Digital Democracy and the Impact of Technology on Governance and Politics:

New Globalized Practices

Christina Akrivopoulou
Democritus University of Thrace, Greece

Nicolaos Garipidis
Aristotle University of Thessaloniki, Greece

Information Science
REFERENCE

Managing Director:	Lindsay Johnston
Editorial Director:	Joel Gamon
Book Production Manager:	Jennifer Yoder
Publishing Systems Analyst:	Adrienne Freeland
Development Editor:	Monica Speca
Assistant Acquisitions Editor:	Kayla Wolfe
Typesetter:	Christina Henning
Cover Design:	Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Digital democracy and the impact of technology on governance and politics: new globalized practices / Christina Akrivopoulou and Nicolaos Garipidis, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book brings together a detailed examination of the new ideas on electronic citizenship, electronic democracy, e-governance, and digital legitimacy, combining theory with the study of law and public policy"-- Provided by publisher.
ISBN 978-1-4666-3637-8 -- ISBN 978-1-4666-3638-5 (ebook) -- ISBN 978-1-4666-3639-2 (print & perpetual access) 1. Internet in public administration. 2. Public administration--Citizen participation--Technological innovations. I. Akrivopoulou, Christina. II. Garipidis, Nicolaos, 1971-
JF1525.A8D543 2013
352.3'802854678--dc23
2012045323

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 5
Action Potentials:
Extrapolating an Ideology from the Anonymous Hacker Socio-Political Movement (A Qualitative Meta-Analysis)

Shalin Hai-Jew
Kansas State University, USA

ABSTRACT

An ideology is defined as a set of ideas that "explains and evaluates social conditions, helps people understand their place in society, and provides a program for social and political action" (Ball & Dagger, 2011, p. 4). As such, these concepts underpin the actions of various groups and organizations, including that of the Anonymous hacker group, which professes no ideology or creed. Rather, the group has styled itself as a kind of anarchic global brain connected by various spaces on the Internet. This work explores four main data streams to extrapolate the group's ideology: the current socio-political context of hacking and hacktivism; the group's self-definition (through its professed values); the group's actions (through the "propaganda of the deed"); and the insights of others about the group This chapter defines the socio-technical context of this Anonymous hacker socio-political movement, which draws ideas from the Hacker Manifesto 2.0, which suggests the advent of a new economic system with the new technological vectors (mediums of communication). This movement is apparently pushing forth the advent of a new information regime in which the abstraction of ideas adds a "surplus" economic value that may be tapped. Styled as fighters against government tyranny, they are pushing hard against an international regime of intellectual property and information control by governments and corporations. This is being published in the spirit that (some) information wants to be free and that there is a value in direct discourse.

DOI: 10.4018/978-1-4666-3637-8.ch005

INTRODUCTION

Especially in our age of globalized communications, no amount of force can kill an infectious inspiration—a potential source of countermobilization, especially when it is spread through informal networks operating below the radar of state bureaucracy (Kurth Cronin, 2003, p. 143).

We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us (Anonymous).

Whatever code we hack, be it programming language, poetic language, math or music, curves or colourings, we create the possibility of new things entering the world. Not always great things, or even good things, but new things. In art, in science, in philosophy and culture, in any production of knowledge where data can be gathered, where information can be extracted from it, and where in that information new possibilities for the world are produced, there are hackers hacking the new out of the old. While hackers create these new worlds, we do not possess them. That which we create is mortgaged to others, and to the interests of others, to states and corporations who control the means for making worlds we alone discover. We do not own what we produce—it owns us (Wark, 2004).

The Anonymous hacker group has presented itself in the public media as an amorphous leaderless group that is all-pervasive but also nowhere. Its role is to keep governments accountable by restricting their instincts against totalitarian control (of information, of privacy, and of individual rights of association). It has a masked leader who is like the proverbial Everyman. It argues for a kind of individual and group freedoms that may be achieved with hacking, and it is guided by some of the ideas of the modern age—such as the idea that "information wants to be free." Its media optics are self-aware and self-promoting, an effort to reach out to their constituents and to win over more powerful allies to their cause. As a so-called self-organizing group with libertarian and anarchist leanings, Anonymous draws from The Hacker Manifesto and other artifacts of the electronic age. An ideology (or "policy package") is critical to a group because it is what is used to recruit group members and to rationalize the group's existence and its actions in the world. An ideology is defined as a set of ideas that "explains and evaluates social conditions, helps people understand their place in society, and provides a program for social and political action" (Ball & Dagger, 2011, p. 4). Ironically, Anonymous claims to have no ideology but does act on some core ideas (this strategy may be a part of the group's messaging and a kind of strategic ambiguity to make it more acceptable to many self-identifying members who opt-in on particular operations). Others have observed that this organization has "no coherent ideology, but a track record of considerable damage" (Sengupta, 2012). Their expressed values are a body of sentiments more than a comprehensive worldview. The organization may be conceptualized as self-organizing, with members opting in and out, and animating ideas capable of emerging from any sector is this dispersed organization (in the study of organizations, a lack of a strong core ideology means lesser abilities to maintain followership beyond the near-term).

While the organization claims not to have any ideology or creed [which may be part of an approach of "strategic ambiguity" (leaving open a broad range of options by not committing to a particular approach) to avoid alienating potential followers], this chapter takes the approach that "character reveals" over time. It is wholly possible to reverse-engineer at least a partial ideology based on the group's actions and public statements. For a global-level group with no figurehead, no charismatic spokesperson (and an anti-leader and anti-celebrity ethic), no dramatis personae (except a mask), and computer synthesized voiceovers of videos, this group all the more needs something to appeal to virtual followers:

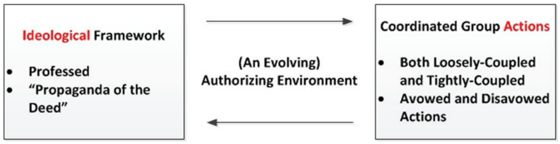
Although there is no authority figure or any leading group in Anonymous, there is 'policy, ethical sensibilities, and norms, all of which develop over time and often continuously formed and reformed in reaction to historical events' (Coleman, as cited in Ohhashi, 2011, p. 5).

Its international brand consists of its logo, its press coverage, and its ideas. The ideas then have to trigger its members, who ostensibly could hail from anywhere in the world. Virtually every public message, digital attack, legal action, ad private security firm research into the group leaves some publicly accessible residual trail. This chapter examines the mass media messages (YouTube™ videos, signs, and official statements) designed to rally supporters and educate the wider publics about their concerns, and the "propaganda of the deed" of this organization to extrapolate this group's ideology. Further, in the spirit of the 360-degree analysis, this group will also be analyzed for its ideology based on the research of those from security firms, targets, law enforcement, authors, former members, and other entities. This assumes that self-definitions are necessarily limited and potentially biased. Creating a more well rounded sense of the organization may result in a more insightful extrapolated ideology. Figure 1, "A Recursive Relationship between Ideology and Actions" posits a relationship between professed thoughts and actions.

Ideologies have shaped human conceptualizations of the world and their actions within it. According to Ball and Dagger (2011), there are four basic functions of an ideology in making sense of the world: "(1) *explanatory*, (2) *evaluative*, (3) *orientative*, and (4) *programmatic* functions" (Ball & Dagger, 2011, p. 4). An ideology explains the state of the world, sets standards for evaluating social conditions, orientates individuals with an identity, and sets forth a program of action. Most ideologies claim to defend a freedom (Ball & Dagger, 2011, p. 9); they are so-called liberating ideologies. MacCallum's triadic model of freedom shows how ideologies conceptualize an agent, an obstacle, and a goal, with ideologies enabling the achievements of particular goals. Because people tend to sense-make and are activated by ideas, ideologies are especially critical to understand. In human history, large social movements and political regimes have been harnessed and led for generations based on the power of organizing ideas—from democracy to imperialism to socialism to fascism/totalitarianism, and other forms. If ideas spark people to action and risk-taking (if they have repercussions), the motivating ideas that shape an "authorizing environment" (a context in which certain actions are considered normal and acceptable, but which would not be allowable in other contexts) should be understood. In light of the research that people strive to behave in a moral way even in "anonymous, one-shot interactions" (Bénabou & Tirole, 2011, p. 805) and in individual and collective behavior (p. 846), it is important to know the limits of moral action as conceptualized by the group, particularly one that sees itself as being revolutionary and altruistic, such as Anonymous. The portrayal of a group as altruistic to its constituents limits that group's actions; any perceived hypocrisy may result in the loss of supporters or even a backlash. Further, anger predicts offensive action tendencies within a dissident group, so it is important to know what may spark the group to action (in terms of contravention to the group's identity or ideals).

An ideology is not a static set of ideas. New ideologies are often seen as reacting to other

Figure 1. A recursive relationship between ideology and actions


Ideological Framework
Professed
"Propaganda of the Deed"
(An Evolving) Authorizing Environment
Coordinated Group Actions
Both Loosely-Coupled and Tightly-Coupled
Avowed and Disavowed Actions

competing worldviews, other explanations of reality. A political ideology evolves over time, and it evolves as the ideas are applied to the world. As changing leaders head up particular groups, the membership evolves, and contemporaneous hacker and hacktivist organizations (like Wikileaks) exist, ideologies will be re-framed and re-interpreted. As long as the ideas in an ideology have relevance to particular followers, these ideas will continue to free-ride humans as memes, and people will support a particular movement for a time as they are sparked by ideas. This means that this particular chapter may be accurate only for a particular time as the group evolves.

Extrapolating an ideology is important because this conceptual model may provide a sense of the group's motivations and potential actions, which are then only limited by the group's imagination, resources, and capabilities. Knowing a group's ideology may aid in terms of predictive analytics or projecting into the future. It may also aid in interactions with the group because those engaging them may be able to connect around shared ideas. To qualify these assertions, this chapter does not suggest any determinism between ideologies and actions. Certainly, there are many in-world examples of discrepancies between what is professed and what is actually believed and acted on in organizations (Argyris, 1993). What is being asserted here is that analyzing an ideology may indicate an organization's random walk (a general probabilistic trajectory with degrees of indeterminacy and uncertainty).

To infer Anonymous' ideology, the author will look at four main areas:

- The current socio-political context of hacking and hacktivism;
- The group's self-definition (through its professed values);
- The group's actions (through the "propaganda of the deed"); and
- The insights of others about the group.

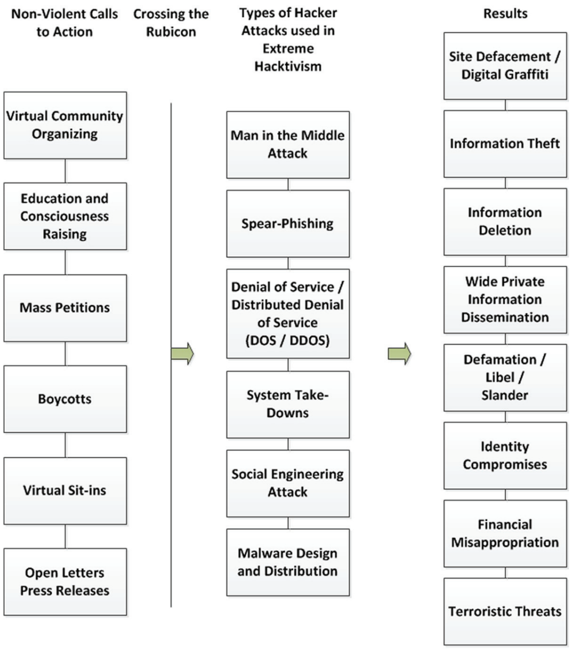
The Limits of Publicly Available Information

Given the secretive nature of the organization and the severe limits of the public information available (with much of it sourced in inaccessible ways), this systematic meta-analysis involves some severe limits (even though the author strove for comprehensiveness).

The limited information comes from statements by the organization (self-definition), the publicized actions of the group, and the insights of others that have varying relationships to the group. Most of the research involves hacktivism (hacker + activism) actions that have occurred over discrete (vs. continuous) time.

These include a range of activities that fits the traditional concept of civil disobedience but then also range into the unlawful. In Figure 2, "Hacktivism Range," this concept is demonstrated with hacktivists working within their rights (broadly speaking) to the left but crossing the Rubicon into potential illegality to the right. As Kreimer (2001)

Figure 2. Hacktivism range


Non-Violent Calls to Action
Crossing the Rubicon
Types of Hacker Attacks used in Extreme Hacktivism
Results
Virtual Community Organizing
Education and Consciousness Raising
Mass Petitions
Boycotts
Virtual Sit-ins
Open Letters Press Releases
Man in the Middle Attack
Spear-Phishing
Denial of Service / Distributed Denial of Service (DOS / DDOS)
System Take-Downs
Social Engineering Attack
Malware Design and Distribution
Site Defacement / Digital Graffiti
Information Theft
Information Deletion
Wide Private Information Dissemination
Defamation / Libel / Slander
Identity Compromises
Financial Misappropriation
Terroristic Threats

has observed, insurgent social movements have evolved their tactics based on the technologies of the Internet. It may be assumed that ideologically driven groups (as others) will experiment, reflect on the effects of their operations, and continually learn and improve their methods. Attacks that end with good results—respectable damage and plenty of media attention—may be repeated; attacks that resulted in their own loss of reputation or effectiveness as an organization may well be avoided.

Denning (2003) describes the threats to networked systems:

These threats involve operations that compromise, damage, degrade, disrupt, deny, and destroy information stored on computer networks or that target network infrastructure. They include computer intrusions and the use of network 'sniffers' to eavesdrop on network communications. They include the use of malicious software, namely, computer viruses, worms, and Trojan horses. They include denial-of-service attacks that halt or disrupt the operation of networked computers, usually by flooding them with traffic, and Web defacements that replace a site's home page with cyber graffiti, false information, and statements of protest (p. 91).

How the ideology is expressed in action reveals much about an organization because it is a kind of "costly signaling" beyond the "cheap talk" of ideology. An organization emphasizes its seriousness by putting it efforts where its apparent ideologies lie.

Simply because prior attacks have manifested in these known forms does not suggest that future forms of hacktivism extremes will remain at this level. Security experts suggest that early skirmishes may morph into more serious forms of attacks. There is certainly potential for escalations of strategies and attacks, combinations and re-combinations of various strategies and tools, and changes in attitudes, thinking, and additional learning. For virtual organizations that can crowdsource, it is possible that new techniques may evolve from any part of the loosely organized organization. Spin-off groups in various countries or regions may break off and conduct attacks on their own based on their interests and hacktivism skill sets.

Some security officials in the U.S. have even suggested that "world havoc" could ensue with impacts on major sectors of the economy of the shut-down of the power grid and other critical infrastructures (defined by Milone as "communications, power, transportation, banking, water supply, and public institutions" (2003, p. 75). A FawkesSecurity account promised that Anonymous would target "national infrastructure" and push for "global financial meltdown" in forthcoming "Lulzworthy" attacks (Lee, 2012).

What is not currently known publicly is legion: who the leaders of this group are, the conversations that may have happened off-line or in other spaces which have gone unobserved (except by the principals), the various technological and social engineering tools used in various hacktivist acts, and then plenty of "unknown unknowns".

Law enforcement has enormous traceback (the identification of where individuals entered the Internet and the paths they took, including through various bouncepoints, to arrive at a certain computer) and forensics capabilities, which are beyond that of a typical general researcher; they can track hacker actions in virtual audit trails into the ether. [Law enforcement gets involved when there are clear indicators of hackers having crossed the line into criminality in their vigilante actions, including unlawful access to private Intellectual Property (IP), illegal interception of information, impersonation of another, unlawful use of telecommunication equipment, forgery, theft of property, breaking into private systems and networks, violations of privacy, the making of threats, and launching Distributed Denial Of Service (DDOS, or pronounced D-dos) attacks and SQL (pronounced "sequel") injection attacks on databases. In recent accounts, law enforcement agencies in many of the world's developed nations have been establishing bodies of laws against cybercrimes and putting into place technological structures that enable law enforcement to meet evidentiary standards in the collection of digital information while protecting citizens' privacy and other First Amendment rights (Schwerha IV, 2004). Law enforcement, even independent of the hackers engaging in criminal activities, has been mapping hackers to understand their evolving capabilities (Glenny, 2011). Beyond a basic text analysis and access to publicly available information, this researcher only has access to publicly available and published information. The Anonymous organization itself may be maintaining its own history and "documentation." If that is even done, there is no access to the organization's internal record keeping. Given the limitations, this work will contribute in a small way to an understanding of a loosely coupled organization that has been around since 2006 and has been active and evolving ever since. The organization came about as a gathering of anonymous individuals interacting in the 4chan message board (Mansfield-Devine, 2011).

This board, with some 7 million regular users, is known for the ephemerality of its messages, with most threads spending "just five seconds on the first page and less than five minutes on the site before expiring" (with an average of 3.9 minutes as the median lifespan) based on *in situ* research over a two-week period in 2010 that involved the collection of 5,576,096 posts in 482,559 threads in their dataset (Bernstein, Monroy-Hernández, Harry, Andre, Panovich, and Vargas, 2011, p. 1). Further, 90% of posts made on the 4chan /b/ were fully anonymous users with identity signals "adopted and discarded at will" (p. 1). Its contents are often profane, pornographic, and anarchic; its users have evolved their own shorthand language, with its own underground value system (anti-authority, pro-individual, pro-lulz, and paranoid. Immersing in this culture enables users to try to influence the crowd, but it apparently involves exposure to being cognitively hacked.

The original "rules" of this space are known to be free-form and full of the 4chan Anon's "memes" collected as the "47 Rules of the Internet," with some of the famous ones reading: "In the Internet all girls are men and all kids are undercover FBI agents," (Rule #29) and "Anonymous is legion" (Rule #4). Some other parts of the rules suggest some features of the "hive mind": "Any topic can be easily turned into something totally unrelated" (Rule # 26) and "All your carefully picked arguments can easily be ignored" (Rule #11) (These rules have since morphed and evolved).

A Short Note on Semantics

To begin, it will be important to define a "hacker". The traditional meaning of the term referred to those who were expert in computing machines and systems.

> *Crackers are those who break into computers in order to achieve destructive ends. Though the media will often confuse the two terms, hackers are very different. "Hacker" was originally a term that was coined to represent an individual's deep understanding of computer systems and networks. Hackers use their skills to invent, modify, and refine these systems, often creatively using computers to achieve a goal for which the system was not originally intended (Levesque, 2006, p. 1203).*

In the present day, the term has evolved to include the work of those who break into computing systems for various aims, potentially more like the original meaning of "crackers." For the purposes of this work, though, the term "hacker" is the one used in the present day and not the original meaning.

Hacktivism, or hacker + activism, if it were to follow the rules of "civil disobedience" should follow the following general guidelines:

- No damage done to persons or property.
- Non-violent.
- Not for personal profit.
- **Ethical Motivation:** i.e., The strong conviction that a law is unjust, unfair, or to the extreme detriment of the common good.
- Willingness to accept personal responsibility for outcome of actions (Manion & Goodrum, 2000, p. 15).

In cyberspace, hacktivism has taken many forms, which go well beyond this civil disobedience ethos, and certain hacktivist ideologies may justify a greater sense of extremism. Further, several researchers have noted that what may be considered hacktivism by some may be considered cyberterrorism by others (Denning, 1999).

A HACKING AND HACKTIVISM IDEOLOGICAL SUPERSTRUCTURE?

The exercise of "cyber power" then refers to the ability to obtain preferred outcomes through "use of the electronically interconnected information resources of the cyber domain" (Nye, 2010, pp. 3-4). To build on the physical and virtual dimensions of cyber power conceptualization of Nye, Anonymous has the capability to deploy hard power using information instruments within cyber space (intra cyber space) as well as soft power (the effect of persuasion through messaging) and by setting norms and standards of hacktivist civil disobedience. Outside of cyber space, they use information instruments and the social networks to promote a "public diplomacy campaign to sway opinion" (Nye, 2010, p. 5). In terms of physical instruments, the organization takes advantage of open-source infrastructures for intercommunications—within and outside of cyberspace—in order to share information and to coordinate actions. Their concentrations of power are mostly soft power, and their hard power is in the realm of information instruments used in "intra cyber space." Nye defines the three faces of power in cyber space:

1st Face: "A makes B do what B would initially otherwise not do".

2nd Face: "Agenda control: A precludes B's choice by exclusion of B's strategies".

3rd Face: "A shapes B's preferences so some strategies are never even considered".

Based on Nye's definitions, Anonymous has some hard power in the 1st Face because of their Denial Of Service (DOS) attacks and their soft power in being able to potentially "change initial preferences of hackers." In the 3rd Face, Anonymous also has the ability to use information in a soft power way to "create preferences" among hackers and to affect what he calls "norms of revulsion" (such as in their stance against child pornography) (Nye, 2010, p. 7). This is a type of relational power in terms of how the organization interacts with other entities in society. Their capability set then involves both soft and hard power, with a focus on the first. Their propagandas of the deed do indeed convey a sense of threat to some entities, which may not want to tangle with the hackers and risk having information loss and public humiliation. Finally, Nye discusses the Relative Power Resources of Actors in the Cyber Domain (Nye, 2010, p. 10) which may illuminate Anonymous's relative advantages vs. the capabilities of the entrenched entities of government and private industries. He shows governments as having vulnerabilities such as high dependence on "easily disrupted complex systems, political stability, reputational losses" and organizations and highly structured networks as being vulnerable to "legal, intellectual property theft, systems disruption, reputation loss (name and shame)" and lightly structured networks (like Anonymous—author note) being vulnerable to "legal and illegal coercion by governments and organizations if caught" but having "low cost of investment for entry, virtual anonymity and ease of exit, (and) asymmetrical vulnerability compared to governments and large organizations (Nye, 2010, p. 10).

