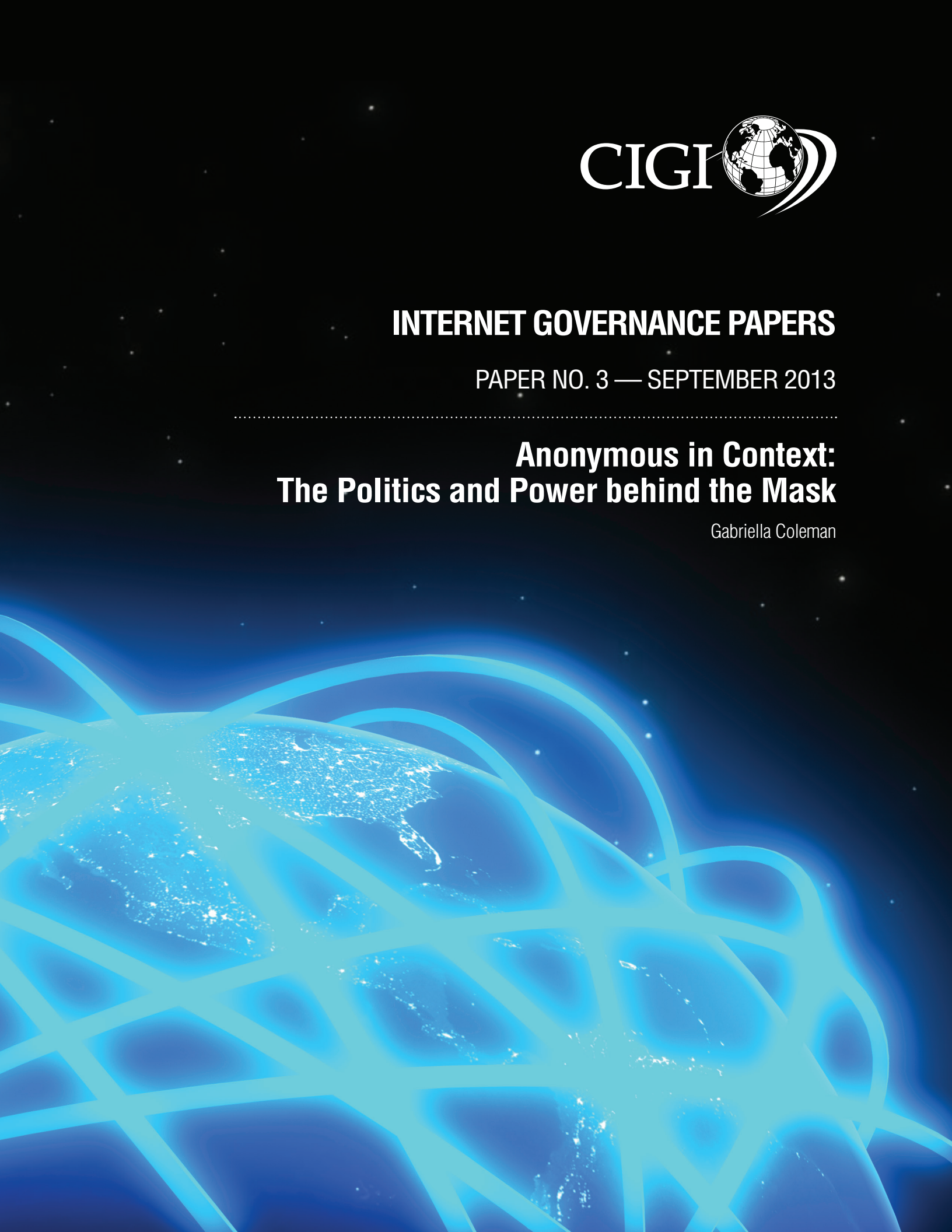

INTERNET GOVERNANCE PAPERS

PAPER NO. 3 — SEPTEMBER 2013

Anonymous in Context: The Politics and Power behind the Mask

Gabriella Coleman

INTERNET GOVERNANCE PAPERS
PAPER NO. 3 — SEPTEMBER 2013

Anonymous in Context: The Politics and Power behind the Mask

Gabriella Coleman

ACKNOWLEDGEMENTS

CIGI gratefully acknowledges the support of the Copyright Collective of Canada.

The author would like to thank Mark Raymond, Christopher Prince, Darin Barney and Maya Richman for their generous and valuable comments.

