–29.

Langman, Lauren. 2005. "From Virtual Public Spheres to Global Justice: A Critical Theory of Internetworked Social Movements." *Sociological Theory* 23(1): 42–74.

La Roche, Julia. 2011. "This Is Awesome: Hacker Group 'Anonymous' Doing Securities Analysis, Attempting To Blow Up Chinese Frauds." *Business Insider,* October 4; accessed July 31, 2012.

Leigh, David. 2010. "Iraq War Logs Reveal 15,000 Previously Unlisted Civilian Deaths." *The Guardian,* October 22;. July 31, 2012.

Lennard, Natasha. 2012a. "Hackers Hit Ohio School Football Team over Gangrape." *Salon.com,* December 27; accessed January 29, 2013.

———. 2012b. "Anonymous Hits Westboro Baptist Church over Sandy Hook Picket Plans." *Salon.com,* December 16; accessed January 29, 2013.

———. 2012c. "Anonymous Retaliates to Israel's Gaza Internet Threat." *Salon.com,* November 15;. accessed January 29, 2013.

Leonard, Andrew. 2012. "Celebrating Anonymous: The Hackers' Big Year." *Salon.com,* December 27;. accessed 29 January 29, 2013.

Levy, Steven. 2010. *Hackers.* Sebastapol, CA: O'Reilly Media, Inc.

Lipschutz, Ronnie D. 1992. "Reconstructing World Politics: The Emergence of Global Civil Society." *Millennium—Journal of International Studies* 21(3): 389–420.

Lipset, Seymour Martin. 1994. "The Social Requisites of Democracy Revisited: 1993 Presidential Address." *American Sociological Review* 59(1): 1–22.

Ludlow, Peter. 2010. "WikiLeaks and Hacktivist Culture." *The Nation,* October 4.

Lynch, Marc. 2011. "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State." *Perspectives on Politics* 9(2): 301–10.

Mackey, Robert. 2010. "Victory for WikiLeaks in Icelands Parliament." *The Lede, New York Times,* June 17; accessed January 29, 2013.

"Marc Garneau on Privilege." http://openparliament.ca/debates/2012/2/29/marc-garneau-1/only/ (Accessed August 5, 2012).

Masnick, Mike. 2011. "Leaked HBGary Documents Show Plan To Spread WikiLeaks Propaganda For BofA . . . And 'Attack' Glenn Greenwald." *Techdirt,* February 10; accessed January 29, 2013.

Mathews, Jessica T. 1997. "Power Shift." *Foreign Affairs* 76(1): 50–66.

McAdam, Doug, John D. McCarthy, and Mayer N. Zald. 1996. *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings.* Cambridge: Cambridge University Press.

McCarthy, John D., and Mayer N. Zald. 1973. *The Trend of Social Movements.* Morristown, NJ: General Learning.

———. 1975. "Organizations Intellectuals and the Criticism of Society." *Social Service Review* 49: 344–62.

———. 1977. "Resource Mobilization and Social Movements: A Partial Theory." *American Journal of Sociology* 82(6): 1212–41.

McCullagh, Declan. 2010. "Congressman Wants WikiLeaks Listed as Terrorist Group." *CNET News,* CBS Interactive, November 28; accessed January 29, 2013.

McIllwain, Jeffrey Scott. 1999. "Organized Crime: A Social Network Approach." *Crime, Law & Social Change* 32: 301–23.

McMillan, Graeme. 2011. "Hackers Turned Journalists? Anonymous Launches 'Analytics' Site." *Time,* September 28; accessed July 31, 2012.

Melucci, Alberto. 1996. *Challenging Codes: Collective Action in the Information Age.* Cambridge: Cambridge University Press.

Memmott, Mark. 2010. "Bank of America Stock Steadies after WikiLeaks-Related Drop." *NPR,* December 1; accessed January 10,. 2013.

Misselwitz, Michael. 2011. "WikiLeaks Technology Superior to Government." *The Daily Aztec,* January 20; accessed March 25, 2012.

Montgomery, Alexander H. 2005. "Ringing in Proliferation: How to Dismantle an Atomic Bomb Network." *International Security* 30(2): 153–87.

Morozov, Evegeny. 2011. *The Net Delusion: The Dark Side of Internet Freedom.* New York: Public Affairs.

Morselli, Carlo, Cynthia Giguère, and Katia Petit. 2007. "The Efficiency/Security Trade-off in Criminal Networks." *Social Networks* 29(1): 143–53.

Murdie, Amanda, and Tavashi Bhasin. 2010. "Aiding and Abetting: Human Rights INGOs and Domestic Protest." *Journal of Conflict Resolution* 54(6): 1–29.

Nakashima, Ellen. 2010. "Messages from Alleged Leaker Bradley Manning Portray Him as Despondent Soldier." *Washington Post,* June 10; accessed July 31,2012.

Neumayer, Eric. 2005. "Do International Human Rights Treaties Improve Respect for Human Rights?" *Journal of Conflict Resolution* 49(6): 925–53.

Nye, Joseph S. 2011. *The Future of Power.* New York: PublicAffairs.

Olson, Parmy. 2012a. *We Are Anonymous; Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency.* New York: Little Brown & Brown.

———. 2012b. "Anonymous Rattles A Chinese Web Giant." *Forbes,* July 3; accessed July 31, 2012.

Owens, Lynn, and L. Kendall Palmer. 2003. "Making the News: Anarchist Counter-Public Relations on the World Wide Web." *Critical Studies in Media Communication* 20(4): 335–61.