If Anonymous has anything like an ideological superstructure that scaffolds a worldview, which it denies, it could partially draw on some aspects of a manifesto (a public declaration of political principles and values) from an external sources. The McKenzie Wark version of The Hacker Manifesto (2004), which illuminates the social relations of production and the material forces of production, draws heavily on revolutionary Marxist ideas (and particularly the Hegelian notion of the master-slave dialectic) but ultimately sees the socialist and communist conclusions as ill-informed. The "false consciousness" of people in this conceptualization relates to the ownership and access to information—which should be free in a kind of gift economy, and the role of the "hacker class" is to build towards a gift economy utopia by setting information free. That's the essential dialectic, and much of it does apply to the work of Anonymous.

Beginning with Two Hacker Manifestos

The first "The Hacker Manifesto"/"Conscience of a Hacker" written by The Mentor (aka Loyd Blankenship) in Jan. 8, 1986, reads like a dialogue between a hacker of a younger generation who has finally found his niche in computers against an individual from the establishment with his "three-piece psychology and 1950's technobrain." Here, the teenaged hacker is cursed by the older generations as being an underachiever, but in the meantime, the hacker is coming into his own. The establishment thinks, "Damn kid. Tying up the phone line again. They're all alike..." but the hackers are finally coming into their own: "This is our world now... the world of the electron and the switch, the beauty of the baud.

We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call U.S. criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals." This serves as a celebration of a newly discovered power and a kind of rebellious shaking the fist at "the Man".

A more fine-tuned and informative "A Hacker Manifesto" (v. 4) comes from McKenzie Wark, and this offers a reasoned economic model behind hacking and the definition of hackers as their own class. In this conceptualization, everything in the world has its own abstraction, what is called "double spooking." Wark writes: "The fortunes of states and armies, companies and communities depend on it. All contending classes—the landlords and farmers, the workers and capitalists—revere yet fear the relentless abstraction of the world on which their fortunes yet depend. All the classes but one. The hacker class." Hackers are a sort of class that has "to hack itself into manifest existence as itself".

The hacker class, by identifying the latent abstractions of immaterial information underlying the world, creates a kind of surplus or additional value. Their new hacks supersede old ones, and it devalues the older ones…so hacking is seen as creating new information out of existing information. Such discoveries are a way of creating other potentials. It is in this abstracting of information that hackers run up against the ruling class that "owns the material means of extracting or distributing information, or with a producing class that extracts and distributes. The class interest of hackers lies in freeing information from its material constraints," writes Wark. Those who benefit from intellectual property as a means of production are termed the "vectorialist class," aka "the emergent ruling class of our town" or those who control the "vectors along which information is abstracted" ("vectors" may be understood as "mediums" or any methods by which information moves):

> *The vectorialist class is waging an intensive struggle to dispossess hackers of their intellectual property. Patents and copyrights all end up in the hands, not of their creators, but of the vectoralist class that owns the means of realising the value of these abstractions. The vectoralist class struggles to monopolise abstraction. Hackers find themselves dispossessed both individually, and as a class. Hackers come piecemeal to struggle against the particular forms in which abstraction is commodified and made into the private property of the vectoralist class. Hackers come to struggle collectively against the usurious charges the vectoralists extort for access to the information that hackers collectively produce, but that vectoralists collectively come to own. Hackers come as a class to recognise their class interest is best expressed through the struggle to free the production of abstraction not just from the particular fetters of this or that form of property, but to abstract the form of property itself (Wark, 2004).*

Hackers' abilities to abstract the world enable them to "break the shackles holding hacking fast to outdated and regressive class interests." The work of hackers may push human societies forward to "liberate productive and inventive resources from the myth of scarcity."

In a sense, the hacker becomes his or her hack based on the circular language in the manifesto: "The hack produces a production of a new kind, which has as its result a singular and unique product, and a singular and unique producer. Every hacker is at one and the same time producer and product of the hack, and emerges in its singularity as the memory of the hack as process" (Wark, 2004). The self is created through self-actions. The discussion of the surplus created by the hack offers a potential for a fresh contribution.

> *The hack produces both a useful and a useless surplus, although the usefulness of any surplus is socially and historically determined. The useful surplus goes into expanding the realm of freedom wrested from necessity. The useless surplus is the surplus of freedom itself, the margin of free production unconstrained by production for necessity (Wark, 2004).*

In this Hacker Manifesto, Wark portrays the hacker classes as working alongside the so-called producing classes to gain freedom from class domination. Wark writes: "The ruling class subordinates the hack to the production of forms of production that may be harnessed to the enhancement of class power, and the suppression or marginalisation of other forms of hacking. What the producing classes—farmers, workers, and hackers—have in common is an interest in freeing production from its subordination to ruling classes who turn production into the production of new necessities, who wrest slavery from surplus." In direct contravention of the Communist approach to centralizing the instruments of production in the power of the state, thus resulting in a new ruling class, hackers diffuse the power of the ruling class by challenging their primacy. Corporations are seen to monopolize intellectual property:

> *Patents and brands—and the means of reproducing their value—the vectors of communication. The privatisation of information becomes the dominant, rather than a subsidiary, aspect of commodified life. As private property advances from land to capital to information, property itself becomes more abstract. As capital frees land from its spatial fixity, information as property frees capital from its fixity in a particular object (Wark, 2004).*

In The Hacker Manifesto, hackers have a value to each successive ruling class because of their ability to abstract information into property, which has value. Hackers are seen as uniquely positioned to affect the world in a positive way, "when freedom from necessity and from class domination appears on the horizon as a possibility," which suggests a kind of possible utopia. To achieve this utopia, hackers have to engage in their activities "free from any constraint that is not self imposed." Further, any information created no longer falls under "the artifice of scarcity once freed from commodification"—and so can be used and re-used without artificial limits as a non-rivalrous good. Wark posits an idealized "social space of open and free gift exchange" in contrast to commodified and limited proprietary use of information by the vectoralists who are depicted as "parasitic and superfluous" and who are seen as dispossessing others by claiming ownership rights. Further, vectors are deployed in the world in highly uneven ways due to political and economic factors, not technological ones, according to this argument. In The Hacker Manifesto, Wark embeds a call to action:

> *The hacker class seeks the liberation of the vector from the reign of the commodity, but not to set it indiscriminately free. Rather, to subject it to collective and democratic development. The hacker class can release the virtuality of the vector only in principle. It is up to an alliance of all the productive classes to turn that potential to actuality, to organise themselves subjectively, and use the available vectors for a collective and subjective becoming (Wark, 2004).*

The work continues and argues that formal education promotes the existing power structure and is a kind of "slavery"—which enchains the mind and makes it a resource for "class power".

Vectoralists turn education into a "profitable industry." A true hacker pursues "the pure liberty of knowledge," not education. His or her true and foremost concern is "a free circulation of information, this being the necessary condition for the renewed statement of the hack." The manifesto allows for the hacker class to view the hack as a kind of property or "as something from which a source of income may be derived that gives the hacker some independence from the ruling classes." The freeing of information will unleash potential that would not be possible otherwise. Hackers have a high calling to free the world from the domination of those who hold proprietary control over information.

> *The arrest of the free flow of information means the enslavement of the world to the interests of those who profit from information's scarcity, the vectoral class. The enslavement of information means the enslavement of its producers to the interests of its owners. It is the hacker class that taps the virtuality of information, but it is the vectoralist class that owns and controls the means of production of information on an industrial scale. Privatising culture, education and communication as commodified content, distorts and deforms its free development, and prevents the very concept of its freedom from its own free development. While information remains subordinated to ownership, it is not possible for its producers to freely calculate their interests, or to discover what the true freedom of information might potentially produce in the world (Wark, 2004).*

In this worldview, the state itself strives to control or "police" representations. In that light, "hacking recognises no artificial scarcity, no official licence, no credentialing police force other than that composed by the gift economy among hackers themselves." In other words, the only law that hackers face is unto themselves. Hackers live then in a state of anarchy without recognition of any nation-state's oppressive role. This organization has called for "cyberspace independence from world governments" as a goal.

In a global class struggle, Wark points to a regressive and Luddite politics that focuses on the past and on national borders. "The other form is the progressive politics of movement. The politics of movement seeks to accelerate toward an unknown future. It seeks to use international flows of information, trade, or activism as the eclectic means for struggling for new sources of wealth or liberty that overcomes the limitations imposed by national coalitions," writes Wark, and hackers are moving towards this unknown future.

The master narrative of hackers is argued by some to be an extension of the radical ethos of labour struggles, which justified various acts of sabotage to benefit workers oppressed by management. Yet, the politics of hacking involves "a synthesis of many irreconcilable things" (Dafermos & Söderberg, 2009, p. 56). Johns (2009) suggests that present-day hacking (and free data haven endeavors) is part of the anti-patenting and pro-piracy approaches of 1960s pirate radio and the ideologies of Friedrich Hayek and Ronald Coase (p. 46).

CONSTRAINING HACKER ETHICS

The "hacker ethic," according to Steven Levy in *Hackers: Heroes of the Computer* Revolution (1984) consists of six basic tenets.

1. Access to computers and anything that might teach you something about the way the world works should be unlimited and total. Always yield to the hands-on imperative!
2. All information should be free.
3. Mistrust authority and promote decentralization.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better (Hacker Ethic, 2012).

Kizza observes the following additional ethics: "Hackers reject the notion that 'businesses' are the only groups entitled to access and use of modern technology. Hacking is a major weapon in the fight against encroaching computer technology. The high cost of computing equipment is beyond the means of most hackers, which results in the perception that hacking and phreaking are the only recourse to spreading computer literacy to the masses" (2009, p. 119), which suggests pro-social motives. Ramsdell (2011) cites Palmås and von Busch in their definitions of central motivations of hackers—to promote access to technology and transparent knowledge about it, to empower computer users, to decentralize control and to create beauty and exceed limitations (p. 5).

Who are Hackers? Hacktivists?

In his cyber-mystical work, Ramsdell writes rapturously of hackers:

> *The sublime is a meta-narrative for transcendence, often rapture, and most importantly, the experience of coming abreast of the limits and looking back to see the world anew. The connection to boundary exploration is easily made to hackers, who are the colonists—but really more like the rugged fur trappers, cowboys, and outlaws—of the manifest destiny of cyberspace. It is they who will see the digital sublime in its purest, jaggedness form before it is simplified and aestheticized for future waves to ogle. It is there—emergence dynamics flowering out of networked e-communities, spontaneous generation and blindingly rapid evolution of memes, whole vast swaths of the unknown. The myth lives and its pioneer is rewarded (Ramsdell, 2011, p. 11).*

Known hackers have been predominantly male, in part reflecting the male dominance in the IT profession (Taylor, 1999, p. 33; as cited in Kleen, 2001, pp. 2-46). Hacker teams tend to work in a "loose hierarchy" of 4-7 members with unique skill sets. Those who are successful tend to be "of above average intelligence, imaginative, curious, and inventive;" they are capable of conceptualizing technological capabilities that the original technologies were not designed to do. Many are loners, and many have an addiction to computing. They "believe they can do anything they want" and enjoy a sense of "power and achievement through the systems they have hacked" (Chantler, 1996, p. 62; as cited in Kleen, 2001, pp. 2-54). Malicious hackers may be motivated by a range of individual motivations—but these include curiosity, challenge, recognition, personal satisfaction, feelings of power, and governmental (the support of one government over another) (Kleen, 2001, pp. 3-11). If a hacker group may be studied in-depth for the "antecedents" to particular hacker attacks (e.g., what triggers the group's motivations and follow-on actions), their attack behaviors may be anticipated and often responded to with appropriate offensive and defensive measures (Jackson, 2012, pp. 35 - 36). Jackson (2011) cautions that the appearance of an antecedent will not guarantee predictable behavior, but it may indicate increased probability of that behavior; after all, "a group's training, guidelines, and teachings" interact with the antecedent (p. 43). A group's "teaching" involves its ideologies, which may both animate and constrain group actions.

Hacker activism (or "hacktivism") takes on a range of forms. Essentially, electronic direct action is taken to create social change. On the mild end, it may be conceptualized as a kind of political activism (some would call it "cyber-agitation") and expression, without laws being broken. At the extreme end, hacktivism may be illegal, may cause harm to others, and may wreak all sorts of damage. One author writes:

> *Hacktivism is a controversial term. Some argue it was coined strictly to describe how electronic direct action might work toward social change by combining programming skills with critical thinking. Others use it as practically synonymous with malicious, destructive acts that undermine the security of the Internet as a technical, economic, and political platform. Yet others associate it specifically with expressive politics, free speech, human rights, or information ethics (Krapp, 2005, p. 72).*

Hacker Methodologies and "the State of the Art"

There are numerous mixes of methods to compromise information systems. All systems on the WWW and Internet are vulnerable to potential hack. Even those with an "air gap" (e.g. not connected to the Net) may be vulnerable with the uses of mobile memory drives that may be introduced into a system and infect it with malware. Hackers may taken on identities of individuals who belong in a network and access information and intellectual property, resources, and relationships to which they have no legitimate rights (Kizza, 2009). Information may be intercepted. In a man-in-the-middle attack, information may be intercepted, changed, and then allowed to reach its natural destination—but now with false information or a malware payload. Hackers may violate individuals' privacy by capturing private information and releasing it to the public. They may engage in industrial espionage to swipe privy information. A penetration ("pen") cyber attack involves the unauthorized access to a protected system by bypassing security mechanisms (Kizza, 2009, p. 109). Social engineering involves breaching the human firewall by using psychological manipulations to gain access to privy information or systems access. This manipulation may involve taking on another's identity and getting an internal staff member to give over information or system rights to an outsider. It may involve creating a diversion in order to gain access. A hack attack may involve any number of objectives and tactics.

Kizza defines a hacking topology as inclusive of some of the following factors: the available equipment, the access to the Internet, the environment of the network, and the offensive and defensive security regime around the information system (2009, p. 122). In Kleen's conceptualization, information operations depend on a variety of factors: the working environment, the supporting information infrastructure, the technologies used, the vulnerabilities of each aspect of the organization, the levels of access to the technologies, the options for attackers (in terms of combinations of vulnerabilities), the other side's measures and counter measures. For an attacking organization, their capabilities, motivations (and limiting rules of engagement), and planning are critical factors (Kleen, 2001, 1998). A greater skill set may broaden organizational vulnerabilities. To understand Anonymous then, it would be important to look at the group's capabilities.

A number of IT security experts have observed that the current state of hacker attacks have been of the so-called "ankle biter" or "script kiddie" variety—those using publicly available tools that may have been partially "modded" (modified) in order to conduct particular attacks. [In the context of cyber attacks, in 2011, only 4 percent were seen as particularly challenging to the hackers. All the others were relatively low-level hacks (Rashid). Most such attacks did not involve 0-day exploits (or any undiscovered software or information system vulnerabilities that the software maker or system administrators are not aware of). Such exploits may occur prior to developer awareness (thus the "zeroth day" reference) and may result in devastating losses or damage. The efficacies of such attacks have been enabled in part by weak security setups in various organizations, with systems left unpatched, with simple-level passwords or password re-use (on multiple sites and accounts), and with a work staff prone to compromise through social engineering (there are many ways into and out of a system). Many of the socio-technical systems in use have not been sufficiently hardened against attack, and many do not have the sufficient surveillance to even know when an attack has occurred or sufficient forensics capabilities to analyze the aftermath of an attack (such as a trackback mechanism) and to make proper attribution for certain actions. However inelegant the attack, the costs to the targeted companies may be astronomical. The SQL injection attack by Anonymous-affiliated LulzSec in 2011 was said to cost $171 million for Sony Pictures to address, and that sum does not even take into account any potential lawsuits from the data spill (Henderson, 2011). Therefore, while the virtuosity of a hack is one measure of power, much damage may be wrought by the lower-end hacks.

To pull off an effective sophisticated hacker intrusion attack in which sensitive information is located and extracted, often without the awareness of the system administrators, requires two critical factors: expertise and deceptive stealth (Jackson, 2012, p. 18). There are current systems protection measures that involve signature or rule-based detection (such as the indicators that show certain types of prior-known attacks are afoot) and anomaly detection (identifying unusual behaviors on a network as compared to that network's baseline indicators), and then human expertise, but those approaches are too reactive and not sufficiently fast; rather, it's critical to anticipate and pre-empt would-be malicious hackers (Jackson, 2012, pp. 79 - 80).

Current generations of hackers tend to be young males in their late teens to early 20s, and they deploy low-level use of cyber tools. They often fail to erase their own tracks. There is usually only one compromised system in between the hacker's system and the target machines, which suggest that such attacks are highly trackable (Preuβ, Furnell, & Papadaki, 2007, p. 138). Based on known cases, they are apparently motivated by blackmail and hate. Often searches of compromised information systems are done manually, not with any sort of high-level program to scan. Their targets tend to be "private persons, companies, or educational organizations in an equal measure" (Preuβ, Furnell, & Papadaki, 2007, p. 137). Many will also brag about their exploits. The authors observe that many hackers take the "path of least effort" in achieving the system exploitation, with downloadable attack scripts easily found off Google and other Web-based search engines. Jackson, who has worked in cyber security for the U.S. Secret Service and the CIA, writes of hackers derisively: "A hacker simply needs to be an automaton and master only a very limited handful of attacks that can be repeated across networks, hiding behind the anonymity that the Internet affords" (2012, p. 119).

A creative and higher-end hacker skill set is thought to belong only generally to nation-states and possibly organized crime groups. These talent sets are rare, and while some may be willing to sell their talents as mercenaries, these skills are generally understood to be used in particular ways—notably by intelligence agencies and criminal enterprises. One of the tools of such high-end hackers involve the so-called undiscovered zero-day exploit—which refers to a way to compromise software or software systems—and for which no patch exists (and no awareness of the exploit's existence).

Rice (2008) suggests that gifted computer science graduates may discover only about 5-10 "significant or critical software weaknesses during their peak years"; a rare few others have found 30 or more vulnerabilities at the heights of their careers (pp. 118-119). The more known zero-day exploits, the broader the range of networks that may be entered and exploited or compromised. The attainment of such a high-end hacker skill set involves plenty of hours of immersion. It may also involve training—often formal—with high-level experts in the field. Rice (2008) warns of "dragons" that discover zero-day exploits but do not flaunt their capabilities or pursue the small prizes. Rather, they know to hold back and wait to attack with great potency.

This section has set the context for hacker activism. Some have argued that the types of attacks launched by Anonymous are not particularly sophisticated even if they do cause actual damage. Their abilities to cause harm are in large part because of a confluence of factors: the poor levels of security enabled in the 1970s technologies of the Internet; the lack of secure patching by system administrators; the power of dark-side social networking, and the prevalence of tools that may be (mis)used. "The low price of entry, anonymity, and asymmetries in vulnerability means that smaller actors have more capacity to exercise hard and soft power in cyberspace than in many more traditional domains of world politics," observes Nye (2010, p. 1).

SELF-PROFESSED DEFINITION

Anonymous was started as an Internet meme, a mass noun, in 2003, and it started its activism first with actions "for the Lulz" (FTL) or "I did it for the lulz" (IDIFTL) or Lulzy banter ("Light-hearted and humorous banter" [Coleman, 2011, p. 7]), for their own irreverent mischief-making amusement. A neologism, "Lulz" is a plural variant of "LOL" or "laugh out loud." This culture of pursuing "the pure joy of creating mayhem" typified some of the early hacks of the self-identified members of this group (which evolved from intercommunications in select message boards—social exchange spaces that use text and imagery for interactions, and distinct and unconnected Internet Relay Chat or IRC networks). One researcher found that the inner core of the Anonymous collective would go to IRC connectivity to talk in real time and this connection served as its core member "think tank" (Ohhashi, 2011, p. 5). This organization, in some tellings, emerged from a "hive mind" from a just-for-laughs organization to one with a political agenda to promote free speech, free information, and to (in some eyes) fight tyranny anywhere. Still, they were not known to engage in serious high-minded debates about these issues but rather in pursuing unsophisticated and "juvenile" approaches to issues (Mansfield-Devine, 2011).

In the lingo of the age, the participants in Anonymous may be conceptualizing this organization's work as a kind of "collective, ongoing flash mob" ("Anonymous," OhInternet). In leetspeak, which is based on an alternative alphabet for the English language used on the Internet, hackers strive to "pwn" ("own" or "dominate") others by their superior skills and virtuosity. "leet" (written as "1337") as an adjective describes prowess or skill in reference to an "elite" hacker. In a more serious comparison, their operations involve information operations, namely: "Offensive IO attempts to deny, disrupt, destroy, or otherwise control the enemy's use of and access to information and information systems" (Kleen, 2001, pp. 2-4). Members will "dox" ("document") anonymous others by tracking their Personally Identifiable Information (PII) and revealing that to the public as a form of harassment or punishment.