57 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CONTENTS

ABOUT ORGANIZED CHAOS: REIMAGINING THE INTERNET PROJECT

Historically, Internet governance has been accomplished *en passant*. It has emerged largely from the actions of computer scientists and engineers, in interaction with domestic legal and regulatory systems. Beginning at least with the 2003–2005 World Summit on the Information Society process, however, there has been an explicit rule-making agenda at the international level. This strategic agenda is increasingly driven by a coalition of states — including Russia, China and the Arab states — that is organized and has a clear, more state-controlled and monetary vision for the Internet. Advanced industrial democracies and other states committed to existing multi-stakeholder mechanisms have a different view — they regard Internet governance as important, but generally lack coherent strategies for Internet governance — especially at the international level. Given the Internet's constant evolution and its economic, political and social importance as a public good, this situation is clearly untenable.

A coherent strategy is needed to ensure that difficult trade-offs between competing interests, as well as between distinct public values, are managed in a consistent, transparent and accountable manner that accurately reflects public priorities. Guided by these considerations, CIGI researchers believe they can play a constructive role in creating a strategy for states committed to multi-stakeholder models of Internet governance.

In aiming to develop this strategy, the project members will consider what kind of Internet the world wants in 2020, and will lay the analytical groundwork for future Internet governance discussions, most notably the upcoming decennial review of the World Summit on the Information Society. This project was launched in 2012. The Internet Governance Paper series will result in the publication of a book in early 2014.

ABOUT THE AUTHOR

Gabriella Coleman is the Wolfe Chair in Scientific and Technological Literacy at McGill University. Trained as an anthropologist, she teaches, writes and researches on the ethics of computer hacking, with a focus on open source software and the digital protest ensemble Anonymous. She is the author of *Coding Freedom: The Ethics and Aesthetics of Hacking* (published in 2012 by Princeton University Press) and is currently working on a second book on Anonymous.

ACRONYMS

ACTA	Anti-Counterfeiting Trade Agreement
BART	Bay Area Rapid Transit
DDoS	distributed denial of service
EDT	Electronic Disturbance Theatre
EFF	Electronic Frontier Foundation
IRC	Internet Relay Chat
LOIC	Low Orbit Ion Cannon
NSA	National Security Agency
PR	public relations
SOPA	Stop Online Piracy Act

EXECUTIVE SUMMARY

Since 2010, digital direct action, including leaks, hacking and mass protest, has become a regular feature of political life on the Internet. This paper considers the source, strengths and weakness of this activity through an in-depth analysis of Anonymous, the protest ensemble that has been adept at magnifying issues, boosting existing — usually oppositional — movements and converting amorphous discontent into a tangible form. It has been remarkably effective, despite lacking the human and financial resources to engage in long-term strategic thinking or planning. Anonymous has neither the steady income nor the fiscal sponsorship to support a dedicated team tasked with recruiting individuals, coordinating activities and developing sophisticated software. Wherein, therefore, lies the power of Anonymous? How has it managed to strike such fear into corporations, governments and other groups? This paper answers these questions by examining the intersecting elements that contribute to Anonymous' contemporary geopolitical power: its ability to land media attention, its bold and recognizable aesthetics, its participatory openness, the misinformation that surrounds it and, in particular, its unpredictability. Anonymous signals the growing importance of what I call "weapons of the geek," a modality of politics exercised by a class of privileged and visible actors who are often at the centre of economic life. Among geeks and hackers, political activities are rooted in concrete experiences of their craft — administering a server or editing videos — skills channelled toward bolstering civil liberties, such as privacy.

INTRODUCTION

In 2012, Obama's re-election campaign team assembled a talented and dedicated group of programmers, system administrators, mathematicians and data scientists to develop software that would help the incumbent president secure a second term. Used for fundraising and voter targeting, the system also crunched and analyzed data to fine-tune voter targeting with the hope of giving the campaign a critical edge over Republican presidential candidate Mitt Romney. Amid much fanfare after Obama's victory, journalists praised his star-studded technology team, detailing members' hard work, success and travails — heralding the system a stellar success.

One of the team's major concerns, however, was not reported in the media. At all costs, the Obama team wanted to avoid attracting the attention of Anonymous, a banner used by individuals and groups to organize diverse forms of collective action, ranging from street protests to distributed denial of service (DDoS) campaigns to hacking. The Obama campaign team treated Anonymous as (potentially) being even more of a nuisance than the foreign state hackers who had infiltrated the McCain and Obama campaigns in 2008.[1] If Anonymous had successfully accessed servers or DDoS-ed the campaign website, it would have ignited media attention and potentially battered the campaign's reputation. Although this alone would not likely have jeopardized Obama's chances for re-election (since his team was confident that there was no controversial information to leak), a visit from Anonymous was considered a real possibility and liability.