Palfrey, John. 2010. "Four Phases of Internet Regulation." *Social Research* 77(3): 981–96.

Perlroth, Nicole. 2011. "Hackers Breach the Web Site of Stratfor Global Intelligence." *New York Times,* December 25; accessed April 2, 2012.

Polletta, Francesca, and James M. Jasper. 2001. "Collective Identity and Social Movements." *Annual Review of Sociology* 27(1): 283–305.

Price, Richard. 1998. "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines." *International Organization* 52(3): 613–44.

Raab, Jorg., and H. Brinton Milward. 2003. "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13(4): 413–39.

Richmond, Riva. 2012. "Web Gang Operating in the Open." *New York Times,* January 16.

Rieff, David. 1999. "The False Dawn of Global Civil Society." *The Nation* 268(7): 11–15.

Risse, Thomas, Stephen C. Ropp, and Kathryn Sikkink, eds. 1999. *The Power of Human Rights: International Norms and Domestic Change.* New York: Cambridge University Press.

Rosen, Jay. 2010. "PressThink: The Afghanistan War Logs Released by WikiLeaks, the World's First Stateless News Organization." *PressThink,* July 26; accessed January 29, 2013.

Rupert, Mark. 2006. *Globalization and International Political Economy.* Lanham, MD: Rowman & Littlefield Publishers.

Rutherford, Kenneth R. 2000. "The Evolving Arms Control Agenda: Implications of the Role of NGOs in Banning Antipersonnel Landmines." *World Politics* 53(1): 74–114.

Shantz, Jeffrey. 2011. *Active Anarchy: Political Practice in Contemporary Movements.* Lanham, MD: Lexington Books.

Shawki, Noha. 2011. "Organizational Structure and Strength and Transnational Campaign Outcomes: A Comparison of Two Transnational Advocacy Networks." *Global Networks* 11(1): 97–117.

Shirky, Clay. 2008. *Here Comes Everybody: The Power of Organizing without Organizations.* New York: Penguin.

Sikkink, Kathryn. 1993. "Human Rights, Principled Issue-Networks, and Sovereignty in Latin America." *International Organization* 47(3): 411–41.

Smith, Jackie, and Dawn Wiest. 2005. "The Uneven Geography of Global Civil Society: National and Global Influences on Transnational Association." *Social Forces* 84(2): 621–52.

Snow, David. 2001. "Collective Identity and Expressive Forms." Unpublished manuscript. CSD Working Papers, University of California–Irvine.

Somaiya, Ravi. 2010. "Hundreds of WikiLeaks Mirror Sites Appear." *Nytimes.com,* December 5; accessed March 26, 2012.

Stratfor website (http://www.stratfor.com/, Accessed September 3, 2013).

Stryker, Cole. 2012. "WikiLeaks' New Phase Begins." *Salon.com,* February 27; accessed April 12,. 2012.

Sutter, John D. 2010. "The Technical Muscle behind WikiLeaks." *CNN,* July 26; accessed January 29, 2013.

Tarrow, Sidney. 1994. *Power in Movement: Social Movements and Contentious Politics.* New York: Cambridge University Press.

———. 2005. *The New Transnational Activism.* New York: Cambridge University Press.

Viano, Emilio C. 2003. "Cybercrime and Cybersecurity: The Post-September 11, 2001, Reality." In *Transnational Organized Crime: Myth, Power, and Profit,* ed. Emilio Viano, José Magallanes, and Laurent Bridel. Durham, NC: Carolina Academic.

Von Lampe, Klaus. 2003. "Criminally Exploitable Ties: A Network Approach to Organized Crime." In *Transnational Organized Crime: Myth, Power, and Profit,* ed. Emilio Viano, José Magallanes, and Laurent Bridel. Durham, NC: Carolina Academic.

Von Lampe, Klaus, and Per Ole Johansen. 2004. "Organized Crime and Trust: On the Conceptualization and Empirical Relevance of Trust in the Context of Criminal Networks." *Global Crime* 6(2): 159–84.

Walker, Rob. 2011. "How Did a Hacker Group That Rejects Definition Develop Such a Strong Visual Brand?" *Slate Magazine,* December 8; accessed March 30, 2012.

Wapner, Paul Kevin. 1995. *Environmental Activism and World Civic Politics.* Buffalo, NY: SUNY Press.

Williams, Jody, Stephen D. Goose, and Mary Wareham, eds. 2008. *Banning Landmines: Disarmament, Citizen Diplomacy, and Human Security.* Lanham, MD: Rowman and Littlefield Publishers.

Williams, Leonard. 2007. "Anarchism Revived." *New Political Science* 29(3): 297–312.

Wong, Wendy H. 2011. "Is Trafficking Slavery? Anti-Slavery International in the 21st Century." *Human Rights Review* 12(1): 315–28.

———. 2012. *Internal Affairs: How the Structure of NGOs Transforms Human Rights.* Ithaca, NY: Cornell University Press.

Zetter, Kim. 2010. "WikiLeaks Was Launched With Documents Intercepted From Tor." *Wired.com,* June 1; accessed March 25, 2012.

———. 2011. "WikiLeaks Donations Topped $1.9 Million in 2010." *Wired.com,* April 24; accessed January 29, 2013.

Zittrain, Jonathan. 2008. *The Future of the Internet—And How to Stop It.* New Haven, CT and London: Yale University Press.

Zukin, Cliff, Scott Keeter, Molly Andolina, Krista Jenkins, and Michael X. Della Carpini. 2006. *A New Engagement? Political Participation, Civic Life, and the Changing American Citizen.* New York: Oxford University Press.