Anonymous is a loosely coupled organization based on some ideas may enable it to have resilience beyond a closely coupled organization—which may be weakened with the arrests of its leaders. This organization has been described as "rhizomatic," with a continuously growing horizontal underground stem system that puts out lateral shoots and "adventitious roots at intervals" (Coleman, 2011, pp. 2-3). Another analogy that has been used involves fractals, the patterned structures that repeat at the micro levels and at the macro levels. Conceptually, fractal organizations can increase exponentially and quickly, to outsized effects.

Gleick suggests that memes are ideas that may infect and colonize the human mind, and like some microbes, they can exist into perpetuity in the environment until they find other hosts to infect and parasitize. In other words, even if the various leaders of this collective movement are arrested, the organization itself may continue with a kind of resilience because of the decentralized structure. What connects Anonymous members seems to be an adherence to shared ideas and an interest in hacking. Their connectivity is electronic and occasionally physical (in real or analog spaces—such as demonstrations or sit-ins), and targets of attacks and mass media statements seem somewhat crowd-sourced. Theoretically and somewhat practically, such spaces are open to the public, but that does involve some investment of time and effort and trust building to get closer to the inner core of the virtual organization. Early knowledge of a potential attack may increase the response time available to an organization or individual to harden attack surfaces, whereas surprise attacks leave very little time for maneuvering.

This light-hearted pranking approach—bordering on vicious trolling harassment now and again—typifies one type of Anonymous attacks. Some targets are apparently whimsical and may not entail much of a payload in terms of any political messaging. The damage caused by their vigilante actions and hacks has ranged from apparently minor (putting electronic graffiti on a site, defacing a site, denying access to sites for short periods) to extensive (with financial accounts compromised, private information released into the wild, private information and accounts deleted and sites sabotaged, and public reputations ruined). The organization's willingness to engage in site intrusions and vandalism have elicited expressions of concern from U.S. government officials who fear attacks on the nation's disparate electrical grids and suggest that national security threats may emanate from this group (Isikoff, 2012). In another case, Anonymous China dispersed information about how government censorship of the Internet may be circumvented and warned the Chinese government of its ultimate demise (Ferran, 2012). The message they posted on hacked websites read, in both Chinese and English: "Dear Chinese government, you are not infallible, today websites are hacked, tomorrow it will be your vile regime that will fall." If this interpretation of this international group as a terrorist organization is to be accepted, those arguing this would have to make the case that the group has a political agenda to promote their sense of "justice" and are willing to use violence to achieve those aims (Cronin, 2003, p. 33). One researcher compares Anonymous to "the anarchists of the late 19th and early 20th centuries—albeit anarchists with a vastly greater network and far more ability to advance their agenda through individual action…But even more, they look like the non-state insurgents the U.S. has faced in Iraq and Afghanistan—small groups of non-state actors using asymmetric means of warfare to destabilize and disrupt existing political authority" (Rosenzweig, 2011, p. 2).

If the organization may be charted in the same way that non-state terror groups have evolved, there are fears that they may achieve a level of tradecraft or even a breakout capability that may threaten critical national infrastructures. "Cybotage" (cyber + sabotage) includes "acts of disruption and destruction against information infrastructures by terrorists who learn the skills of cyber attack" (Adkins, 2001, p. 12). Cronin (2009) makes a cogent argument for the criticality of primal motives in bringing in a wider base of support for terror groups and a need for alignment to larger "historical, economic, and political changes" in order to be successful (p. 91). Further, she points out that a majority of terror groups are not ultimately successful in their political aims, with group life spans of only about eight years (p. 92). While proximate or process goals may be achieved, such as the gaining of media attention, the long-term successes of such weak groups using weak strategies (as compared to the power and resources of nation-states) are rare.

That said, cyber-security experts have made a variety of comments about the actual skills of Anonymous, the collective or group. A few in the inner core of the organization are considered adept hackers. Some members of the group manage the electronics communications infrastructure used by the hacker collective. Some manage the media wing with press releases to both mainstream media and social media; even more sophisticated group members engage the media in long-term communications and the offers of exclusives to communicate their stories and further their interests. However, the majority of populist "followers" or sympathizers serve as drones by letting their computing machines be used for DDOS attacks. This is a case of using "resource-exhaustion" to take down target servers (Mansfield-Devine, 2011, p. 5).

Another type of activism linked to Anonymous relates to electronic civil disobedience, with DDOS attacks seen as a modern-age tactic of "trespass and blockade from earlier social movements" (Adkins, 2001, p. 8) or the "hack-in" in place of the traditional "sit-in." Some political themes of Anonymous have related to making information free, fighting child pornography, promoting freedom movements against dictatorial governments, and other more localized political (broadly defined as relating to power and its uses in the world) aims. This push for free speech rights suggests a strong libertarian tendency.

There is also a very firm AntiSec (anti-security) bent to Anonymous, which hacks into various law enforcement-related organizations, both public and private. A splinter group from Anonymous, AntiSec stands opposed to the computer security industry and advocates against the full disclosure of security vulnerabilities and exploits to the public.

Other attacks seem to establish the organization's credentials as hackers by public feats of derring-do supporting by the vast downloads of private information or financial hacking into individuals' accounts or listening in on law enforcement calls—purely for the bravado of the actions. The bigger the organization take-down, the higher the credibility out in the online universe and the greater the amount of online chatter and public attention. In the political economy of some parts of the Internet, individuals and groups build social capital and reputation by putting themselves at risk.

Finally, this organization has embodied a tit-for-tat strategy (returning in kind; punishing the other side when punished; extending cooperation when the other side cooperates) in an iterated infinite bargaining game. In the Net parlance, they are "b-slapping" those who would disagree with them or their tactics. This means that if they perceive anyone that is against the ideals or actions of the organization, they may target that entity or individual with various types of hacks and other expressions of disagreement. Theirs is a rebuttal using electronic means.

Some have compared this organization to an “anarchic global brain” connected by the electronic synapses of the WWW and Internet. “Anyone can use the Anonymous umbrella to hack anyone at anytime,” says Rob Rachwald, Imperva’s director of security (Perlroth & Markoff, 2012). The inclusiveness of this organization means that anyone who self-identifies may call themselves “anons” and participate in various activities linked to the group.

In this construct, the loose membership of the organization involve individuals who may never know who their actual “genius hacker” leaders are (estimated to be between half-a-dozen to a dozen by law enforcement sources who have been tracking this group) who identify targets, define strategies, and spark the activism (with various “calls to action” in social networking sites) in the organization and are its central core.

In a social network (sociogram) conceptualization, which focuses on the structure of an organization to understand power flows, the core leadership exercises concentrated power in directing the organization. While ideas can flow from anywhere in the network, the activating spark seems to come from a center. In the semi-periphery, there are those who handle the technologies: adding code to particular open-source attack tools or creating multimedia to convey the hacker collective’s messages. In the outer periphery are those who are automorphically equivalent actors—clones or other substitutables—who can bring the power of mass effect against selected targets. Within this construct, small clusters or cells may well exist with particular groups homophilously (like-minded individuals preferring similar others) and closely connected with potential shared interests, under the much larger umbrella of Anonymous.

Other Anonymous spinoff endeavors involve the launching of various attacks. Still others create the propaganda that accompanies many of the group’s campaigns and activities. This organization seems to have a flat hierarchy or may even be conceptualized as a loose social network of individuals with varying skill sets but a shared value system or worldview (based in part on a hacker and “information wants to be free” ideology). The “flash” actions have been observed by security personnel—for one attack (on the Vatican), a security firm observed that the initial call to actual launch of an attack took 18 days, with many “drones” self-radicalizing based on the call-to-action. Anonymous, from a majority of available accounts, may be characterized by a kind of fragmentation as a loosely coupled organization (Orton & Weick, 1990), which may make it more adaptable and resilient. As the organization itself has observed, Anonymous is based on an idea, which is difficult—if not impossible—to squelch from the environment. In that sense, this anti-authority meme of free information may be sufficient by itself to spark some action potentials (the transmission of nerve signals through cells) in this electronic brain. In the wired ubiquitous memetic culture, low-density networks of individuals may be activated to act on their political sympathies collectively (Underwood & Weber, 2011). Finally, while this organization asserts that it has no ideology, one can extrapolate one from its own statements; its targets and campaigns; and the findings of various researchers and publicly cited individuals in government and security agencies who provide yet another perspective.

Even from its early days, Anonymous has maintained an awareness of its public role and has focused on social media to release some of its messages and to engage with its multiple publics. One core goal of hacktivism is to draw attention to particular issues, so hacktivists “draw attention to particular issues by engaging in actions that are unusual and will attract some degree of media coverage” (Adkins, 2001, p. 9). The open-source anarchy movement "posits an elastic relationship between power and ideas in which non-State actors directly participate, thus affecting, in various ways, how anarchy operates," suggests Fidler (2008, p. 282), in a model which may shed light on Anonymous' engagements of a public dialogue (to shape the world). As an organization, its members are well aware of how media has a multiplier effect. They have had members help groom their image and clarify their main values. Further, they have used social media to deliver warnings and to conduct light debriefings post-operations.

In various physical demonstrations, they have taken to wearing Guy Fawkes masks with the smirky grin. Fawkes (Apr. 13, 1570 – Jan. 13, 1606) was a Brit who fought the Spanish in the Low Countries and is known for having taken part in the planning for the failed Gunpowder Plot of 1605, to restore the Catholic monarch to the throne. He was in charge of the gunpowder stockpiled beneath the House of Lords but was discovered. Shortly before he was to be hanged, he jumped off the scaffold and avoided being hung and quartered. In *V for Vendetta* (2006), the anti-hero "V" wore a Guy Fawkes mask. This knife-throwing anti-hero "V" was fighting what he saw as a totalitarian and fascist government. His approach to the world: "People should not be afraid of their governments. Governments should be afraid of their people" (which is derived from John Basil Barnhill, who said, "Where the people fear the government you have tyranny. Where the government fears the people you have liberty"). This popular film serves as an allegory of oppressive or intrusive government, which Anonymous uses as a rallying point and potentially a work of inspiration. A core point of the film is the use of fear to maintain power, and fear is a weapon by both sides—the government and the people. Guy Fawkes Day (Nov. 5) has been a day in which big targets are announced by "Anons," such as the promise to take down Facebook™ (Tennant, 2011).

GROUP ACTIONS: "THE PROPAGANDA OF THE DEED"

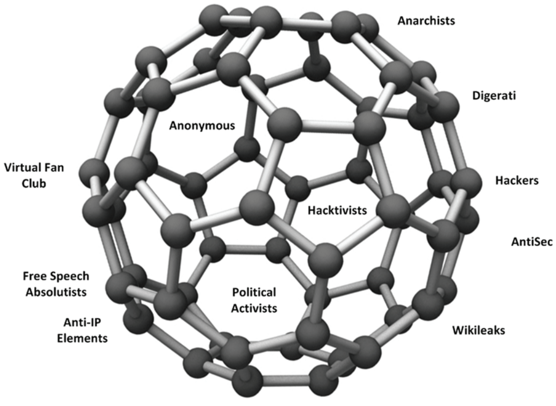
In the International Relations (IR) literature, in regards to politically motivated non-state actors, they communicate to the broader public using the so-called "propaganda of the deed." They use such often costly signaling to not only demonstrate their power but also communicate their sense of resolve. (A "costly signal" is one, which involves both risk and investment to an organization to prove its capabilities but also its commitment to a certain cause. A cost-free signal, by contrast, would be "cheap talk." These would include poses and statements but little in the way of action or follow-through.) Such actions may also enhance the commitment of members to the group. Based on this conceptualization, Anonymous has some unique signature "tells" (a change in behavior or appearance that reveals something about the individual; a term used in poker and gambling; what the other side does or doesn't do that reveals something hidden) that indicate particular actions as their own.

The actions of political groups may be understood as both striving to advance the objectives of the group and of providing a "shout out" to their respective constituencies—to raise their credibility and to recruit even more followers. All actions are also "polysemic" or many-meaninged; they may be interpreted in different ways depending on perspective.

The Company We Keep

Something may be said about an organization by the other entities with whom it socializes and/or aligns for political actions. In Figure 3, "In the Anonymous Hacker Socio-Political Sphere (Buckyball) of Influence," this depiction conceptualizes a loose-knit group of possible stakeholders that may be conceptualized as satellites of Anonymous. Individuals decide how much they want to self-select into the loose orbit of Anonymous and

Figure 3. In the Anonymous hacker socio-political sphere (buckyball) of influence



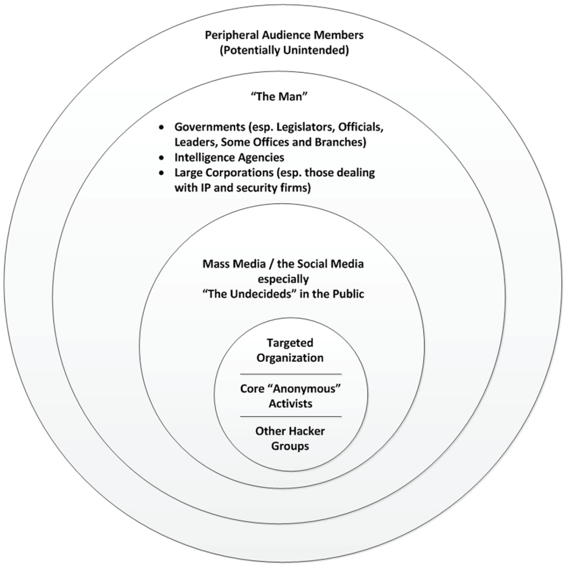
how much they may want to participate in one campaign or another. It is questionable how close any one member can get to the core membership, which is likely regularly probed by law enforcement and others. There are broad constituencies though who exist on the periphery of the group. (A "buckyball" or "spherical fullerene" is a molecule composed of carbon and appears as a hollow sphere or "empty cage" of 60 or more carbon atoms. It is used here not because of anything else than its general sense of a loose social network illustration. This illustration does not show the sense of an attraction to the organization, something that might be better indicated by some gravitational mass.)

A more nuanced and informative illustration would show fatter and thinner nodes and clearer lines of communication. As it is, this only provides a broad sense of the Anonymous sphere of mutual influence. This also captures the "all channel" reality of the Internet in which any code can theoretically connect with any other for possibly unusual and unpredictable coalitions of individuals with temporally shared interests. Anonymous has spun off various organizations, such as LulzSec (which hacks for the "laughs" or the "fun" of causing havoc and has been active on and off, with a self-professed hiatus) and AntiSec (which disrupts the security structures used on the Internet by hacking various private companies and government entities) hacktivist organizations. It is reportedly close to a hacker group known as Script Kiddies, Red Hack, and other groups—many linked to particular countries or regions. It has aligned beside Wikileaks organizations/movements, and also has stood behind individuals they see as typifying certain shared values like Julian Assange (founder of Wikileaks), Bradley Manning (the individual accused of leaking secret U.S. documents to Wikileaks), and others. Such organizations share a temporary mutualism of interests, which result in temporal alliances.

Part of this organizational influence involves the "soft" power of messaging to a number of individuals from different audiences. Figure 4, "A Conceptualization of Audience Members for Anonymous Acts/Attacks/Messages," offers a conceptualization of the various audience members who are apparently affected by Anonymous actions.

The actions taken by this group may be understood to be conveying messages to a number of potential audience members. The targeted or-

Figure 4. A conceptualization of audience members for Anonymous acts/attacks/messages


Peripheral Audience Members (Potentially Unintended)
"The Man"
• Governments (esp. Legislators, Officials, Leaders, Some Offices and Branches)
• Intelligence Agencies
• Large Corporations (esp. those dealing with IP and security firms)
Mass Media / the Social Media especially "The Undecideds" in the Public
Targeted Organization
Core "Anonymous" Activists
Other Hacker Groups

ganization that is the subject of an attack is the recipient of a direct message about the organization's displeasure with particular ideas, statements, or actions. Within the core group, there are others receiving direct messages include the core constituencies: the hacktivists and other hacker groups. The propaganda of the deed conveys a particular power about the group's potency and commitment to political ideals and actions. In the next layer out of the concentric circle would be the mass media, the so-called "undecideds" in the public who may choose to side with Anonymous's ideals and actions. Virtually all the known successful Anonymous "operations" were lauded with press releases, official statements, and information shared through social networking sites. In many cases, prior to attacks, the organization released information about impending attacks—both to verify their hand in the attack and to garner publicity to appeal to their various audiences. The organization invests a fair amount into their outreach and recruitment efforts, based on the videos they have released for public consumption through videosharing spaces like YouTube™ and microblogging sites like Twitter™. Their messages emphasize their legitimacy and moral rightness; some of their campaigns focused on a "Robin Hood" approach in terms of giving away hacked funds to charities (for example). In the third periphery would be "The Man," those elements of government and corporate power against whom Anonymous is fighting—for free information, freedom of citizens, and other issues. In the far external ring would be the peripheral audience members who are aware and may not even be the intended audience.

Beyond the different messages to the different audience members, one act may have multi-layered meanings. An ideological meaning may affirm the members' creed. It may convey a message about the organizational identity and brand—with the hack defining the hacker, the hacktivism defining the hacktivist. To do is an act of being. An operation may have political implications in terms of both soft (messaging and persuasive) and hard (actual) power. As the organization becomes more sophisticated and innovates new attacks, there may be technological messaging (think the allegedly state-sponsored software saboteur Stuxnet, Duqu Worm, and the espionage-based Flamer/Flame/sKyWIper, but at a much simpler level).

The Direct Targets of Anonymous Cyber Operations: Global and Local

The targets of Anonymous "operations" inform observers about what this pluralist and anomic interest group sees as its objectives. How a group formulates and acts on its "enemies list" may be used to understand a group's self-definition and ideology (Reagan, 2012). An analysis of documented targets shows a broad range of targets—from those who seem to be targets of whimsy (lulz-y targets) and those which are powerful and high-profile (various governments, corporations, and individuals). Some press accounts suggest that Anonymous calls its own work "guerrilla cyberwar" (Isikoff, 2011). Some targets are critical to certain local interests, and others are more obviously global in focus. As an organization, Anonymous stances have to go beyond mere symbolic help and moral support. They need to signal their resolve by having actual effect to bolster their threats and standing. The organization's issuing of prior warnings to some entities and organizations shows this attempt at projecting power even by the power of reputation alone. The dubbing of various larger operations with specific names makes their endeavors more memorable. The fallout effects of their operations have ranged also from annoyances to actual damage to reputations, corporate earnings, and privacy. If there is a signature in an analysis of the organization's targets, it is that the movement does not back off a challenge and will pursue high-profile medium-impact events—but with high message value.

Early operations—like the Habbo raids (social networking site), the Hal Turner raid (a "white-supremacist" radio host), and the Chris Forcand arrest (an "alleged Internet predator")—involved a range of almost idiosyncratic political issues. "Project Chanology" (2008) against the Church of Scientology's "Internet censorship" apparently followed Wikileaks' lead; this attack involved DDOS attacks (using the now-defunct Gigaloader.com tool for server load testing), prank calls, and so-called black faxes (to run down the toner of the receiving organization if they printed out faxes on paper). In the same year, there was an attack on the Epilepsy Foundation with flashing computer animations to trigger photosensitive and pattern-sensitive epilepsy—an operation which some Anonymous members disavowed as planted information by an adversary. Another attack was launched the same year against an online hip hop site, which involved defacement of the site and a DDOS attack.

Olson (2012) suggests that this organization came of age in 2008 with its first full-blown attack on the Church of Scientology but that its membership split in 2009 between those pursuing "lulz" and those pursuing political activism, which resulted in plenty of "e-drama" on the various message boards and communications channels (p. 93).

In 2009, a teenager who advocated "no cussing" came under attack with his personal information released to the public. Anonymous members rallied some 22,000 supporters to uphold the Iranian Green Movement (a protest movement) that aligned with The Pirate Bay (a site for illegal sharing of media contents) and Iranian hackers. These hacktivists also set up an information exchange between the world and Iran. In "Operation Didgeridle," the German and Australian governments were attacked for plans for ISP-level censorship of the Internet; Anonymous aimed to "protect civil rights" (Anonymous, 2012). In early 2010, Anonymous launched Operation Titstorm, a DDOS attack against the Australian government for its consideration of Internet filtering legislation. In Operation Payback (2010), this organization worked to deface sites and launch denial of service attacks against anti-piracy law firms and financial companies that closed accounts used for fund-raising by Wikileaks (including PayPal, MasterCard, and Visa. This organization deployed botnets of "zombie computers" that were infected by malware that enabled their takeover and use to attack these companies, resulting in a powerful capability at shutting down commercial-grade systems; Panda Security found that 90 percent of the DDOS-ing firepower for the attack on PayPal came from zombie computers, not direct Anonymous volunteers—even though the public relations wing of the organization preferred to credit their followers (Olson, 2012, pp. 116 – 119). While some of the organizers were well aware that the power to DDOS systems came not from hordes of activists but more from the botnets, they played up the idea of many engaged hacktivists to the press (Olson, 2012, p. 122).