Unlike Anonymous, many hackers work surreptitiously. Organizations that have been hacked usually get to decide whether or not to disclose their situations to the public. This was the case, for example, with *The New York Times*, which made the

1 See Brian Todd (2008), "Computers at the Headquarters of the Obama and McCain Campaigns Were Hacked CNN Confirms," CNN, November 6, available at: http://politicalticker.blogs.cnn.com/2008/11/06/computers-of-obama-mccain-campaigns-hacked.

decision to go public after allegedly being targeted by Chinese state hackers for months. Anonymous, on the other hand, seeks publicity before and after every successful action.

There is a paradox at work here: state-supported hacking is generally much better organized and funded and, in some respects, far more powerful than actions undertaken by Anonymous. Stuxnet is a perfect example. Developed by the Israeli and American governments, this state-of-the-art malware was used to disable Iran's capacity to produce enriched uranium. While Anonymous once claimed to have created Stuxnet, its statement was immediately identified as a hoax. Anonymous lacks the human and financial resources to engage in the long-term strategic thinking or planning required to code military-grade software. It has neither the steady income nor the fiscal sponsorship to support a dedicated team tasked with recruiting individuals, coordinating activities and developing sophisticated software.

Anonymous is difficult to pin down. Some "Anons" work independently, while others work in small teams or join a swarm of demonstrators during a large-scale campaign. Anonymous tends to ride and amplify the wave of existing events or causes. Even if it magnifies and extends the scope of an event — sometimes so significantly as to alter its nature or significance — the campaign eventually ends as the wave hits the shore. Sometimes Anonymous misses the wave, especially when the mainstream media fails to jump on board to report on its operations.

Wherein, therefore, lies the power of Anonymous? How has it managed to strike such fear into corporations, governments and other groups, such as the Obama campaign team, and accomplish its objectives?

This paper showcases various intersecting elements that contribute to Anonymous' contemporary geopolitical power: its ability to land media attention, its bold and recognizable aesthetics, its participatory openness and the misinformation that surrounds it. One feature stands out: Anonymous' unpredictability.

Take, for example, its birth as an activist endeavour. Before 2008, the name Anonymous was deployed almost exclusively for "trolling," which in Internet parlance means pulling pranks targeting people and organizations, desecrating reputations and revealing humiliating or personal information. Trolling was coordinated on the Internet, often on the image board 4chan.org, for the sake of "the lulz," that is, "the laughs." Anonymous accidentally — although dramatically — enlarged its repertoire of tactics in 2008, when it sprouted an activist sensibility during a full-fledged pranking campaign against the Church of Scientology. By 2010, distinct and stable activist nodes of Anonymous had emerged. The name Anonymous was increasingly being used to herald activist actions, often in ways that defied expectations.

Mutability and dynamism continue to be a staple of Anonymous' activism and historical development. As a result, it is difficult to forecast when or why Anonymous will strike, when a new node will appear, whether a campaign will be successful and how Anonymous might change direction or tactics during the course of an operation. A by-product of the Internet, Anonymous rises up most forcefully and shores up the most support when defending values associated with this global communication platform, such as free speech. As one Anonymous participant phrased it during an interview, "free

speech is non-negotiable."[2] But Anonymous has repeatedly demonstrated that it is not bound to this or any other imperative. Over the last five years, Anonymous has contributed to an astonishing array of causes, from publicizing rape cases in small-town Ohio and in Halifax to aiding in the Arab and African Spring of 2011. This growth, circulation and ongoing metamorphosis make their next steps difficult to ascertain.

Despite media reports to the contrary, Anonymous, although it may be nimble, flexible and emergent, is not random, shadowy or chaotic. Anonymous may be devilishly unpredictable and difficult to study, but it still evinces core features. These attributes are discussed in this paper.

Further contextualizing Anonymous in light of global currents over the last few years, it is rather unsurprising that a fiery protest movement, often wedded to the Internet, has arisen at this time and in this particular form. As indicated by its name, Anonymous dramatizes the importance of anonymity and privacy in an era when both are rapidly eroding for citizens, and when government secrecy and systematic surveillance are on the rise, especially in the United States. Anonymous has also roared and soared in a tumultuous period of global unrest and discontent, evident in the large-scale popular uprisings: the 15-M movement in Spain,[3] the Arab and African Spring and the Occupy movement. Over the last two years, sharp economic inequalities the world over have been met by a tide of protest activity. While distinct, Anonymous is part and parcel of these trends, symbolically showcasing the ideal for privacy and acting as the popular face of unrest across these movements. Anonymous thus demonstrates the power of symbolic engagement as a subspecies of direct social action.