Anonymous used the slogan "You call it piracy. We call it freedom" to explain their stance. "Operation Bradical" advocated for better treatment of Bradley Manning, the private first-class alleged to have released numerous confidential U.S. government documents to Wikileaks. Operation Leakspin (2010) was launched to support an activist effort to vet the Wikileaks cables in order to identify any previously overlooked ones. It was at this time that some activists in Anonymous created their own IRC channel for organizing battles against copyright:

> *Scattered between Britain, mainland Europe, and the United States, these mostly young men pooled their access to ten computer servers around the world. Some had rented the servers, some owned them, but with them, they could make a chat network that Anonymous could finally call home. No more herding hundreds of people between different places before getting kicked off. That month they established what they called AnonOps, a new IRC network with dozens of chat rooms just for Anons, some public and some private (Olson, 2012, p. 105).*

For a five-day period in 2010, the website of Kiss frontman Gene Simmons was targeted by an Anonymous hacker (who used the handle "spydr101"), who was arrested in 2011 by the FBI in late 2011. What raised the ire of the hacker? Apparently, the performer lamented the fact that the music industry could not sue "every fresh-faced, freckle-faced college kid who downloaded material" (Schwartz, 2011).

In 2011, Anonymous hacktivists broke into the Syrian Ministry of Presidential Affairs' email server as a protest against President Bashar al-Assad, who had been fighting peaceful protestors with deadly force. In February 2011, there were some public statements between Anonymous and the Westboro Baptist Church (in Kansas) but no final word on if Anonymous members actually launched an operation or whether the church was alleging an attack for its own publicity purposes (It turns out that both sides used the event for self-promotion, according to *We are Anonymous*).

In "Operation Pharisee," (in August 2011), the organization launched an attack that was observed from start-to-finish by security professionals—who documented the "reconnaissance and warfare tactics used by the shadowy hacking collective" (Perlroth & Markoff, 2012, p. 1). The target here was the Vatican, and the observing company was Imperva—which had been aware of the rally against the Vatican through YouTube™, Twitter™, and Facebook™. It took Anonymous some 18 days to raise the sufficient number of people for the attack, which ultimately did not succeed because of the security measures taken. (In a sense, the Vatican sites were used as a virtual "honeypot" or "honey net" or trap to elicit information about Anonymous' tactics). Anonymous expressed its displeasure at the conservative organization Americans for Prosperity for supporting Wisconsin governor Scott Brown (R) in his efforts to take away union bargaining rights. In a continuing of the organization's support for the Iranian Green Movement, Anonymous infiltrated a mail server for the government and copied 10,000 internal emails and images. This hacker collective launched Operation UnManifest in July 2011 by asking its members to modify copies of the manifesto by Norwegian mass shooter Anders Breivik to disrupt the distribution of his ideology (Mansfield-Devine, 2011, p. 5). In mid-2011, in Tango Down, these hacktivists targeted both the CIA and Alabama state to protest immigration legislation that the group saw as "racist." The group hacked into government sites, launched DDOS attacks, and harvested over 45,000 Alabamans' personal information. To promote their fight against firms supporting anti-piracy endeavors, this hacker collective launched DDOS attacks against a Spanish agency, a French government agency, Hustler, and the Recording Industry Association of America (RIAA) in Oct. – Nov. 2011. Then in late 2011, Stratfor Global Intelligence Service was attacked with private client information released to the public (often in "data dumps" to Pastebin (a Web application that enables the uploading of text for sharing), Torrent (peer-to-peer file sharing), Pirate Bay (file sharing site), and other sites—and often encouraging others to make sure of the information by illegally accessing others' accounts. (The damage from that attack was estimated to be $2 million [Olson, 2012, p. 396].) They have created mirror sites to ensure that loads of swiped code have been downloadable by any who might be interested. Private companies have turned to law enforcement to address such hacks, and some have even taken part in law enforcement stings to increase cyber security. Many private companies and publicly traded corporations have put in loss tolerance and stop-loss policies and measures to limit the damage that may be done by hacks. It is highly likely that downloads from the various sites that stolen code has been placed is monitored closely by law enforcement. The Irish political party Fine Gael was criticized and its site was hacked by Anonymous for their stance regarding censorship.

In 2011, some websites of the Zimbabwe government were targeted because of censorship of the Wikileaks documents. The Arab Spring movements in Egypt, Tunisia, Libya, Bahrain, Jordan, and Morocco were supported by Anonymous with various operations. (Olson [2012] writes that one of Anonymous's top hackers, Sabu [Hector Xavier Monsegur] had actually remoted in to a Tunisian citizen's account—with his permission—in order to launch an attack against that country's prime minister's site. The relative sophistication of this cyber attack was higher than the normal tactics which relied on simple downloads and commands).

A skirmish with a security firm occurred in February 2011. Aaron Barr, the CEO of HBGary Federal, broke news that his firm had infiltrated Anonymous. According to press reports, he correlated timestamps; a user in IRC would post something, and then a Twitter post on the same topic might appear a second later. He also posed as an Anonymous member in the various communications spaces that the organization was known to haunt. He tracked communicators with various unique identifiers. He matched handles to real names. Some suggested that his approach erroneously implicated individuals who were innocent bystanders. *Forbes* London-bureau chief Parmy Olson (2012), in her investigation into Anonymous, highlighted some of the holes in his investigations. Anonymous's response was apparently to hack the company's email, dump a trove of 68,000 emails from their system, erase files, and disrupt their telephone system. This coordinated attack involved a combination of semi-sophisticated hacks (in a hybrid attack), including spear (targeted) phishing. In an act of vicarious retribution, the Anonymous organization released privy information found on HBGary Federal servers, and select email messages that showed how the security company functioned were revealed. It also launched private attacks on Barr himself by taking over his Twitter feed and posting his alleged Social Security number. Press reports suggest that only 5 hackers were needed to "take down" HBGary Federal. Barr later resigned from this company (Anderson, 2011). This attack was seen by many as the politics of personal destruction and a potential miscalculation by the group.

Another interpretation of the prior attack may be that it was an expression of their protectiveness of their own. An April 2012 DOS attack on the British Home Office expressed concerns that European hackers were being extradited to face justice in the U.S. for their activities on behalf of Anonymous ("UK government website disrupted by hacker attack," Apr. 8, 2012).

In another case, the home of a cybercrime expert was surrounded by a Special Weapons and Tactics (SWAT) unit based on an elaborate prank by Anonymous members who were harassing him for a statement he'd made about cyberbullying (Newcomb, 2011).

The group made a stand against Indian corruption in 2011. In mid-2011, it launched attacks against 91 websites of the Malaysian government because of the country's blocking websites like Wikileaks and The Pirate Bay, which Anonymous saw as censorship.

In a local attack, in Operation Orlando (June 2011), the organization launched operations against various government websites in Orlando, Florida, in response to the arrests of members of Food Not Bombs for feeding the homeless in a local park against city ordinances. The group called for boycotts of Orlando. Operation Intifada (June 2011) resulted in attacks against a website of the Knesset of Israel based on assertions that Israeli intelligence had released the Stuxnet virus against the Iranian nuclear program.

Anonymous operations move into real or physical space as well. In August 2011, the group called for mass physical protects in response to the Bay Area Rapid Transit's plan to shut down cell phone service to discourage protestors from assembling non-violently to a police shooting of a rider. Members affiliated with Anonymous apparent "sent out a mass email/fax bomb to BART personnel" as well (Anonymous, 2012).

In Operation DarkNet (October 2011), this organization made a statement against child pornography by taking down 40 child porn sites and publishing the names of 1,500 people who frequented the sites. They invited the FBI and Interpol to follow up on that information. The same month, this group released a video asserting that the Los Zetas cartel had kidnapped one of their group members and threatened to publish personal information about the cartel members and their collaborators in mainstream society unless this individual was let go.

The first report of a possible extortion plot linked to the Anonymous name involved an attack on Symantec pcAnywhere (Ribeiro, 2012). One researcher speculates that this organization would not misuse credit card data or commit felonies (Ohhashi, 2011, p. 9). An email account of a member of Scotland Yard was accessed in early 2012, and in Opinfiltration, members of Anonymous recorded a call between the FBI and Scotland Yard about their group and posted it for public consumption. When a U.S. Marine plead guilty of killing two dozen unarmed Iraqi women and children in 2005 and was given a demotion instead of prison time, Anonymous posted 3 gigabytes of the email correspondence by attorneys in the case in early 2012. The controversial Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) were so unpopular with Anonymous members that a number of government and corporate targets were hit with DDOS attacks. This fight against SOPA and PIPA involved "the first direct and public activist malware from Anonymous." Here, individuals clicking on a link to get more information actually ended up triggering the LOIC that helped in the attack (Norton, 2012). In early 2012, Operation Blitzkrieg involved the targeting of neo-Nazi organizations, and there were links claimed between such organizations and an American presidential candidate. Mid-year, they participated in a live protest in Montreal against Bill 78, which restricted the freedom of association after weeks of student protests. On the cyber front, the organization took down the websites of the Liberal Party of Quebec, the Ministry of Public Security of Quebec, and a government site addressing police ethics. This organization has supported various Occupy protest movements against some of the U.S. government's economic policies, and it protested the International Monetary Fund's role in the Greek bailout. An Indian branch of the Anonymous hacker collective took on an East Indian company for its role in Internet "censorship." Other operations have been credited to this organization, but the main themes of these actions have been captured in the above examples.

From this overview of the organization's operations, it is clear that the leadership is politically aware and engaged. They use a variety of strategies to plan and launch their attacks. They have taken an "information wants to be free" (or "pro-piracy" stance—said another way) approach and has defined the access to information as a basic human right. Their hacks of governments have involved those that fall along a political range from democratic to authoritarians. The anarchic stance means that any government that takes an information-control or proprietary stance may become a target. The protection of workers' rights and pro-independence demonstrators seems to suggest a left-leaning agenda. However, the attacks on IP could suggest more of a Far Left agenda, with more of a focus on open-source than on property rights. From their selection of targets against whom they've acted, the ideology of Anonymous does not fit easily into any particular pre-set mode but seems to be evolving from a smorgasbord of ideas. Often, their actions seem reactive to what has occurred in the world already and is a move to change the direction of certain policies or practices. One reporter has observed that Anonymous "is fueled by a raft of causes" (Sengupta, 2012).

By contrast, Brey (2007e) argues the unsustainability of hacker ethics because absolutely free information means that intellectual property would not exist—and creators of works would not have an ability to benefit from their own labors; further, their property rights would be violated. Hacking then goes against the ethics if the information technology field. The Anonymous collective describes themselves as fighters against censorship.

Their actions suggest a kind of anarchism in how they comfortably take on various governments around the world. Their appeals to mass media and social media demonstrate a savvy about framing their actions in a political theatre and even a kind of cyber performance art. They are clearly able to conduct multiple attacks simultaneously or at least in close time proximity to each other. Host of Surprisingly Free (Mercatus Center at George Mason University), Brito has made the note that the organization has become more "self-aware" as they have engaged in more hacktivism (Brito, 2012).

Just because the organization has participated in some high-profile operations does not mean that it does not also potentially conduct operations quietly and without the usual attendant publicity. Some researchers have identified attempted takedowns that did not fully work, which the organization did not claim (Perlroth & Markoff, 2012).

Finally, what an organization says about itself for public consumption is clearly informed by their self-conceptualization and also by their organizational objectives. However, self-identity is seldom comprehensive nor particularly insightful. When objective information about an individual is not available, that may well lead to imperfect self-knowledge, and that knowledge by be affected also by "minor manipulations of salience such as cues, reminders and transparent veils of personal responsibility" (Bénabou & Tirole, 2011, p. 807). How they are seen by others may provide more critical layers of insight, particularly for an organization as elusive and private as Anonymous.

THE INSIGHTS OF OTHERS

For a group that is security conscious and tries to live by its name, Anonymous has been interpreted by law enforcement, researchers, thinkers, and other hacktivist groups. In public spaces, there are plenty of opinions about this group and how it functions. Tennant (2011) has called this group of "Anons" "a border-less, leader-less, ever expanding army of techno-vigilantes, misanthropic pranksters, human-rights crusaders, and free-speech absolutists" (p. 1). This section then addresses some of the insights of researchers who have studied this group and released their findings publicly.

The name Anonymous is a misnomer (and possibly wishful thinking) in several ways. It suggests that the organization is constructed of the proverbial Everyperson but also no one. The generic term is used as an attribution. This implies that individuals may participate in Anonymous activities and stay unknown—which is a near impossibility on the Internet, even with widespread uses of online aliases, anonymization techniques and tools, and privacy protections. It's also disingenuous to suggest that this group is leaderless. Published reports have suggested that there is a small leadership core that serves as the brainchild of this organization, and while others may make claims to membership, they may well be on the periphery or not connected to the organization beyond a self-identification. (The organization itself will demonstrate some aspects of the "black-sheep effect" in response to in-group members that have been seen to be disloyal—such as members who have been later identified to be working with law enforcement or those who opt-in as spokespeople for the group. In extreme cases, such members are expelled, and their accounts are deleted out of virtual communities by system administrators. The public and electronic lambasting of these individuals may play a role in keeping members in line).

There have been claims of Anonymous attacks to come that have not materialized within the operational window, and these have not been claimed by the organization. Some attacks claimed by people who claim membership in Anonymous have been directly outright disavowed. For example, in July 2010, when the Oregon Tea Party used Anonymous slogans for its event, the Party's site was flamed and defaced (Anonymous, 2012).

Other actions taken by self-affiliating members have resulted in public chidings through social media. One example involves the debate over splinter groups like Lulzsec posting private data like credit card and Social Security numbers on Web users and launching DDOS attacks against media organizations that did not provide coverage that the group could agree with. The group does not have a selected spokesperson but only a few who self-identify as pseudo-insiders who self-appoint to speak for the group in public—at great cost of public ridicule. The lack of access to the leadership has meant that some have gone to public channels to release "open letters to Anonymous" in order to try to get a response, with varying levels of success.

The Apparent Leadership

Cyber security researchers agree that there appears to be a core leadership for the group, even if their identities are not widely known outside a small circle. These are the individuals "running key Twitter accounts, producing YouTube™ videos and controlling important channels (some closed to the general public) on IRC servers"(Mansfield-Devine, 2011, p. 5). Others have identified the group's structure as a half-dozen "geniuses" surrounding by a lot of others willing to be used by the leaders of the group (Perlroth & Markoff, 2012) as drones, who turn their computers over to be used in attacks. Another suggests that "skilled programmers, security researchers, and system administrators" support this organization (Coleman, 2011, p. 2). A recent book, *We are Anonymous,* introduces some of the real-world individuals behind their handles Sabu, Topiary, Kayla, AVunit, Tflow, and others based on interviews and direct communications between the author and the various hackers. The leaders are depicted as more healthily cautious: going through Virtual Private Networks to mask their unique Internet Protocols; disconnecting their handles from any real-world identifiers on the Internet; using virtual machines to hack from; encrypting sensitive files and passwords; vetting all individuals angling for a position of trust, and taking tactical conversations private on closed IRC chat areas.

Funding Steams

As an organization, except for a few reports of self-proclaimed members trying to extort money from companies (or else their stolen information will be published on a website), Anonymous does not seem to have solicited funds. They may well free ride the structure of the Internet and certain freeware tools. Operations are apparently self-funded by the participants. Moneys that have been taken from compromised accounts seem to have gone to charities but even those would be reverted back to the original owners. Various hackers aligned with Anonymous have been accused of eliciting funds, nude images, passwords, and other concessions from their various victims—as part of pranking and apparently even extortion. Its spin-off LulzSec did solicit digital currency through Bitcoin and apparently raised some $7,500, which was distributed—$1,000 each—to its leadership after electronic laundering through moving the digital money through a series of accounts (Olson, 2012, pp. 264, 304 – 306).

The Technology Tools of Anonymous

One of the weaknesses of Anonymous is that they often have to tip their hand in public through communications sites to rally support, share information, recruit and mobilize, and share propaganda before they can launch a wide-scale or distributed attack. If the organization engages in too much security, they lose out on group organization efficiencies, particularly for a global organization firmly reliant on public information and communication technology. This means that any in law enforcement and security firms can have fair warning and can help various targeted entities and individuals prepare for the potential attack. They can infiltrate the organization with undercover agents (which partially explains the continual messages of paranoia expressed on the shared communications spaces). Further, targeted organizations may set up various "honeypots" or "honey nets" to record all aspects of an attack and learn more about the organization and its methods. Compared to the structured attacks "by transnational and national groups," those of hacktivists tend to be unstructured or semi-structured. Most use freeware or off-hacker-site tools. Most attacks are not sustained or sustainable currently by the organization but may be standalone or sequential but discrete attacks. Hackers self-reveal with every operation (Mansfield-Devine, 2011, p. 5), so their concerns should generally be both offensive and defensive. Anonymous' high response rates to provocations show a deeper lack of sophistication.

In some cases where they may act with stealth and secrecy, this involves hacks that are apparently only executed by some elite members of the group with specialized hacking skills. If successful, such events are then sometimes publicized by the collective. Researchers who have studied this group suggest that their language capabilities seem to be English, Spanish, and French—but with the group's use of voice synthesizers and translators, they could actually broaden their reach. Various media accounts have put the numbers of potential actors in an Anonymous operation at a wide range of participants from hundreds to about 22,000 ("Timeline of events involving Anonymous," Mar. 2012). A core approach to understanding a hacker group involves mapping its *modus operandi.*

For Anonymous, various DDOS (distributed denial of service) and DOS (denial of service) attacks have used a tool by Praetox Technologies called Low Orbit Ion Cannon (LOIC), which was designed for use to "load-test" or "stress-test" a site. This tool may be used as a Windows executable file that is downloaded and run from a PC, or a Javascript-based version that may be integrated into a Web page and used by site visitors. Since Operation Payback in 2010, an in-browser Javascript version of LOIC has been in use for various Anonymous operations.

The version used by Anonymous, according to one security researcher, has been retrofitted with a "crude command and control capability" to enable the launching of a broad-based attack against particular sites selected by the group's leaders/the group.

> *No skill is required to use LOIC. The Javascript version just needs the user to enter a target address and click the 'fire' button, although there are some optional settings. The Windows executable can be equally simple to use, and also offers a 'hive mind' option in which it will attempt to discover the current target from an IRC channel (with the IRC server and channel specified by the user). This makes it even easier for the user, who simply has to start the program running. Knowledgeable users can select a variety of options, such as type of packets sent (TCP, UDP, or HTTP), port numbers, and so on (Mansfield-Devine, 2011).*

The use of this tool as a hacking one is tantamount to sending "a menace letter with a return address" (Pras, et al., 2010, p. 8) because the tool captures the Internet Protocol (IP) of the user. The organization's power lies partially with its "surge" capacity in terms of activating individuals to take part (Olson, 2012, p. 49).

Law Enforcement and Anonymous

Arrayed against the hackers are those in law enforcement who train in both offensive and defensive cyber measures and who work to protect computer forensic evidence in order to ensure that the information is sufficiently pristine to be used in a court of law. One author suggests that the government may acquire a court's permission to put key loggers on a suspect's computer system to read every keystroke in order to learn more about potential criminal enterprises and to bring charges (Glenny, 2011). He also cites the case of

DarkMarket where American law enforcement ended up co-hosting a site which was used by "carders" to compromise the financial data of many around the world, so U.S. law enforcement could work with their colleagues around the world to capture those abusing the global financial system. One "public enemy #1" against hackers is John Vranesevich, whose computers track and "often archive, hacker chatter on some 142,000 different Web sites and I.R.C. channels. In other words, he has much of the hacking world wired for sound" (Burrough, 2000, p. 3).

Law enforcement agencies in a number of countries have arrested those involved in illegal hacking. Maintaining pseudonymity (anonymity over time) or even a deceptive self-presentation is a very difficult proposition given today's "traceback" technologies and criminal forensics techniques that are capable of revealing Personally Identifiable Information (PII) on a computer and network. There are unique identifiers for virtually all computing machines and places on a network. All accounts may be traced back to individuals. HTML files may be pathed to a local drive on which the file was created (this goes for other authored files), which can lead to real names, for example. Such unique identifiers lead to real-world identities. In cases where crimes have been committed, law enforcement has been effective in many countries in arresting the individuals, and various courts have had success prosecuting cases of hacktivism as cyber crimes and the work of malicious actors. The counter-narrative of law enforcement is that people are accountable for what they do online even if they may feel anonymized or invisible, and the inter-jurisdictional reality of Internet crimes may provide a challenge to them—but will not stop crime fighters from tracking down those involved in cyber crimes (even if there are hacktivist or political or ideological motives). There is no impunity for crimes actualized through computer technologies, even if there may be perceived less risk by the perpetrators. Their law enforcement actions suggest that hacking not only does not pay but does not really institutionalize lasting changes. There are other ways to make statements and have a voice in civic discourse. Hacking itself is illegal. The members who would risk law-breaking and who under-estimate the capabilities of law enforcement do so to their own detriment. Foremost, law enforcement's counter-narrative unmasks members and charges them with crimes—and uses many of the same tools to reach the public to convey this message as Anonymous uses to reach theirs. At an international level, some are working to turn "pirates of the ISPs" into "international pariahs" through political and policy strategies (Shachtman, 2011).

In the past few years, there have been arrests for attacks against private corporations and government offices—in The Netherlands, the U.S., Britain, Australia, Spain, Turkey, and other countries.

In terms of a future ambition, Anonymous has expressed interest in pulling off "Operation Global Blackout," which they described in a video and released on Facebook™. They expressed an interest in shutting down Facebook's 60,000 servers. In another attack under the same label, the group suggested that it would strive to bring down the Internet by attacking the root name servers (which connect URLs to particular numbers to make the various resources on the WWW and Internet locatable. These endeavors would be quite a bit more complex than the current levels of known Anonymous attacks.

Anonymous is like a meta-memetic, multi-user identity. No person is anonymous, and yet people act through Anonymous and refer to one another as anonymous or 'anon.' Anonymous has a written history spread across various wikis all over the Web.8 Anonymous has create crushing volumes of visual media from photo-shopped images ranging from cats (lolcats), to political threats, to porn created to satisfy one of their central tenets: Rules *of the Internet: Rule 34: If it exists, there is porn of it. No Exceptions (Ramsdell, 2011, p. 8).*

In terms of counter measures, law enforcement has a number of ways to identify members of the organization. They may map out the actual social networks behind hacktivist groups. They may monitor sites where swiped information has been placed for download, and they may use the legal system to force private corporations to turn over information about users. Law enforcement has been known to use shell accounts to emulate members of a company or organization in order to elicit information about such groups and their demands.

Various governments have been putting into place legislation to increase law enforcement powers to pursue those who launch cyber attacks. To protect its own freedom of movement and in line with their stated goals, this organization has taken on the controversial Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA), both of which went down in defeat. Then, in early 2012, the Cyber Intelligence Sharing and Protection Act (CISPA) passed the Senate. The group put out a video calling U.S. citizens to contact their legislators to vote down this measure, which would enable deep packet inspection of communications on the Internet.

An Extrapolated Ideology

The Anonymous hacker collective draws from various elements of popular culture in order to elicit support from the larger population and to pull off their various operations. While their actions do apparently draw from Wark's The Hacker Manifesto and from *V is for Vendetta*, the group seems to be even more responsive to real-world news and a worldview of keeping the Internet free from government interference of any kind. Their ideology is a flexible one that evolves with the world's issues and events. As such, it must be understood as a malleable entity defined by the (active) members of the organization.

Theirs is also not an all-encompassing doctrine concerned with humanity's external and internal well-being, the state of his soul or spirit, human livelihoods, but rather, a sliver of human concerns—related to human freedoms from government controls and the freeing of information from others' control.

At one end of the continuum, the Anonymous hacktivist collective seems to subscribe to a form of extreme libertarianism. While Propertarian libertarians suggest that there should be no violence against private property, this hacktivist collective apparently takes a non-propertarian libertarian approach in that their role is to abolish authoritarian institutions that control various means of production and subordinate the majority to the property-owning class. At the far end of the spectrum are the anarchists who profess no use for government even in a limited sense and so challenge all levers of government power head-on.

Definition by negation may be illustrative here as well. As an ideology, theirs is secular, non-theological, non-religious, or a-religious. There is nothing here that is particularly transcendent. Much is left to silence, unaddressed. The progress that is promised is economic. By implications, humans may advance with more access to protected information.

The only universality is that of a practical lived world in which the group pursues the unleashing of the power of information and ideas—through illicit means, which do not respect the rights of governments or of private industry. Their tenets focus around the action of the hack and artful deception to achieve their aims. (In a way, the methods define the group.) It alludes to a past and a present in which those with the power—the Man—would deny others access to the liberating freedom from released information. This Anonymous ideology promises a kind of altruistic participation in a larger cause without necessarily conveying an identity. After all, to belong in the inner circle would require a rare skill set. To belong to the periphery may be as simple as clicking on a button to participate in a virtual takeover that may leave the illusion of achieving an aim without cost and without law enforcement knowledge. This act may give the illusion of empowerment, at least for a brief moment.

The "End of History" According to Anonymous?

What would a utopian ideal under an Anonymous ideology look like, if taken to an extreme logical end conclusion? In this thought experiment, all information would be "free." There would be no secrets, nothing protected, no "security" around information. People would share what they invent, if they chose to invent. People would be liberated. There would be no governments to struggle against. Without the hierarchies of information, people would theoretically be classless. People and entities might be more accountable with everything known or knowable, or would they be more blasé to the revelations of each other? With no structured governance, how would people socially organize? With no private ownership of information, would other property rights also disintegrate? (Would people be able to own property or land or moneys, for example?) Would they connect virtually through their various computing machines? Would this end mean the end of the hacker, with nothing to hack? Does Anonymous only exist in symbiosis with the extant power structures of nation-states and multi-national companies? Would this mean a surplus from abstraction, and what would that surplus look like and mean? If this were the "end of history," would it be a desirable state? Would it be practical? Would it align with human nature, as people know it to be? (The "thought experiment" here may be too heavy of a stress test on a nascent ideology, but there is a value in trying to visualize what an ideology may look like put into extreme practice—even though the real world often moves to "contain" such ideologies and practices that challenge the larger system).

Figure 5, "A Wordle Tag Cloud of the Anonymous Hacker Collective's Wikipedia Page," offers a simple text analysis to gain a sense of the popular recurrences of terms on that page. The URL used for this particular tag cloud was http://en.wikipedia.org/wiki/Anonymous_%28group%29.

This tag cloud shows the predominance of the group's name over any of its specific issues—which are referred to in much smaller text. The organization's reputation is very high profile and possibly much more outsized than any one attack or another. This may show the predominance of the meme. In one microbial analogy, while organizations have life cycles and beginnings and ends, memes may be more like latent endospores that may exist many hundreds (or eternities) of years in the environment and not have expression in a host until they are picked up and activated (potentially pathogenically). Aspirants or new converts to a group (known colloquially as "wannabe's" or want-to-be's) tend to take more risks to prove their mettle (to signal their new identity and commitment) and may be instigated to take part in ever more virulent attacks to increase their chances of acceptance by the in-group. Peripheral group members tend to experience more group loyalty if they anticipate future acceptance; peripheral group members tend to experience less group loyalty if they anticipate future rejection (Jetten, Branscombe, Spears, & McKimmie, 2003). Those who are insecure in their in-group identity tend to react more extremely to in-group members who are seen as disloyal because of their foundational insecurity and to out-group members who might challenge that identity (Branscombe, Wann, Noel, & Coleman, 1995). The social costs of misidentification with an out-group (such as law enforcement) could have high negative repercussions on a virtual group member. Further, in virtual groups, those minimal groups who are brought into subgroup assignments tend to experience greater in-group vs. out-group identification (Wang, Walther, & Hancock, 2008), which suggests that tasked individuals may emotionally relate more closely to the virtual organization.

Figure 5. A Wordle tag cloud of the Anonymous hacker collective's Wikipedia page

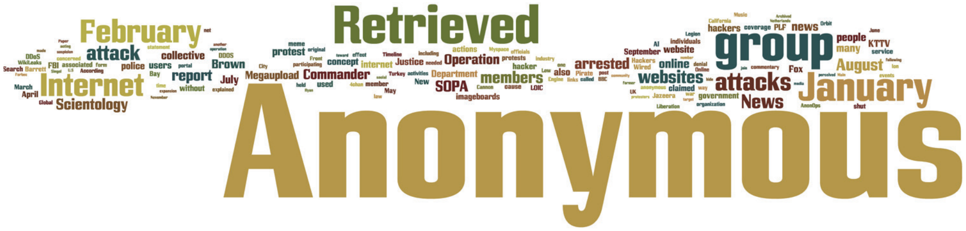


Figure 6. A wordle tag cloud of Anonymous in the Twitterverse

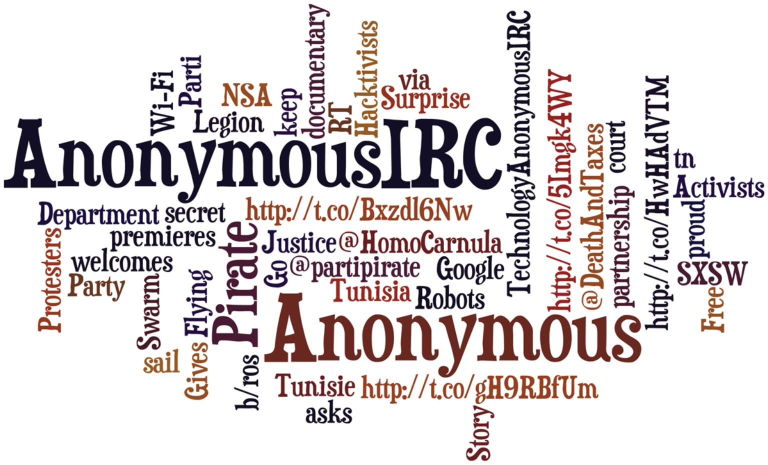


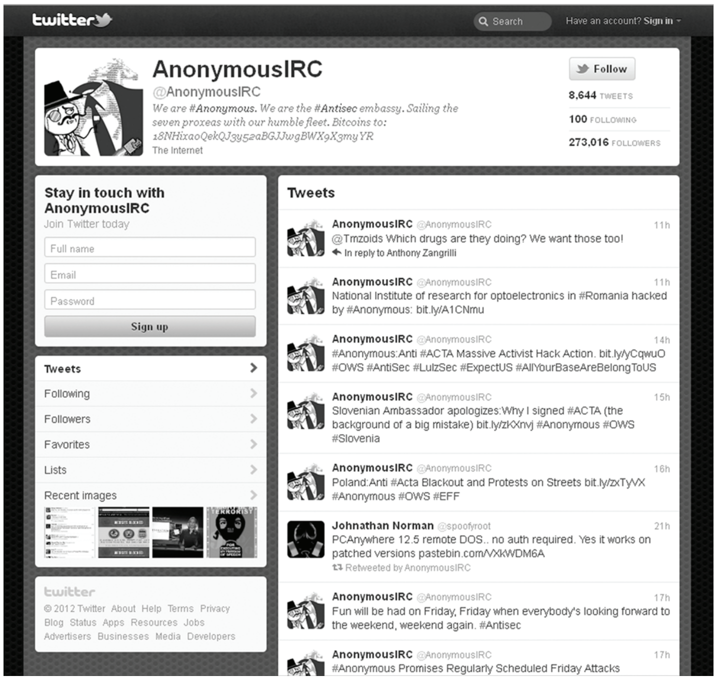
Figure 6, "A Wordle Tag Cloud of Anonymous in the Twitter Verse," highlights some of the terms that are popular in relation to micro-blogging about the Anonymous group at that particular time slice. What is trending may very much relate to a current news story or public release by the group or some other factor. These words refer to some of the mystique of the organization, referring to "secret" and the National Security Agency (NSA), the hyper-secretive U.S. signals intelligence organization. The URL used in this particular tag cloud is http://twitter.com/#!/anonymousirc.

In the Twitterverse, Anonymous involves a broad range of trending issues. It is a relevant organization that has sparked broad conversations about the roles of the Internet, information, and government. Figure 7, "A Screenshot of the Twitter Feeds Related to AnonymousIRC" provides a sense of the user interface for this group and a sense of the brief discourses.

In the Internet universe, an event has not occurred if it is not present somehow in the electronic space. In that sense, Anonymous has left tracks on the public track and also much in private spaces. In Internet time, much of these will have changed, and other operations will have come to the fore.

Another analysis, enabled by NodeXL (from the Social Media Research Foundation), shows a network of social microbloggers that is intensely concentrated in terms of relationships, with some pendant nodes on the periphery. Figure 8, "Anonymous Hacker Community by Tweeting Interests (per NodeXL and using a Harel-Koren Fast Multiscale Algorithm)," shows 836 vertices (individual nodes) that have recently "Tweeted"

Figure 7. A screenshot of the Twitter feeds related to AnonymousIRC



AnonymousIRC
@AnonymousIRC
We are #Anonymous. We are the #Antisec embassy. Sailing the seven proxeas with our humble fleet. Bitcoins to: 18NHixaoQekQJ3y52aBGJJwgBWX9X3myYR
The Internet

8,644 TWEETS
100 FOLLOWING
273,016 FOLLOWERS

Tweets

AnonymousIRC @AnonymousIRC 11h
@Tmzoids Which drugs are they doing? We want those too!
In reply to Anthony Zangrilli

AnonymousIRC @AnonymousIRC 11h
National Institute of research for optoelectronics in #Romania hacked by #Anonymous: bit.ly/A1CNmu

AnonymousIRC @AnonymousIRC 14h
#Anonymous:Anti #ACTA Massive Activist Hack Action. bit.ly/yCqwuO #OWS #AntiSec #LulzSec #ExpectUS #AllYourBaseAreBelongToUS

AnonymousIRC @AnonymousIRC 15h
Slovenian Ambassador apologizes:Why I signed #ACTA (the background of a big mistake) bit.ly/zKXnvj #Anonymous #OWS #Slovenia

AnonymousIRC @AnonymousIRC 16h
Poland:Anti #Acta Blackout and Protests on Streets bit.ly/zxTyVX #Anonymous #OWS #EFF

Johnathan Norman @spoofyroot 21h
PCAnywhere 12.5 remote DOS.. no auth required. Yes it works on patched versions pastebin.com/VXKWDM6A
Retweeted by AnonymousIRC

AnonymousIRC @AnonymousIRC 17h
Fun will be had on Friday, Friday when everybody's looking forward to the weekend, weekend again. #Antisec

AnonymousIRC @AnonymousIRC 17h
#Anonymous Promises Regularly Scheduled Friday Attacks

about the Anonymous Hacker collective. This sampling was taken during a time when there are efforts against the Syrian regime in the Syrian civil war (in terms of a publicized Anonymous operation). The algorithm used to display the graph results is the Harel-Koren Fast Multiscale view. This search was conducted with a maximum limit of 1,000 nodes for both efficiency of search and for manageability of the data.

The visualization shows an intense complex of interactive nodes in the dark area at the center of this network and multiple other spinoff groups with other centers (or influential nodes). Another visualization of the same data may be done using a Fruchterman-Reingold algorithm.

Figure 9 shows more of some central influential nodes which connect to many on the periphery. This visualization is from the same data. The graph metrics for the Figures 8 and 9 visualizations are shown in Table 1, "Graph Metrics for the "Anonymous Hacker" Twitterverse in December 2012.

In terms of reciprocated "following" of each other's microblogs, the network seems fairly distributed, without many mutual connections. This could suggest that the information about the

Figure 8. Anonymous hacker community by tweeting interests (per NodeXL and using a Harel-Koren fast multiscale algorithm)

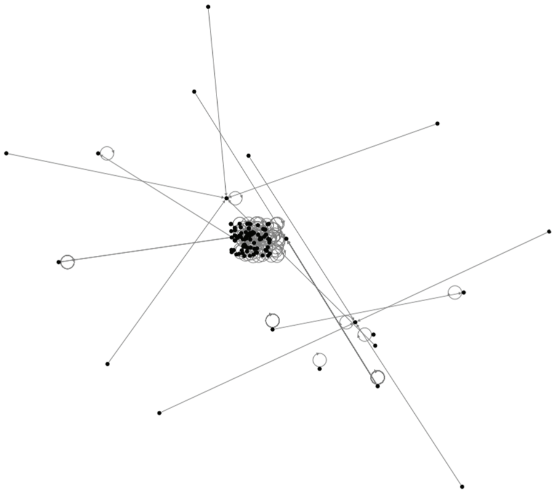
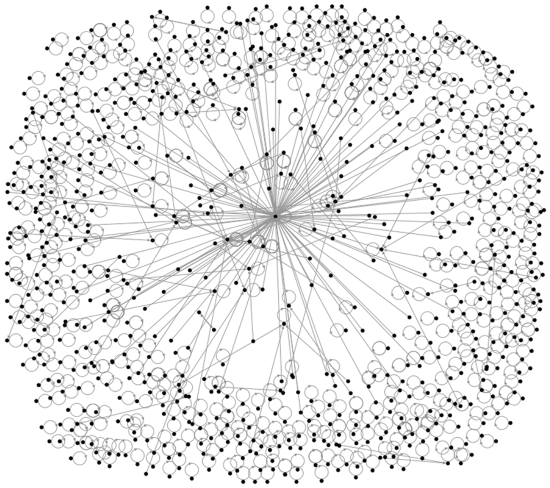


Figure 9. Anonymous hacker community by tweeting interests (per NodeXL and using a Fruchterman-Reingold algorithm)



Anonymous Hacker collective appeals to many separately from mass media and social media coverage, and they are each communicating with their various smaller networks and social groups. This shows something about the appeal of the Anonymous message. The largest cluster consists of 113 in one group based on the sharing of the 140-character messages. The graph is very low in terms of density, at 0.00024783.

Ironically, if this collective is pushing for more open-access to information, their actions are sparking pushback from private sector companies that are calling for a "collective defense" of this information commons (Charney, 2010) and more stringent controls on the Internet. In the military and government vein (public sector), countries are calling for a cyber counter-insurgency strategy. While offensive capabilities are constantly changing, so far defensive ones, and where vulnerabilities occur is where there are serious or temporal gaps in the defense. With some two billion people online, a range of vulnerabilities are possible for the civilian unhardened targets.

Table 1. Graph metrics for the "Anonymous Hacker" Twitterverse in December 2012

Graph Type	Directed
Vertices	836
Unique Edges	775
Edges With Duplicates	569
Total Edges	1344
Self-Loops	1088
Reciprocated Vertex Pair Ratio	0.011695906
Reciprocated Edge Ratio	0.023121387
Connected Components	668
Single-Vertex Connected Components	635
Maximum Vertices in a Connected Component	113
Maximum Edges in a Connected Component	411
Maximum Geodesic Distance (Diameter)	6
Average Geodesic Distance	2.292391
Graph Density	0.00024783
Modularity	Not Applicable
NodeXL Version	1.0.1.229
Readability Metric	**Value**

CONCLUSION

In 2011, hacktivists conducted only 3 percent of 855 data breaches investigated (and 174 million compromised records lost) but in those breaches stole more than 58% of the compromised data for the year (with criminals pursuing funds accounting for the rest) (Rashid, 2012). Even so, data theft is a relatively new expression of protest.

Prior to March 31, 2012, Anonymous promised to take-down the Internet by attacking its root servers handling the Domain Name System or "DNS" (the core of the Web's infrastructure that help link URLs to the actual servers); that date came and went without noticeable incident (Sengupta, 2012). However, if anything, that showed that the organization has an ambition for "spectacular" hacks that would trump prior hacks—as is suggested in escalation theory in the International Relations (IR) literature. The tendency towards outsized claims has affected spinoff organization LulzSec, which has claimed to "backdoor" a software company's anti-virus, which the company denies. Other attack claims have been made with no response by the target organization or business. An organization may be understood to comprise a wide range of factors. In the murky realms of the Internet, verification of claims may be hard to come by. Anonymous, LulzSec and AntiSec have been known to deface sites with false news stories (such as those including Tupac Shakur being alive or Rupert Murdoch being found dead or a president of a Western nation having been assassinated). Given such standards of engaging the world, their method of making a statement undercuts their own veracity. Hoaxing has become such a part of the culture and actions of some hacktivist organizations that announcements often come with reporter speculation that the assertion may well be a ploy.

On a more down-to-earth scale, an organization may be analyzed to understand its potency. Ideally, these would be questions posed at the beginning of the chapter and answered in the body text, but rather, the questions are posed here to show the severe limits to what is currently known about the organization.

Profiling the Hacker Collective/Organization

Some questions that may inform watchers of Anonymous involve the following:

- The Leadership
  - What is the vision of the leadership of the organization?
  - How is this vision expressed? How is that vision interpreted?
  - What are the leadership capabilities of the organization's leaders? Are they capable of rallying a broad range of people?
  - How are targets selected?
  - Is the leadership in control of the various fronts on which it is fighting?
- The Membership
  - What are the self-identities of the participants of the group?
  - How long do they tend to stay with this organization (their length of tenure)?
  - What are main causes (motivations) for joining the group, and then for leaving the group?
  - How strong is the commitment of the participants of the group?
  - How is the membership trained up?
  - How do members evolve? Do they "outgrow" the organization? What do they move to? Are they assimilated into the mainstream?
- Organizational Culture and Dynamics
  - What sort of organization is this?
  - What is the organizational culture? What informs this culture?
  - What are its motifs? Its symbols? Its main values?
  - How closely does the group hone to its stated values?
- Organizational Skill Sets
  - What are the capabilities and skill sets of the organization's leaders?
  - What are the skill sets of the organization (the "followers")?
- Organization Resources
  - How well funded is the organization? What are the resources of the organization?
  - How coherent is the organization's agenda? Who sets the agenda? How independent (vs. reactive) is the agenda?
  - What contributions are provided to the organization by its followers (if any)?
- Information Flow
  - Where does the organization get its information?

  - How does the organization release information?
  - How does it communicate with its followers?
  - How does the organization reach the media? How coherent is its message?
- Engagement with the Larger Publics
  - How much support or buy-in does the organization have from the larger public?
  - How appealing are the messages of the organization to the larger public? What is the "soft power" of the organization?
- The Attacks and Operations
  - How effective is the organization in projecting an independent, non-state-based anarchic power?
  - How much power does the organization have in creating real change? Or is the group fairly diversionary in approach?
  - How persistent or sustainable are their operations?
  - How technologically and socially and informationally sophisticated are their attacks?
  - What combinations of tactics are used?
- Spin-Off Groups
  - How inspiring is the original group?
  - Who are allies with this organization?
  - What are the spin-off groups that have derived from the original organization? How do these differ from the original organization?

The Organizational Ecosystem

Further, in terms of the environmental context for the group, it may help to consider some additional questions.