This paper is divided into three sections. The first provides a fairly straightforward narrative account of Anonymous from 2005 to 2012, honing in on major events and turning points in its constitution and evolution. This chronology is necessary given Anonymous' chameleon nature and the high degree of misinformation surrounding it. The second section briefly considers the core features of Anonymous, which shed light on its political significance. Section three focusses on the strengths and weaknesses of Anonymous as a protest movement.

THE FORMATION AND MUTATIONS OF ANONYMOUS

2005–2010: From Trolling to Irreverent Activism

Anonymous' ancestry lies in the often obnoxious, occasionally humorous and at times terrifying world of Internet trolling, where pranking abounds. Trolling can be within the purview of a single individual, anonymous crowds or tight-knit trolling associations with offensive and racist names like "Gay Niggers Association of America." Whether lighthearted or gruesome, propelled by a horde or delicately masterminded by a few individuals, trolling almost always entails an unpredictable combination of trickery, defilement and deception.

By 2007, Anonymous was so well known for trolling that Fox News anointed it the "Internet hate machine" (Fox News, 2009). Anonymous mockingly embraced this hyperbolic title, no doubt enjoying having gotten under the media's skin. Soon after, someone used the name Anonymous to release a video, a grim parody drawing on Hollywood slasher flicks. The video proclaimed Anonymous as "the

2 Unless otherwise indicated, quotes from Anonymous derive from interviews conducted with participants during anthropological research carried out between 2008 and 2013.

3 The 15-M movement refers to a series of demonstrations over the economic crisis in Spain launched on May 15, 2011.

face of chaos" that "laughs at the face of tragedy" (Anonymous, 2007) and captured trolling's terrifying potential, especially for those who are not in on the joke.

Six months after being labelled the "Internet hate machine," other individuals, largely from 4chan, used the name Anonymous and its associated iconography (headless men in black suits) to troll and subsequently organize earnest street demonstrations. Trolling against the Church of Scientology began in January 2008, catalyzed by the infamous internal recruitment video of Tom Cruise praising the church's efforts to "create new and better realities." The video, leaked by critics of the church, promptly went viral.

When the Church of Scientology threatened Web publishers such as Gawker with legal action if they did not remove the video, Anonymous initiated what even today is considered by Anonymous to be one of their most legendary raids. Impelled by the lulz, Anonymous launched DDoS attacks to jam Scientology websites, ordered unpaid pizzas and escorts for Scientology churches across North America, faxed images of nude body parts to churches and relentlessly phone pranked the church, in particular the Dianetics hotline (where callers can get advice about the "first truly workable technology of the mind"). Within a matter of weeks, trolling gave way to Project Chanology, a prolonged and earnest political campaign against the Church of Scientology, which continues to this day.

Various forces and factors unexpectedly converged to ignite this metamorphosis. One inspiration was a viral video calling for the "systematic dismantling of the Church of Scientology" (Anonymous, 2008). Although the video was intended as a joke (that is, for the lulz), it prompted a debate about whether Anonymous should more purposively protest the church or remain faithful to its madcap roots. Enough individuals were willing to move forward with the proposed experiment, and on February 10, 2008, over 7,000 individuals protested in 127 cities. Many demonstrators sported plastic Guy Fawkes masks in order to conceal their identities. Since then, the mask has remained Anonymous' signature icon.

Although the protests were well organized and hailed as a triumph by participants, many of them knew very little about the Church of Scientology and its abuses, at least outside of pop culture references. A combination of mischief and exploration drove many of them to streets. Since the image board 4chan is anonymous and discourages even the use of pseudonyms (persistent nicknames and identities), many Anons went for the rare opportunity to meet their brethren with no intention of engaging in further activism. Nevertheless, a large enough number of rabble-rousers carried on with the demonstrations to constitute Anonymous as an activist enterprise; copious media coverage (which is a common feature in the history of Anonymous) also secured the ongoing life of Anonymous as a medium for directed political organizing.

Although many participants, especially trolls, contested Anonymous' newfound political will, enough Anons stayed on to sustain a nascent political movement. The seeds of unpredictability, irreverence and deviance had also been sown among these politically minded Anons. Some degree of pranking and trickery has played a part in Anonymous' political operations ever since.

2010–2012: The Explosion of Digital Direct Action

In 2009 and 2010, Anonymous' actions were centred on Project Chanology and trolling. Some people participated in Project Chanology solely online, engaging in boisterous discussion on the popular web forum Why We Protest. Others, especially

those living in or close to major cities across North America and Europe, showed up at monthly street protests rain or shine (or snow) to mock Scientology adherents and air the documented human rights abuses of the church. They were supported by a small cadre of committed Scientology defectors, some of whom started to identify as Anonymous. Some of these defectors hail Anonymous as the "game changer" that enabled them to be open and public about their ordeals with the church (Christman, 2012).