- Are there natural limits to this organization in the environment?
- Who are the competitors to this organization?
- What can the government offer to potential followers of the group that the group cannot offer, and vice versa? In the competition for the hearts and minds (and computers) of the general populace, what is being offered to the mainstream?

As of early 2012, there are concerns that this group will evolve capabilities within a few years to potentially attack the U.S. electronic grid and potentially cause harm to individual lives and critical physical infrastructures. There are speculations on how the leadership may change in terms of "character in power" or character in any organizational circumstance, depending on how the law enforcement and cyber environment changes. Other concerns are that they will potentially bring in mercenaries with even greater capabilities than self-trained hackers. Prior hacks have been exploited by foreign intelligence agencies. Right now, there is insufficient information to speculate about the ranges of possibilities. However, it is also irresponsible to take away any possibilities from the range of conceptual possibilities on the one hand or to cast aspersions on this organization, on the other.

While human and group motives are constantly evolving, private motives are often more complex and enduring than even publicly acknowledged ones. There may be hidden other motives that were not even considered in this work.

As it is, truth has to be conceptualized as a shimmer—with a wide range of potential realities. The action potential of a hacktivist group will change depending on a variety of factors—the ideologies, the leaderships, the capabilities of the group, and those of competitor groups and their targets. (If Wikileaks is any indication, the troubles of its leader have led to spinoff groups—like OpenLeaks—and a diminishment of the original organization, which had an unstable funding structure [Domscheit-Berg, 2011].) An organization informs its own history by interpreting that history, but it is also defined and informed by that history. Those external to the group—say, law enforcement, mainstream media, academics, and others—also have a voice in defining that history. If a hacker is defined by his or her hack, and if it is true that people are constantly striving for power (in whatever ways they may best express their power, according to various motivation theories), then one may assume that there is continuous upward pressure to top prior efforts—in order to show the organization's resolution and to encourage more membership and participation. Activists have been using the Internet in more creative ways in terms of "intercreative texts, intercreative tactics, intercreative strategies, intercreative networks" (Meikle, 2010, p. 364).

As a meme, the Anonymous stance about the need for the freedom of information may be a universalist one, but the concepts may not be widely salient. As an archetype, Anonymous may fit the role of the trickster character, according to anthropologist Gabriella Coleman, who has been studying the group (Sengupta, 2012). Without a charismatic leader or an emotional appeal or even a "homeland" message, the ideology of Anonymous may not contain the seeds for wider participation. While this approach will go "viral" any time soon, it is clear that the fight with hackers and hacktivists is already a global fight for law enforcement. These are all speculations. Still, there is no denying that Anonymous is a critical player in the definition of the future of the Internet and the respective roles of information and its dispersion in the world. Most information systems are "secure enough (but insecure)" (Sandhu, 2012) because absolute security may be an impossibility. In the face of the Advanced Persistent Threat (APT) of hacktivism to establishment systems, there is a value in setting this baseline understanding founded on the extant available information up to the present.

ACKNOWLEDGMENT

Thanks to Jan Travers of IGI-Global, and Christina M. Akrivopoulou and Nick Garipidis (editors), for taking a chance on this chapter. If anything, this chapter addresses the limits of the publicly knowable given the current time about an elusive group which is striving to make an impact. Thanks also to Dr. Annelise "Thu" Nguyen, Eric Dover, and R. Max for their encouragement. These are all "go for broke" kinds of people who know when to take smart risks. I hope this is one. Thanks also to Dr. Laurie Johnson, in whose course a sidebar for this chapter was initially developed and evolved. I have long wanted to pursue this question of Anonymous' ideology. This is for R. Max.

REFERENCES

Adkins, B. N. (2001). *The spectrum of cyber conflict from hacking to information warfare: What is law enforcement's role? A research report*. Unpublished.

Anderson, N. (2011, February 10). How one man tracked down Anonymous—And paid a heavy price. *Wired.* Retrieved from http://arstechnica.com/tech-policy/news/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price.ars

OhInternet. (2012). *Anonymous*. Retrieved from http://ohinternet.com/Anonymous

Anonymous. (2012). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Anonymous_%28group%29

Argyris, C. (1993). *Knowledge for action: A guide to overcoming barriers to organizational change*. San Francisco, CA: Jossey-Bass.

Ball, T., & Dagger, R. (2011). *Political ideologies and the democratic ideal* (8th ed.). Boston, MA: Longman.

Bénabou, R., & Tirole, J. (2011). Identity, morals, and taboos: Beliefs as assets. *The Quarterly Journal of Economics*, *126*, 805–855. doi:10.1093/qje/qjr002

Bernstein, M. S., Monroy-Hernández, A., Harry, D., André, P., Panovich, K., & Vargas, G. (2011). 4chan and /b/: An analysis of anonymity and ephemerality in a large online community. *Association for the Advancement of Artificial Intelligence*. Retrieved from http://projects.csail.mit.edu/chanthropology/4chan.pdf

Branscombe, N. R., Wann, D. L., Noel, J. G., & Coleman, J. (1995). In-group or out-group extremity: Importance of the threatened social identity. *Personality and Social Psychology Bulletin*, *19*(4), 381–388. doi:10.1177/0146167293194003

Brey, P. (2007e). Ethical aspects of information security and privacy. In Petković, M., & Jonker, W. (Eds.), *Security, Privacy, and Trust in Modern Data Management* (pp. 21–36). Berlin, Germany: Springer. doi:10.1007/978-3-540-69861-6_3

Brito, J. (2012, March 12). Gabriella Coleman on Anonymous and LulzSec. *Surprisingly Free*. Retrieved from http://surprisinglyfree.com/2012/03/13/gabriella-coleman/

Burrough, B. (2000, June). Invisible enemies. *Vanity Fair.* Retrieved from http://www.vanityfair.com/culture/features/2000/06/web-hackers-200006

Charney, S. (2010). *Collective defense: Applying public health models to the internet*. Retrieved from http://download.microsoft.com/download/7/F/B/7FB2F266-7914-4174-BBEF-2F5687882A93/Collective%20Defense%20-%20Applying%20Global%20Health%20Models%20to%20the%20Internet.pdf

Coleman, G. (2011, May 9). Anonymous—From the Lulz to collective action. *The New Significance.* Retrieved January 23, 2012, from http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/

Coleman, G. (2011). Hacker politics and publics. *Public Culture*, *23*(3), 511–516. doi:10.1215/08992363-1336390

Cronin, A. K. (2003). Behind the curve: Globalization and international terrorism. *International Security, 27*(3), 30 – 58. Retrieved January 18, 2012, from http://www.jstor.org/stable/3092113

Cronin, A. K. (2009). *How terrorism ends: Understand the decline and demise of terrorist campaigns*. Princeton, NJ: Princeton University Press.

Dafermos, G., & Söderberg, J. (2009). The hacker movement as a continuation of labour struggle. *Capital and Class*, *97*, 53–73. doi:10.1177/030981680909700104

Denning, D. (1999). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. *Information Axioms*. Retrieved from http://www.nautilus.org/gps/info-policy/workshop/papers/denning.html

Denning, D. E. (2003). Information technology and security. In Brown, M. E. (Ed.), *Grave New World: Security Challenges in the 21st Century*. Washington, DC: Georgetown University Press.

Domscheit-Berg, D. (2011). *Inside Wikileaks: My time with Julian Assange at the world's most dangerous website*. New York, NY: Random House.

Ferran, L. (2012, April 5). *Anonymous lashes out at Chinese government*. ABCNews.

Fidler, D. P. (2008). A theory of open-source anarchy. *Indiana Journal of Global Legal Studies, 15*(1), 259 – 284. Retrieved from http://www.jstor.org/stable/10.2979/GLS.2008.15.1.259.

Gleick, J. (2011). *The information: A history, a theory, a flood*. New York, NY: Random House. doi:10.1109/TIT.2011.2162990

Glenny, M. (2011). *DarkMarket: Cyberthieves, cybercops and you*. New York, NY: Random House.

Hacker Ethic. (2012). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Hacker_ethic

Henderson, N. (2011, June 3). *Hackers attack Sony Pictures with single SQL injection*. Retrieved from http://www.thewhir.com/web-hosting-news/hackers-attack-sony-pictures-with-single-sql-injection

Isikoff, M. (2012, February 25). Anonymous attacks 'alarming,' says top security adviser. *MSNBC*. Retrieved from http://www.technolog.msnbc.msn.com/technology/technolog/anonymous-attacks-alarming-says-top-security-adviser-196804

Isikoff, M. (2011, March 8). Hacker group vows 'cyberwar' on US government, business: Actions to retaliate for treatment of Wikileaks, Manning, spokesman for Anonymous says. *MSNBC*. Retrieved from http://www.msnbc.msn.com/id/41972190/ns#.T3i2odmt_fc

Jackson, G. M. (2012). *Predicting malicious behavior: Tools and techniques for ensuring global security*. Indianapolis, IN: John Wiley & Sons.

Jetten, J., Branscombe, N. R., Spears, R., & McKimmie, B. M. (2003). Predicting the paths of peripherals: The interaction of identification and future possibilities. *Personality and Social Psychology Bulletin*, *29*, 130–140. doi:10.1177/0146167202238378

Johns, A. (2009). Piracy as a business force. *Culture Machine*, *10*, 44–63.

Kizza, J. M. (2009). Cybercrimes and hackers. In *A Guide to Computer Network Security, Computer Communications and Networks* (pp. 107–132). London, UK: Springer-Verlag. doi:10.1007/978-1-84800-917-2_5

Kleen, L. J. (2001). *Malicious hackers: A framework for analysis and case study*. (Thesis). Wright-Patterson, OH: Air Force Institute of Technology, Air University.

Krapp, P. (2005). Terror and play, or what was hactivism. In *Grey Room, Inc*., (pp. 70-93). Cambridge, MA: The MIT Press. Retrieved from http://www.jstor.org/stable/20442704

Kreimer, S. F. (2001). Technologies of protest: Insurgent social movements and the first amendment in the era of the internet. *University of Pennsylvania Law Review*, *150*(1), 119–171. doi:10.2307/3312914

Lee, J. (2012, March 21). Hacker group LulzSec says it will resume attacks on April fool's day. *Web Host Industry Review*. Retrieved from http://www.thewhir.com/hacker-group-lulzsec-says-it-will-resume-attacks-on-april-fools-day

Levesque, M. (2006). Hacktivism: The how and why of activism for the digital age. In Weiss, J. (Eds.), *The International Handbook of Virtual Learning Environments* (pp. 1203–1214). Berlin, Germany: Springer. doi:10.1007/978-1-4020-3803-7_49

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *Computers & Society*, *30*(2), 14–19. doi:10.1145/572230.572232

Mansfield-Devine, S. (2011). Hacktivism: Assessing the damage. *Network Security*, *8*, 5–13. doi:10.1016/S1353-4858(11)70084-8

Mansfield-Devine, S. (2011). Anonymous: Serious threat or mere annoyance. *Network Security*, *1*, 4–10. doi:10.1016/S1353-4858(11)70004-6

Meikle, G. (2010). Intercreativity: Mapping online activism. In Hunsinger, J. (Eds.), *International Handbook of Internet Research*. London, UK: Springer.

Milone, M. (2003). Hacktivism: Securing the national infrastructure. *Knowledge, Technology & Policy*, *16*(1), 75–103. doi:10.1007/s12130-003-1017-5

Needleman, R. (2011, July 1). Reporters' roundtable: Anonymous, LulzSec, and hacktivism. *CNET*. Retrieved from http://www.cnet.com/8301-30976_1-20076235-10348864/reporters-roundtable-anonymous-lulzsec-and-hacktivism/

Newcomb, A. (2011, September 5). When Anonymous comes after you. *ABCNews*. Retrieved from http://abcnews.go.com/Blotter/anonymous-focus-individual-targets-alleged-high-profile-hacks/story?id=14446772

Norton, Q. (2012, January 20). Anonymous tricks bystanders into attacking justice department. *Wired Magazine*. Retrieved from http://www.wired.com/threatlevel/2012/01/anons-rickroll-botnet/

Nye, J. S. Jr. (2010). *Cyber power*. Boston, MA: Harvard Kennedy School: Belfer Center for Science and International Affairs.

Nye, J. S., Jr. (2011, Winter). Nuclear lessons for cyber security. *Strategic Studies Quarterly,* 18 – 38.

Ohhashi, K. (2011, July 26). Anonymous and me. *COSMOS*. Retrieved January 23, 2012, from http://cosmos.ucdavis.edu/archives/2011/cluster4/Ohhashi_Ken.pdf

Olson, P. (2012). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. New York, NY: Little, Brown and Company.

Orton, J. D., & Weick, K. E. (1990). Loosely coupled systems: A reconceptualization. *Academy of Management Review*, *15*(2), 203–223.

Perlroth, N., & Markoff, J. (2012, February 27). Failed Vatican hack attack sheds light on Anonymous' methods. *The New York Times.*

Pras, A., Sperotto, A., Moura, G. C. M., Drago, I., Barbosa, R., & Sadre, R. Hofstede, R. (2010). *Attacks by 'Anonymous' WikiLeaks proponents not anonymous*. CTIT Technical Report 10.41, (pp. 1-10). CTIT.

Preuβ, J., Furnell, S. M., & Papadaki, M. (2007). Considering the potential of criminal profiling to combat hacking. *Journal of Computational Virology, 3*, 135 – 141.

Ramsdell, W. (2011). Hackers and the digital sublime. *Diskpunk.com*. Retrieved from http://diskpunk.com/closet/Hackers%20and%20the%20Digital%20Sublime.pdf

Rashid, F. Y. (2012, March 22). Hacktivists stole more data than criminals in 2011. *PC Magazine.* Retrieved from http://securitywatch.pcmag.com/hacking/295701-hacktivists-stole-more-data-than-criminals-in-2011

Ribeiro, J. (2012). Anonymous claims to have released source code of Symantec's pcAnywhere. *InfoWorldHome*. Retrieved from http://www.infoworld.com/d/security/anonymous-claims-have-released-source-code-of-symantecs-pcanywhere-185839

Rice, D. (2008). *Geekonomics: The real cost of insecure software*. New York, NY: Addison-Wesley, Pearson Education.

Rosenzweig, P. (2011, May 31). *Lessons of WikiLeaks: The US needs a counterinsurgency strategy for cyberspace*. Washington, DC: The Heritage Foundation.

Schwartz, M. (2011, December 14). Kiss off: Anonymous hacker took on Gene Simmons, feds say. *Information Week.*

Schwerha, J. J. IV. (2004). Cybercrime: Legal standards governing the collection of digital evidence. *Information Systems Frontiers*, *6*(2), 133–151. doi:10.1023/B:ISFI.0000025782.13582.87

Sengupta, S. (2012a, March 31). After threats, no signs of attack by hackers. *The New York Times*. Retrieved from http://www.nytimes.com/2012/04/01/technology/no-signs-of-attack-on-internet.html

Sengupta, S. (2012b, March 17). The soul of the new hacktivist. *The New York Times.* Retrieved from http://www.nytimes.com/2012/03/18/sunday-review/the-soul-of-the-new-hacktivist.html?_r=1&scp=3&sq=lulzsec&st=cse

Sengupta, S. (2012c, March 30). Warned of an attack on the internet, and getting ready. *The New York Times.* Retrieved from http://www.nytimes.com/2012/03/31/technology/with-advance-warning-bracing-for-attack-on-internet-by-anonymous.html

Shachtman, N. (2011). *Pirates of the ISPs: Tactics for turning online crooks into international pariahs*. Washington, DC: Brookings.

Tennant, C. (2011, October). The anti-establishment. *Vanity Fair.*

Timeline of Events Involving Anonymous. (2012). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Timeline_of_events_involving_Anonymous

MSNBC. (2012, April 8). *UK government website disrupted by hacker attack*. Retrieved from http://www.msnbc.msn.com/id/43913115#.T4IyfNkosSE

Underwood, P., & Welser, H. T. (2011). *The internet is here: Emergent coordination and innovation of protest forms in digital culture*. Seattle, WA: ACM. doi:10.1145/1940761.1940803

Wang, Z., Walther, J. B., & Hancock, J. T. (2009). Social identification and interpersonal communication in computer-mediated communication: What you do versus who you are in virtual groups. *Human Communication Research*, *35*, 59–85. doi:10.1111/j.1468-2958.2008.01338.x

Wark, M. (2004). *A hacker manifesto*. Retrieved from http://subsol.c3.hu/subsol_2/contributors0/warktext.html

KEY TERMS AND DEFINITIONS

0-Day Exploit: A vulnerability in a technology system that is yet unknown by the software makers and system administrators (often very difficult to identify).

4chan: An Internet message/image (bulletin) board.

/b/: An electronic bulletin board.

Action Potential: After cell activation by a stimulus, the following change in an electrical impulse along a plasma membrane (of a muscle or nerve) in the transmission of nerve signals.

Air Gap: A physical disconnection between a computer network and the Internet, initially thought to be capable of protecting an information system against compromise.

Anarchy: The lack of a government.

Ankle Biter: A neophyte, an amateur.

Anomic: Alienated, without a sense of direction or meaning.

Anonymous: Not unidentified by name; without distinguishing features; impersonal; unknown.

Backdoor: A way to illicitly access network systems by bypassing normal authentication.

Blackhat Hacker: A hacker who hacks for malicious reasons, usually to cause damage.

Civil Disobedience: Purposeful non-compliance with select laws as a non-violent form of political expression or protest.

Costly Signal: An indicator of an organization's type by a particular action that his risky to the organization, often to prove its resolve to a cause and its capabilities (an antonym to a "costly signal" is a "cheap talk" signal, which is cost-free to provide).

Creed: A formal statement of beliefs.

Cybotage: A form of cyber terrorism which involves the disruption and destruction of information infrastructures, often for political aims.

Defacement: The purposeful harming of the appearance of a website, often through digital graffiti.

Denial of Service (DOS) Attack: An attack which involves the uses of many "drone" computers to request service from a targeted website to overwhelm their servers to deny the servers' provision of services to potential users.

Distributed Denial of Service (DDOS) Attack: An attack that involves the takeover of many "drone" computers (multiple attack systems) to request service from a targeted website with the purpose of taking the site down (leading to service outages from the target website).

Domain Name System: The underlying system that links names of websites to their Internet Protocol (IP) addresses, enabling the location of the site.

Dox: A verb that means to "document" or identify the real people behind handles.

Drone: A machine that is remote-controlled; an unthinking and unpiloted computer.

Exploit: A compromise of a computing machine.

Forensics: The study of evidence on computers and digital storage media.

Gray Hat Hacker: A hacker who hacks computers, software, and networks for both benevolent and malevolent reasons.

Hacker: A skilled person who breaks into computing systems and computers—for any range of purposes.

Hacktivism (Hacker + Activism): The uses of computers and computer networks to make political statements; a form of civil disobedience using computers and computer networks; a portmanteau of hacker and activism; electronic civil disobedience.

Honeypot: A virtual trap designed to be attacked by hackers in order to learn about hacker strategies, tools, identities, and behaviors (a "honey net" is a simulated network for the same purposes as a "honey pot").

Hybrid Attack: A hacker attack that uses multiple tactics to compromise systems.

Ideology: A set of ideas that may define goals, values, and actions of a (often political) group.

Image Board (also Imageboard): A channel, an internet form that focuses on the posting of images.

Internet Protocol Address (IP): A unique identifier to a particular computer connected to the Internet.

Internet Relay Chat (IRC): Real-time text messaging application.

Key Logger: A malicious type of software that may be used to "log" or record all the keystrokes of an individual using a computer, in order to access their private accounts and other information.

Kiddie Hack: A low-level hack using publicly available tools (a derisive label indicating amateurism).

Libertarianism: A political philosophy that promotes as little government as possible to enable individual free will and decision-making.

Lulz: The plural form of "lol" or "laugh out loud".

Manifesto: A public declaration of political principles and values.

Meme: A unit of cultural transmission, which may be ideas or practices or other forms.

Mercenary: An individual who sells his or her skills for money.

Microblogging: The Web logging of short messages usually limited to 140 characters, distributed in real time to the various "followers" of a particular individual or group.

Mirroring: The preservation and copying of a Web site in its original form.

Neologism: A newly created word.

Non-Propertarian Libertarianism: The philosophy that true human liberty requires the absence of any authority; this belief system rejects any authority of private property to the detriment of others.

Pen (Penetration) Attack: Successful unauthorized access to a protected system resource, usually information.

Personally Identifiable Information (PII): Information that serves as a unique identifier of an individual and can lead to a non-repudiatable naming of the person.

Phishing: An illegal elicitation of private information by taking on a false identity through electronic communications.

Propaganda: Information designed to influence people in regards to a political issue; persuasive communication to affect attitudes, ideas, and behaviors.

Pseudonymity: The maintenance of long-term anonymity; the state of not being identifiable for a long period of time.

Random Walk: A probabilistic trajectory based on observations and mathematical formulas but which offer a range of indeterminacy; an expression of a stochastic process.

Script Kiddies: A derogatory term referring to low-level hackers who are using simplistic methods.

Social Network: The connection of individuals through socio-technical spaces online; a branch of network science that focuses on human power relationships and the exchanges of resources and information.

Spear Phishing: A targeted (a known individual or organization) fraudulent elicitation of private information through electronic communications.

SQL Injection Attack (SQLIA): The inputting of SQL statements in a Web form to extract the database contents or to send other commands to the server.

Tag Cloud: A text analysis tool that enables the display of words in a document or a website that calibrates the number of appearances of that word with the size of that word in a "tag cloud"; a type of visual informational-graphic.

Unique Identifier: A number or name that uniquely categorizes a particular digital or other object.

Web Log ("Blog" as a Portmanteau of "Web Log"): A Web journal, usually focused around a particular individual or personality, or topic.

Whitehat Hacker: A computer expert who hacks into computer systems in order to find weaknesses so that they may be addressed without causing damage to the software maker or software users.

APPENDIX 1

Extrapolating the Ideologies of the Anonymous Hacker Collective's Spin-Offs: AntiSec and LulzSec

For virtual organizations that do not have a formal structure (except for the inner group of the leadership), very little research exists about how spinoffs occur. In this scenario, though, the Anonymous hacker collective has spun off two specialized organizations and movements in 2009 and 2011 respectively, some years after the organization initially became active with hacktivism in 2006: AntiSec and LulzSec.

Anti Security (AntiSec) 2009

A core element of Anonymous is reflected in the spin-off AntiSec movement or group. Initially, the Anti-Sec Movement (started in 1999) was about the eradication of full disclosure of computer system compromises and zero-day software exploits (as-yet unknown exploits) by cyber-security companies, which the hackers saw as an effort to instill fear and therefore raise profits for these particular companies. The original Anti-Sec movement took over the ImageShack site in order to post their manifesto, which decried the mirroring (copying and hosting) of hacked sites, as a way to raise money for profit-seeking corporations through the sales of firewalls, anti-virus software, and security auditing services. The neo-Anti Security Movement ("antisec" or "anti-sec"), as expressed through this Anonymous spin-off, is apparently about combating security efforts on the Internet as elements of totalitarian governments. Their media releases discussed fighting the high-level corruption of "profiteering gluttons" in terms of government and corporations. Foremost, they focused on what they call "the government and whitehat security terrorists across the world" (Diaz, 2011). Their own AntiSec image shows a monocle personae wearing a very black top hat.

They launched Project Mayhem ("pr0j3kt m4yh3m" in leetspeak) in 2009 as an attack against security communities (Astalavista and milwOrm and ImageShack). ("leetspeak" refers to "elite"—or a special cipher used online. "leet," expressed as '1337,' is an adjective to describe prowess or accomplishment, particularly in computer hacking. leetspeak appears in various media releases by the group, which asserts that it will 'pwn' or own or dominate various governments, corporations, or individuals).

The AntiSec wing of Anonymous undercut anonymous reporting of crime by compromising a law enforcement website in an operation termed "Shooting Sheriffs Saturday Release" which compromised 70 U.S. law enforcement agencies' sites and information (Mills, 2011).

A compromise of software giant Symantec involved the capture of its pcAnywhere source code. The hacker requested $50K in extortion to not release the code and then released it when that amount was not paid (Storm, 2012). This push for funding, again, is another recent innovation off of Anonymous activities—which earlier decried any entrepreneurial or monetary-gain aspect. Was this extortion attempt the work of a renegade or a change in organizational tactics?

The OpAntiSec banner has enabled a range of highly focused campaigns against particular organizations with actual and symbolic value in the neo-AntiSec agenda. While the ambitions are broad, and there have been some severe and expensive compromises ranging in the hundreds of millions of dollars of damage, the sophistication of the various hacks are not technologically that difficult.

With the 2011 passage of the Anti-Counterfeiting Trade Agreement (ACTA) treaty and proposed Protect IP Act (PIPA), the AntiSec hackers promised to "bring a fu**ing mega-uber-awesome war that rain torrential hellfire down on all enemies of free speech, privacy and Internet freedom".

Lulz Security (LulzSec) 2011 -

While Anonymous members use terms like “guerrilla cyberwarfare” to describe their work, the origin of LulzSec (“LulzSecurity” with an earlier incarnation as Internet Feds—under Anonymous) might seem to be a return to the roots of Lulzy hacking or the joy at creating havoc or disruption. This group has released statements such as: “You find it funny to watch havoc unfold, and we find it funny to cause it” (Hoffman, 2011, p. 20). Their motto is the following: “Laughing at your security since 2011!” and their bio on Twitter read in part “the world’s leaders in high-quality entertainment at your expense.” Their microblogging Tweets are full of “Wink, wink, double wink!” Their website, which was created in June 2011, plays the theme-song for *Love Boat.* Their ASCII-art banner of the LulzBoat (based on a pirate ship theme) shows that the organization is all about the “laugh out loud”s.

The work of this splinter group differed from mainline Anonymous hacktivism in the sense that they made the dumping of private information into the public realm a centerpiece of its work. This group (veterans of the infamous HBGary hack) fielded a small team of trusted hackers. They used an automated tool to scan the Internet for SQL-injection network vulnerabilities, and there was another open-source tool for downloading databases for easier analysis. This off-shoot focused on attacking .mil and .gov sites. Various hackers would send in floods of hacked network vulnerabilities, in pursuit of lulz but also acts of vengeance. Not all attacks or data releases were instigated from the central group of core hackers.

However, the targets of the attacks beginning with a two-month spree in May –June 2011 were high-impact and high-attention ones. The earliest known hack attributed to the group began on May 5th, 2011, against Fox Broadcasting Company. The group released the X Factor contestants database with 73,000 applicants’ personal information. Shortly thereafter, the Fox.com sales database was released. In May, 2011, the U.S.-based Public Broadcasting Service (PBS) was hacked by LulzSec in retaliation for its Wikileaks documentary. A faked story about late rapper `Tupac Shakur’s quiet living in a secret location was shared on the hacked site. This escapade was broadly trumpeted through social networking channels.

Another attack occurred in early June 2011 and involved the accessing of a U.S. Senate server and an attack on Bethesda Softworks, with the release of gamers’ identities and passwords (with a high risk of compromise for repeat passwords used on multiple accounts).

An attack on an FBI-linked network of cyber-technology specialists supporting national security called Infragard was attacked, and 180 passwords from the members were revealed. The organization focused on trying to interfere with FBI work and even made a hash tag called “#fuckfbifriday” to organize their Tweets. This new direction in hacking law enforcement drove away some of the hacker stalwarts who’d participated in earlier attacks for “lulz” and less for politics or challenging government. They compromised Pron.com (a porn site) computers and revealed some 26,000 log-ins and passwords, many email addresses with .mil and .gov extensions. In June, LulzSec hacked the UK’s Serious Organized Crime Agency (SOCA) in retaliation for the arrests of some hackers.

A member of both Anonymous and LulzSec admitted in court in participating in an extensive hack of Sony Pictures Entertainment, which was said to have suffered $171 million in losses (Henderson, 2011) and others suggesting that the company would have to spend over a billion to shore up its systems and to pay out costs from lawsuits. The group broke into Nintendo in June 2011, but they limited the harm they caused because of a professed “fondness for the game console maker” (Henderson, 2011).

Law enforcement is a particular target of choice. In late June 2011, the group hacked and released information from the Cyberterrorism Defense Initiative’s Security and Network Training Initiative and National Education Laboratory (Sentinel program). The following image shows ASCII-text art released with the attacks on Arizona law enforcement agents in response to what the members saw as anti-immigration laws and their enforcement. This attack in June 2011 leaked personal details of those in law enforcement. It came with a statement against "racial profiling anti-immigrant police state." According to P. Olson, this trove of emails and files came from an activist who was not a core leader in LulzSec but a participant (2012, pp. 338 – 339). The release of these files caused consternation among the leadership, who did not want to cause increased risks to the police officers.

A DDOS attack on the C.I.A. for the laughs was the apparent reason for contact by Wikileaks founder Julian Assange, who requested that the group hack the Icelandic government's sites as retaliation for their treatment of a journalist who supported Wikileaks (Olson, 2012, pp. 324 – 329). (Assange verified his identity by sending a link to a near-live video of himself sitting at the computer with the text of their IRC chat in the window on his laptop).

For all the publicity, this organization was losing its street credibility. The exploits into various networks—for "Fox, Sony, NATO, Senate.gov" were given to LulzSec by other hackers loosely affiliated with the group. LulzSec's inner circle could claim only Infragard and PBS as their direct hacking victims (Olson, 2012, p. 343). Intermittent arrests of various members further dampened membership rolls, and the leadership themselves was starting to feel the pressure.

After two intense months of hacking and a last data dump of their electronic heists on June 25, 2011, the group claimed retirement at the end of June. On June 26, 2011, the group commemorated "50 days of lulz" and claimed that they had only intended to be active for 50 days from the beginning. In other accounts, this came about as a response to the arrests of some of the core leadership in multiple countries. According to an organizational press release, the group claimed only 6 members, which law enforcement charging documents seem to corroborate. Their new media savvy resulted in the group having more than 283,000 followers on its Twitter feed when it first retired.

A group re-emerged as LulzSec Reborn on April 1, 2012 (April Fool's Day), after many of its first-generation core members were arrested by the FBI and other law enforcement agencies around the world—when it was revealed that the group's titular head Sabu (Hector Xavier Monsegur) had been turned by the FBI and had helped identify the other group members (Sengupta, 2012); law enforcement intercepted hacker "finds" of various network vulnerabilities in order to warn corporations and organizations, so the vulnerabilities could be patched. (It was surmised in the aftermath of the arrests that Monsegur was used by the FBI to attract some of the world's best hackers for arrest or recruitment by intelligence agencies or law enforcement.) These hackers face serious risks in their respective countries of citizenship and operations. In the U.S., a conspiracy charge may result in up to five years in prison, if the individual is convicted. Intentional damage to a protected computer may result in a maximum sentence of 10 years in prison. Each charge comes with a potential $250,000 fine. Hacker arrests related to LulzSec occurred in the UK, Ireland, New York, and Chicago. Some cyber security experts have said that this new Anonymous is likely wholly new as the first group was rolled up in an FBI sting (Rubenking, 2012).

Hacker groups do not function in a competition-free environment. They are not only combating law enforcement with their outsized legal powers of information access, infiltration, subterfuge, access, and serious technology skills and tools. Hacker groups compete with other hackers and groups, who want to claim dominance, skills, and political righteousness. Loyal insiders may turn into outsiders and "enemies" based on a small disagreement. LulzSec members have been "doxed" and outed by rival hacker groups, such as TeaMp0isoN, KillerCube, BlaCkCat, Team Web Ninjas, The Jester (using th3j35t3r as his handle), Oneiroi, and m_nerva.

The LulzBoat "Operation Anti-Security" manifesto reads like a call-to-action:

> *We encourage any vessel, large or small, to open fire on any government or agency that crosses their path. We fully endorse the flaunting of the word "AntiSec" on any government website defacement or physical graffiti art. ... To increase efforts, we are now teaming up with the Anonymous collective and all affiliated battleships.*
>
> *Top priority is to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments. If they try to censor our progress, we will obliterate the censor with cannonfire anointed with lizard blood.*

This "reborn" group broke into a dating site (MilitarySingles.com) for military personnel and released some 160,000 account details from their database (Constantin, 2012). Rupert Murdoch's *The Sun* and *The Times* were hacked in July 2012. So too were the following: the government of Zimbabwe; the municipality of Mosman; and the government of Tunisia. In terms of corporate hacks, AT&T, Sony, Viacom, Disney, EMI, NBC Universal, and a Fox News Twitter account were all hacked. There were cyber-attacks in Austria and Italy. Of special concern to law enforcement were the attacks on NATO (with a gigabyte of private data released) and the International Monetary Fund (IMF) because of the potential impact on national security and international economies (Hoffman, 2011). The U.S. Director of National Intelligence suggested that LulzSec's incursions into NASDAQ and the International Monetary Fund result in significant risks to national security infrastructures (Clapper, 2012, p. 7). Indeed, such hactivist organizations have engaged in calling for attacks on the U.S. "national infrastructure" and such rhetoric (Lee, 2012).

Monsanto was hacked in July 2012: "The group claimed they performed the attack to protest the company's lawsuits against farmers who manufacture organic milk in an effort to stop them from stating on the label that their milk does not contain artificial Bovine Growth Hormones. Monsanto confirmed the attack but claimed that only about ten percent of the information published came from current or former employees of the company. They said that the other ninety percent were email addresses and names of media contacts and employees of other agricultural companies," according to the "Operation AntiSec" Wikipedia entry.

In an escalatory innovation, the group used compromised financial information to make donations to various charitable causes with the credit card numbers of police officers' compromised accounts.

This organization dumps the raw data en masse on data sharing sites (and piracy sites), but they do little in the way of analysis—only highlighting a few particular points of interest in Tweets or on their websites. At this point, it is unclear what the secondary or tertiary exploitations of this data may be. Some press reports have mentioned financial identities compromised, and others have mentioned exploitation by foreign intelligence services ("AntiSec hackers…," Jan. 5, 2012).

The phenomenon of LulzSec is intriguing in two fundamental ways. One is the setup of Bitcoin to collect donations to fund its activities along. Anonymous did not have a clear publicly identifiable income stream, and it seemed like an out-of-pocket sort of endeavor for those who would participate under that group's banner. Second, LulzSec itself has splintered into other groups—or spawned or inspired others. LulzRaft conducted hacks in Canada. LulzSec Brazil, a regional organization, hacked Brazilian government sites and the large energy company Petrobras. Raising resources may strengthen the organization even as if opens up potential further legal (criminal) liabilities for both the organization and its funders. The splintering off of its message and its hacking practices suggests that others continue to see hacktivism as a way of righting social wrongs. As has been observed, many of those hackers arrested in LulzSec and other Anonymous-related groups have been dispossessed young males who turned to breaking into establishment sites to find meaning, voice, and entertainment.

CONCLUSION

The "propaganda of the deed" of various hacktivist spin-offs from the Anonymous hacker collective reveals AntiSec and LulzSec as pursuing some aligned goals of disrupting the Establishment *status quo* of Internet security, intellectual property protections, and information privacy protections online. Their attacks on governments, corporations, law enforcement, and security firms show a clear disruption strategy and combined hacker tactics. The two hacker manifestos and the various public statements by these spinoff organizations indicate the thinking behind the various actions of the groups. While the targeting of Anonymous (the originating organization) covers a much wider range of potential interests and more global territory (in cyberspace), the spinoff organizations tend to have clearer ideologies and activating messages. One core value in hacking is that the hacker is the hack, and as the hacker evolves in virtuosity, he (or she—but much rarer) will express that capability in more sophisticated ways to send a message to the world. An ideology provides an animating *raison d'etre* for various groups, but it also evolves as the group's leadership and membership evolves. In that light, it is critical to monitor both the ideologies and the actions to understand the direction and capabilities of the hacktivist groups.

An ideology provides an animating *raison d'etre* for various groups, but it also evolves as the group's leadership and membership evolves. In that light, it is critical to monitor both the ideologies and the actions to understand the direction and capabilities of the hacktivist groups. Closer monitoring of these spin-off groups, interviews with their arrested leaders, conducting text analyses of conversations between the followers, and even more formalizing querying of the group's leaders and followers may reveal deeper insights about the groups' ideologies. While the original Anonymous purposefully claimed to have no ideology, their spin-off organizations are somewhat less doctrinaire on this point, which has enabled this early look at their nascent animating ideology.

It will be important also to see if these ideologies, which inspire up to tens of thousands to take part in DDoS and DoS attacks by turning over their computers as drones offer some constraints on the actions of the members of the groups. In the case of Anonymous, the distributed and virtual nature of the collective has meant that various cyber attacks may be seen as not only contravening their own ideology (such as by shutting down the free speech of others, such as reporters in mainstream media) but also resulting in factions that take opposite sides of an issue and who hack and counter-hack each other. The cyber skirmishes among various factions of the hacktivist community are well documented, with the tools of social engineering and hacking brought to bear against each other (Olson, 2012). Meanwhile, members of the hacker groups are being "doxed" by law enforcement and brought into various legal systems for their day in court.

It may be that law enforcement may be the only ones who are watching these spinoff groups closely, and it's not likely that any will be revealing methods or insights into the public realm for some time yet (while investigations are on-going). Academics are limited to what is available legally and publicly and within the capabilities of current technologies. It may be that tools written to scrape the so-called Dark Web may surface other insights about AntiSec and LulzSec.

REFERENCES

OhInternet. (2012). *Anonymous*. Retrieved from http://ohinternet.com/Anonymous

United Press International. (2012, January 5). *AntiSec hackers bare data on Kissinger, Quayle*. Retrieved from http://www.upi.com/Top_News/US/2012/01/05/AntiSec-hackers-bare-data-on-Kissinger-Quayle/UPI-99971325745702/

Clapper, J. R. (2012, February 2). *Unclassified statement on the worldwide threat assessment of the US intelligence community for the House Permanent Select Committee on Intelligence*. Washington, DC: US Government.

Coleman, G. (2011, May 9). Anonymous—From the Lulz to collective action. *The New Significance.* Retrieved January 23, 2012, from http://www.thenewsignificance.com/2011/05/09/gabriella-coleman-anonymous-from-the-lulz-to-collective-action/

Constantin, L. (2012, March 27). Reborn LulzSec claims hack of dating site for military personnel. *PC World.* Retrieved from http://www.pcworld.com/businesscenter/article/252647/reborn_lulzsec_claims_hack_of_dating_site_for_military_personnel.html

Diaz, J. (2011, June 20). Lulzsec and Anonymous declare open war against all governments and fat cats. *Gizmodo*. Retrieved from http://gizmodo.com/5813560/lulzsec-and-anonymous-declare-open-war-against-all-governments-and-fat-cats

Glenny, M. (2011). *DarkMarket: Cyberthieves, cybercops and you*. New York, NY: Random House.

Henderson, N. (2011, June 3). Hackers attack Sony Pictures with single SQL injection. *Web Hosting Industry News*. Retrieved from http://www.thewhir.com/web-hosting-news/hackers-attack-sony-pictures-with-single-sql-injection

Henderson, N. (2011, June 6). Hacker group LulzSec attacks Nintendo, FBI affiliate security firm InfraGard. *Web Hosting Industry News*. Retrieved from http://www.thewhir.com/web-hosting-news/hacker-group-lulzsec-attacks-nintendo-fbi-affiliate-security-firm-infragard

Hoffman, L. (2011). Risky business. *Communications of the ACM*, *54*(11), 20–22. doi:10.1145/2018396.2018404

Kleen, L. J. (2001). *Malicious hackers: A framework for analysis and case study*. (Thesis). Wright-Patterson, OH: Air Force Institute of Technology, Air University.

Lee, J. (2012, March 31). *Hacker group LulzSec says it will resume attacks on April fool's day*. Retrieved from http://www.thewhir.com/hacker-group-lulzsec-says-it-will-resume-attacks-on-april-fools-day

Mansfield-Devine, S. (2011). Anonymous: Serious threat or mere annoyance. *Network Security*, *1*, 4–10. doi:10.1016/S1353-4858(11)70004-6

Mills, E. (2011, August 6). AntiSec hackers post stolen police data as revenge for arrests. *CNET News*. Retrieved from http://news.cnet.com/8301-27080_3-20089054-245/antisec-hackers-post-stolen-police-data-as-revenge-for-arrests/

Olson, P. (2012). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. New York, NY: Little, Brown and Company.

Piratpartiet. (2008). *Pirate party declaration of principles 3.2*. Retrieved from http://docs.piratpartiet.se/Principles%203.2.pdf

Pras, A., Sperotto, A., Moura, G. C. M., Drago, I., Barbosa, R., & Sadre, R. Hofstede, R. (2010). *Attacks by 'Anonymous' WikiLeaks proponents not anonymous*. CTIT Technical Report 10.41, (pp. 1-10). CTIT.

Rubenking, N. J. (2012, March 28). LulzSec reborn? Not likely, says F-Secure. *PC Magazine*. Retrieved from http://securitywatch.pcmag.com/hacking/295984-lulzsec-reborn-not-likely-says-f-secure

Sengupta, S. (2012, March 6). Arrests sow mistrust inside a clan of hackers. *The New York Times*. Retrieved from http://www.nytimes.com/2012/03/07/technology/lulzsec-hacking-suspects-are-arrested.html?partner=rss&emc=rss

Storm, D. (2012, February 7). AntiSec leaks Symantec pcAnywhere source code after $50k extortion not paid. *Computer World*. Retrieved from http://blogs.computerworld.com/19695/antisec_leaks_symantec_pcanywhere_source_code_after_50k_extortion_not_paid

Wark, M. (2004). *A hacker manifesto*. Retrieved from http://subsol.c3.hu/subsol_2/contributors0/warktext.html

APPENDIX 2

Code Politics: The Pirate Party and European Political Structures

Introduction

By definition, a "disruptive" technology is one that challenges the current order, whether political or economic or social. By any measure, the popularization of the Internet and WWW in the past two decades has meant challenges to the *status quo* on all three fronts. One example of this involves the battle over information and who should or should not have access to it. WikiLeaks has been pushing for the release of secret information in order to hold governments accountable. Anonymous and its spinoff organizations have pushed for government and corporate accountability and free information. The Pirate Bay has used technologies to enable the distributed exchange of unauthorized media content sharing and downloads. So far, such groups have functioned globally but on the fringes of illegality. A move by the Pirate Bureau in Sweden in 2006 resulted in the establishment of a political party advocating a technology-infused agenda, and in the intervening years, the Pirate Party has involved presences on all continents and over 40 countries, with its branch parties enabled by networking. Pirate Parties have added other policy planks: civil rights; direct democracy; government transparency; the freedom of information, and network neutrality.

These political developments indicate a shift in strategy by using the democratic process in order to publicize a political ideology and agenda. This sidebar offers a light analysis of the Pirate Party and some possible implications for the global order. Namely, it will focus on the following questions:

This party is the first global supranational political party with presences in numerous countries with an ideology based on a mix of anarchist concepts, information piracy values, anti-corporatist approaches, and radical open-source concepts. Their combined membership rolls number in the tens of thousands. The policy package promised by this group involves privacy for individuals and open access to information with the dismantling of corporatist- and government-based intellectual property protections.

If anything, this shows that the digital piracy ideas may have some traction. Some suggest that the social norms around intellectual property protections are much more liberal than the extant laws (Svensson & Larsson, 2012). Further, its proponents have sufficient sophistication to amplify their ideas across many countries and to win adherents globally.

Research Questions: What is the platform of the Pirate Party in Europe? Who are its stakeholders, funders, and main supporters? What change is it trying to bring about? How does it use information and communications technology (ICT) to promote its ideologies? Who are its main rivals?

The International Pirate Party and its Founding

The human enchantment with the Internet and WWW may be seen in early publications about it, when the medium was depicted as somehow transcendent. In cyberspace, people could explore wholly new identities; interact and problem-solve in global communities; share knowledge; "crowd-source" ideas, and immerse in sci-fi realities (Holeton, 1998). Online, people could find meaning. While many of these ideas have dissipated with time, the concept of free information (and "information wants to be free") has been more resilient.

Yochai Benkler (2006), in the print and free e-book *Wealth of Networks,* made the case that digital production enabled nearly costless re-distribution after the marginal cost of creation of the original product. Digital products are non-exclusive and non-consumable, so scaling up the distribution of various digital goods may result in a beneficial surplus for people. MacKenzie Wark (2004, 2006) offered his Hacker Manifesto, which collects a hodge-podge of revolutionary rhetoric to describe the content producers who are taken advantage of by the vectoralist class (which owns the mediums of communications); hackers free the abstracted surplus value from such inventions and improve the lived experiences of the general public. This is an anti-capitalistic approach that advocates resistance against globalization and the world economic system. Some have gone so far as to call this the "New Socialism," which advocates a communal core in digital culture. Here, technological tools are seen to reshape human minds and ways of interacting (Kelly, 2009). Finally, there is the idea of the need for information that may save people. Neal Stephenson in *Cryptonomicon* (1999) wrote of protected "data havens" being set up to enhance people's survivability in a challenging world. (People engage in sense-making of the world around them, and their overlays of understandings of various technological phenomena are fully to be expected).

Technologists followed through with actions. In 1983, Richard Stallman sparked the free software movement with the "GNU is Not Unix" license. Lawrence Lessig, Hal Abelson, and Eric Eldred created the Creative Commons licensure for releasing digital contents into the public commons. A number of search engines enable free searching of open-source contents.

A range of technologies have been deployed that enable the actualization of some of these concepts. Various anonymizers enable some shielding of personal identities as people access information (and/or break into sites). Hacking, malware, spoofing, phishing (and spear-phishing), and social engineering strategies have been used in concert to access privy information from governments and corporations.

Rogue sites have published out or "leaked" various types of copyrighted or protected data. High-level encryption regimes have been made available in open-source ways to protect data from some governments. While content creating companies have been deploying various sorts of Digital Rights Management (DRM) regimes, most of these are broken by hackers and the tools used for the breaking are made available on the Internet. "Torrent" sites have enabled individuals to access unauthorized large-size (megabytes and terabytes) digital contents (software, movies, games, music, electronic books, and other digital contents) from distributed collections and computers through peer-to-peer file sharing. Intellectual piracy has some cachet among certain demographic groups.

One analyst suggests that modern-day digital pirates are informed by a mix of historical and cultural depictions of pirates. Land (2007) writes:

> *Whilst a certain image of piracy has been commodified, another more oppositional and insurgent figure of piracy has carried over from this period to disrupt contemporary regimes of accumulation both through the practices of digital piracy and through anti-capitalist protest. Both of these forms of contemporary organization carry with them the proto-anarchist ideology of autonomy, equality and community that the pirates of the golden age pioneered and which are still articulated today under the banner of Jolly Roger (Land, 2007, p. 170).*

Indeed, modern day digital pirates (under the names of The Pirate Bay, LulzSec, and others) do use self-referential pirate flags.

In Sweden, The Piracy Bureau (Piratbyran) came into being in the Summer of 2003. It was a community space for the Swedish hacker scene and Internet radio broadcasting community. It was conceptualized as a think tank about cyber issues. The group presented lectures, public discussions, and online events—to publicize their interests. One of the group's members, Gottfrid Svartholm, originated the Pirate Bay in November 2003 (Li, 2009).

The Pirate Bay as a site where people download a client onto their computers. Through this, they may find search The Pirate Bay's list of available files for download and access these "torrents" by extracting many segments of a file simultaneously from multiple computers for ease of download in a data swarm (Reynolds, 2010). BitTorrent maintains metainfo files (usually files with a .torrent extension) of available contents. A central tracker identifies the computers running the software which have particular files and enables the sharing. "With the Bittorrent system, the central server need not ever have access to the original file being uploaded by the user," observes one author (Li, 2009, pp. 286 – 287). Simultaneous to their downloading, a downloader's computer is also pushing out contents to others, with their computers acting as both clients and servers.

Essentially, intellectual pirates seem to accept the foundational concept that the author of a work is its first owner (Perry & Margoni, 2010, p. 621), but concepts diverge from there.

In January 2006, the Swedish Pirate Party (*Piratpartiet*) was founded. One has called it "the first political party that works on a global level" (Arsov, 2010) and certainly the first in the Internet Age inspired by some of the free and open principles spawned by the Net. The *Piratpartiet's* stated platform involved three main issues:

1. The fundamental reform of the Copyright System;
2. The abolition of the Patent System; and
3. Respect for personal privacy (Li, 2009, pp. 289 – 290).

The Piratpartiet asserts that the current copyright regime goes too far to protect the commercial interests of publishers to the detriment of the consumers. In this light, they want to decriminalize the file sharing of copyrighted contents. Some advocates suggest that a "pay-per society" may emerge, with pervasive fees for virtually all contents. There is a sense that there are social benefits to open-sharing of cultural artifacts balanced against the harm to copyright holders (Van Eijk, Poort, & Rutten, 2010). The Pirate Party suggests that copyright itself should only last five years. They want to see an end to digital rights management systems and contractual restrictions on copyrighted materials. Finally, they suggest that government filtering of messages, surveillance techniques (like web beacons), and other efforts, may be used to try to track copyright infringers—but also regular private communications—which they see as a risk to common citizens. Citizens should have a right to anonymity, they assert. They should not be trackable using Personally Identifiable Information (PII) on the Internet. Advocates of the Pirate Party stance suggest that there are risks of a "digital enclosure" in which surveillance is common, and a panopticon (where everything is known in a surveillance society) as described in Mark Andrejevic's *ISpy* (2007) may emerge.

The Piratpartiet's anti-copyright and anti-DRM stance goes against a range of extant international treaties: the Berne Convention (1887), signed by Sweden in 1904, and the Trade Related Aspects of Intellectual Property Rights or TRIPS treaty, required as part of membership to the World Trade Organization (WTO) (1994). Such treaties work to harmonize Intellectual Property (IP) laws. This political party's stance also contradicts a number of Sweden's and the European Union's Copyright Laws (affirmed by the EU's Court of Justice of the European Community).

In practice, though, people who would access copyrighted materials without permission did so without much in the way of punishment.

> *In principle, copyright in Sweden has always meant that it was forbidden to share protected material on the internet without the consent of the rights holder. However, it has been very difficult to punish those who engage in this kind of activity, since in practice it has not proved possible to identify individual file-sharers. The absence of functioning legal tools, surveillance, and sanctions has contributed to the development within society of a large measure of acceptance of this type of crime, and, quite simply, people have not taken this law seriously (Svensson & Larsson, 2012, p. 4).*

The European Union's Intellectual Property Rights Enforcement Directive (IPRED law) further affirmed these intellectual property (patent and copyright) laws, with a focus on online infringements. The law's passing resulted in an 18% drop in Swedish internet traffic in the six months following the passage of this law Increased sales of physical music by 27% and digital music by 48% (Ademon & Liang, 2010, p. 1). The law had no significant effects on theater ticket sales or the sales of DVD movies, showing that illegal downloads substituted for some purchases of physical and digital music but not so much in terms of theater and DVD movies. (To contextualize broadly, BitTorrent's multi-source streaming is responsible for a large amount of Internet traffic. Sandvine's Fall 2011 report on Global Internet phenomena observed that BitTorrent accounted for 20 – 50% of all upstream traffic and .07 to .17% of all downstream traffic based on geographical regions during peak periods (Han, Kim, Chung, Kwon, Kim, & Choi, 2012, p. 77)).

If legislators were hoping that laws would work as a forcing function in terms of changing culture, they did not see any changes in the near-term. The EU IPR Enforcement Directive 2004/48/EC did not much change the social norms for file sharing in Sweden. Even in the six months after the IPRED law, few felt social pressure to stop illegally accessing copyrighted files (Svensson & Larsson, 2012, p. 13). The before- and after-surveys bracketing the IPRED law did not show much difference in social attitudes. What surveys found was that if enforcement were shored up, then free-riding downloaders would be less likely to help themselves.

The EU focused on shoring up the legal structures protecting copyright among its member states. Contemporaneously, the various countries' law enforcement were acquiring the skills to start pursuing IP pirates.

> *However, other legislation also affects the enforcement of copyright, such as the Data Retention Directive (Directive 2006/24/EC, 2006), while copyright is also involved in different legislative procedures such as the European Telecoms Reform Package and the Anti-Counterfeit Trade Agreement, ACTA (Larsson, 2011b). The overarching goal within the EU is to harmonize the national legislation of the different EU Member States with regard to Information and Communications Technology (ICT), thereby achieving greater control over the use of the internet. This is considered to be essential, if the objective is to support copyright owners in their fight against illegal file sharing. In addition, copyright holders' representatives are being given legal tools that allow violators to be identified. There is also a trend towards allocating greater responsibility to internet service providers for the type of content that is transmitted through their infrastructure (Svensson & Larsson, 2012, p. 2).*

Fund-Raising Endeavors

The Pirate Party launched Relakks, a commercial darknet service that cost €5 a month to access encrypted private networks that enable the distribution of contents with relative anonymity from detection and surveillance (Paul, 2006). Darknet is a protocol layer that exists on current networks to enable a range of silent or semi-anonymous actions, such as peer-to-peer sharing. [The lack of so-called "endpoint anonymity" had been a risk to many downloaders for years (Biddle, England, Peinado, & Willman, 2002), with potential traceability by both commercial and government entities.] This service was set up to fund the political activities of the Pirate Party.

Another fund-raising effort was started in early 2007, albeit by The Pirate Bay, to buy its own "nation" based on the concept of a "data haven" that would be a "pirate utopia":

> *The target of the proposed acquisition was a self-proclaimed independent state named Sealand. Perched atop an old World War II anti-aircraft gun emplacement long since abandoned by the British military, Sealand had been inaugurated by an Essex fisherman and part-time pirate radio entrepreneur, Roy Bates, in the late 1960s. Bates had originally intended to use the platform as a base for a revived pirate broadcasting effort, but in the end that plan had fizzled, and successive efforts to come up with some other way of making the 'principality' a going concern had been little more successful. The latest scheme had been to make it a data haven. In 2000, Westminster seemed set to legislate for all ISPs to be brought under the purview of official investigators. Sealand saw an opportunity in the move, and announced that it would offer a venue for anyone wanting to issue material to the Internet beyond the reach of any such state oversight. Its London-based commercial arm, named HavenCo, invited applications (Johns, 2009, p. 44).*

This endeavor came to nothing, and the funds raised were insufficient for a serious bid (Johns, 2009, p. 45).

In 2007, the Pirate Party launched a youth organization, known as the Young Pirates. The organization's power base in Sweden was not in urban areas, per se, but in "provincial towns around Sweden as Tidaholm and Markaryd, but also small university cities as Lund and Uppsala" (Demker, 2008, p. 18). The party advocated a variant of liberal individualism: people have privacy rights and rights to information. Further, they asserted that "immaterial rights should be abandoned" (Demker, 2008, p. 18).

Content creating corporations—particularly those in movies and music—had been working for years to push through legislation to protect their interests. They went to the Supreme Court in *MGM v. Grokster,* 125 S.Ct. 2764 (2005) to establish third-party liability for "inducing" infringement. (Already on the books were laws related to vicarious and contributory liabilities. It is illegal to publicly perform unauthorized licensed contents. Further, there have been efforts to make linking to unauthorized streaming contents illegal (Lunardi, 2009).) While the case was ultimately remanded, the justices made it clear that they saw some liability in third parties that enabled the compromise of copyright (Radcliffe, 2006).

The Pirate Bay, hosted in Sweden, was raided by the Swedish police on May 31, 2006. Swedish law enforcement was under pressure to act by the U.S. government and the Motion Picture Association, the international branch of the U.S.-based Motion Picture Association of America (MPAA). The site reappeared only three days after the raid. (The Pirate Bay site is still up and functioning at http://thepiratebay.se/.)

However, the raid resulted in the Pirate Bay doubling the number of its users due to media attention, and the membership of the Piratpartiet went up by thousands (Li, 2009). The Pirate Party has been labeled a "virtue party" based on its ideological platform with "utopian goals." None of the party's founders had any parliamentary experience (Demker, 2008, p. 17).

In the 2006 elections in Sweden, the Pirate Party won 34,918 votes or 0.63% of the voting population. It placed one elected member in the parliament. It became known as the "third largest political group now represented within Sweden's parliament" (Li, 2009, p. 289) and the fourth largest political party in Sweden. It was both a social movement of digerati and copyright liberalists as well as a political party.

In April 2009, the four individuals supporting The Pirate Bay in Sweden were found to be in breach of the Copyright Act. They were handed down a year's imprisonment and a fine of $4.5 million (Reynolds, 2010).

The Impact of the Pirate Party on Various European Countries and their Political Systems

The Pirate Party has presences in a number of other countries in the European Union and around the world. (The German Pirate Party (*Pratenpartei*) was founded in 2006 and modeled after the Swedish *Pirapartiet*. In the 2009 German general election, it garnered 2% of the vote. In 2011, in the Berlin state elections, The Pirate Party won 8.9% of the votes and first-ever seats in a state parliament and have gained representation on every German state parliament since then (North Rhine-Westphalia, Saarland, and Schleswig-Holstein), with about 8% of the votes. ("Pirate Parties International," Nov. 1, 2012)) The Pirate Party International was founded in Brussels at the PPI Conference on April 18, 2010.

One may conceptualize governments and commercial companies promoting physical and intellectual property rights. One organization tracks the international property rights of 125 countries annually based on similar measures. These 125 countries cover 97% of the world's peoples. A 2010 report of the world's

International Property Rights Index (IPRI) shows much of Europe listed in the top quintile for enforcing property rights, but some of its countries show only in the mid-range (along with countries like China). Those protecting intellectual property are seen as some of the powers arrayed against the Pirate Parties.

According to the International Property Rights Index, Sweden is #2 in the world in terms of its property rights ranking (higher than the U.S. at 15). So far, no known nation-state has capitulated to the agenda of this party, based on a review of the literature. Mounted against these parties are the extensive powers of state: their laws, law enforcement, intelligence agencies, surveillance capabilities, and media access. It is highly unlikely that the Pirate Party (in any country) will be more than an ephemeral political phenomenon given the hard-won protections for property rights in many regions of the world.

The high costs of Research and Development (R&D) for corporations mean that if patents and copyrights no longer exist, these companies will lack the funding streams to actually innovate with educated and trained professionals and the quality assurance regimes in place. (If the world described by The Pirate Party were created, one could imagine a "tragedy of the commons" phenomena occurring—with individuals taking advantage of what is free but contributing little to its actual upkeep. A study of Wikipedia has shown that the power law is in play, with a few contributed inordinately much, but a majority of users just free-riding that resource.) Governments have a vested interest in protecting their respective economies, and those that serve as illegal data havens will likely find themselves constrained by the legal regimes around the world. Law enforcement agencies have become much more adept at working through the global bureaucracies that protect global trade from counterfeits, and the same bureaucratic levers will be employed to protect digital goods. Identities on the Internet and WWW are eminently trackable through Personally Identifiable Information (PII), and it will be very difficult to set up digital shops to distribute unauthorized digital contents without being identified, blacklisted, and shut down, if not also prosecuted. While individuals may ardently access copyrighted goods, as free riders, most will not likely be willing to suffer sanctions in order to access such materials (in a cost-benefit consideration).

CONCLUSION

This is not to say that in the struggles over information and privacy that those who are sympathetic to the Pirate Party's agenda will not occasionally win skirmishes.

The popularization of the Pirate Party shows the global connectivity of the Social Web, which enables collaborations and political organization around motivating ideas in a globalized way. Those who are self-declared rebels against the established order, the capitalist *status quo*, have a range of electronic communications tools at hand to promote their ideas and actions. That they would pursue legitimate elected power simultaneous with their appeals to the broad masses and their darknet efforts shows sophistication in their political advocacy and activism.

Finally, while the social norms and cultures of the European Union seem to be lined up for free and open-source access to digital contents, the legal levers and leaders seem aligned against IP pirates. Unless they can bring some powerful allies alongside and field as-yet-unknown technologies, their cause will not likely progress beyond the present.

REFERENCES

Ademon, A., & Liang, C.-Y. (2010). *Piracy, music, and movies: A natural experiment*. Working Paper 2010: 18. Uppsala, Sweden: Uppsala Universitet.

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence, KS: University Press of Kansas.

Arsov, S. (2010). The pirate party and copyright liberalists. *Entertainment and Sports Lawyer, 27*(4).

Benkler, Y. (2006). *Wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press. Retrieved from http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf

Biddle, P., England, P., Peinado, M., & Willman, B. (2002, November 18). The darknet and the future of content distribution. In *Proceedings of the 2002 ACM Workshop on Digital Rights Management*. Washington, DC: ACM Press. Retrieved from http://www.bearcave.com/misl/misl_tech/msdrm/darknet.htm

Demker, M. (2008). *A new era of party politics in a glozalised world: The concept of virtue parties.* Working Paper Series 2008: 20. Gothenburg, Sweden: University of Gothenburg.

Han, J., Kim, S., Chung, T., Kwon, T. T., Kim, H.-C., & Choi, Y. (2012). Bundling practice in BitTorrent: What, how, and why. [London, UK: ACM Press.]. *Proceedings of Sigmetrics*, *2012*, 77–88. doi:10.1145/2318857.2254768

Holeton, R. (1998). *Composing cyberspace: Identity, community, and knowledge in the electronic age*. Boston, MA: McGraw Hill.

Johns, A. (2009). Piracy as a business force. *Culture Machine*, *10*, 44–63.

Kelly, K. (2009). The new socialism: Global collectivist society is coming online. *Wired Magazine, 17*(6).

Land, C. (2007). Flying the black flag: Revolt, revolution and the social organization of piracy in the golden age. *Management & Organizational History*, *2*(2), 169–192. doi:10.1177/1744935907078726

Li, M. (2009). The pirate party and the pirate bay: How the pirate bay influences Sweden and international copyright relations. *Pace International Law Review*, *21*(1), 281–307.

Lunardi, J. J. (2009). Guerrilla video: Potential copyright liability for websites that index links to unauthorized streaming content. *Fordham Intellectual Property*. *Media and Entertainment Law Journal*, *19*(4), 1077–1129.

Paul, R. (2006, August 15). Swedish political party offers commercial darknet access. *Ars Technica*. Retrieved from http://arstechnica.com/uncategorized/2006/08/7502/

Perry, M., & Margoni, T. (2010). From music tracks to Google maps: Who owns computer-generated works? *Computer Law & Security Report*, *26*, 621–629. doi:10.1016/j.clsr.2010.09.005

Pirate Parties International. (2012, November 1). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Pirate_Parties_International

Radcliffe, M. F. (2006). Grokster: The new law of third party liability for copyright infringement under United States law. *Computer Law & Security Report*, *22*, 137–148. doi:10.1016/j.clsr.2006.01.005

Reynolds, G. (2010). Pirate bay on English bay? Bittorrent file sharing and copyright infringement in the Supreme Court of British Columbia. *University of British Columbia Law Review*, *43*, 193–204.

Strokova, V. (2010). *International property rights index 2010 report*. Washington, DC: Property Rights Alliance.

Svensson, M., & Larsson, S. (2012, August). Intellectual property law compliance in Europe: Illegal file sharing and the role of social norms. *New Media & Society*, 1–17.

Van Eijk, N., Poort, J., & Rutten, P. (2010). Legal, economic and cultural aspects of file sharing. *Communications & Strategies*, *77*(1), 35–54.

Wark, M. (2006). *A hacker manifesto*. Retrieved from http://subsol.c3.hu/subsol_2/contributors0/wark-text.html