During this period, Anonymous branched out politically. For instance, some individuals who were active in Chanology contributed to Iran's fervent (though unsuccessful) green revolution. In 2009, denizens of 4chan were still using the name Anonymous for notorious trolling escapades. Trolling began to wane in 2010, when Anonymous' political portfolio diversified considerably. At the time of this writing, pure trolling under the name Anonymous had largely ceased. There is, however, nothing preventing its resurrection.

In February 2010, individuals coordinated "Operation Titstorm," a DDoS attack on the Australian government to protest legislation aimed at curbing pornography by requiring Internet service providers to use filters. "No government should have the right to refuse its citizens access to information solely because they perceive it to be unwanted," declared Anonymous in an email sent to the press. "The Australian government will learn that one does not mess with our porn. No one messes with our access to perfectly legal (or illegal) content for any reason" (quoted in Cheng, 2010).

The political use of a DDoS attack placed Anonymous in a camp alongside "hacktivists" like the Electronic Disturbance Theatre (EDT), which had hosted "virtual sit-ins" in the late 1990s. In 1997, for instance, the EDT flooded Mexican government websites to support the Zapatistas' struggles for autonomy. While Anonymous had initially deployed DDoS attacks during their first trolling raid against the Church of Scientology, Project Chanology abandoned this tactic. It never approved of nor relied much on hacking. To this day, Project Chanology opposes the use of DDoS attacks and tends to dismiss the networks that deploy them. To acknowledge its internal feuds and sectarianism, Anonymous eventually adopted the refrain "Anonymous is not unanimous." This message has yet to penetrate public consciousness — the mainstream media still tends to describe participants only as hackers, technological actors already freighted with simplistic and pejorative associations.

In September 2010, seven months after "Operation Titstorm" (and two years after venturing into the world of political activism), a new node hatched following a rift over protest styles. Organizing in the name of Internet freedom, a group of Anons had set their eyes on protesting the multilateral Anti-Counterfeiting Trade Agreement (ACTA) through legal channels alone. A handful of the group clamoured for direct action tactics, which included "black fax, emails, phone calls, pizzas called to the office, a full on classic Anon assault," as one participant described it to me. In the minority, they were banned from a particular Internet Relay Chat (IRC) server, but naturally could still use the name. So they did, and proceeded to "blitz these guys [copyright industry] into paying attention" by DDoS-ing pro-copyright associations such as the Motion Picture Association of America in defence of piracy and file sharing.

This group eventually managed to attract a sizable street team of participants and supporters. After roaming from one IRC network to another, these participants eventually established a dedicated IRC server named AnonOps in November 2010. This

network, known by the name of its IRC server, would come to boldly embrace DDoS tactics and eventually endorse hacking as a political weapon, thus becoming one of the biggest and most controversial media sensations.

By early December 2011, however, AnonOps IRC chat rooms, once bustling with life, had come to a standstill. Core AnonOps participants — system administrators, organizers, media makers and hackers — were concerned by its dwindling number of supporters. Then on December 9, 2010, the number of supporters skyrocketed. AnonOps managed to tap into, channel and thus render visible the collective furor over what its supporters deemed to be a wholly inappropriate act of censorship against the whistle-blowing organization WikiLeaks, which had caused a firestorm of controversy after releasing a trove of leaked classified diplomatic cables. Anonymous, specifically AnonOps, launched a DDoS campaign aimed at PayPal, MasterCard and Visa in response to their refusal to accept donations for WikiLeaks' front man, Julian Assange.

The technical work of jamming website access was coordinated by a select number of participants using botnets (a large network of compromised computers). Many other individuals contributed using a tool known as Low Orbit Ion Cannon (LOIC). An open source application available for download on the Internet, LOIC allows users to contribute to a DDoS campaign. LOIC lacked privacy protections, however, and participants were not consistently informed that they would be put at legal risk unless they took extra precautions to hide their IP addresses. (Eventually, 14 individuals, now known as the PayPal 14, would be arrested in the United States in mid-July 2011 over alleged participation in these events.) This mass participation may not have been technically necessary, and it was certainly ethically dubious. Nevertheless, it revealed to the world at large the level and scope of supporters' disenchantment with what they saw as unacceptable corporate censorship.

This gathering was also one of the first large-scale spontaneous online demonstrations. The outpouring of support even surprised AnonOps. Numbers on the IRC channel jumped from 70 individuals to 7,000 in a couple of days (a fraction were also bots). As one participant explained, this left AnonOps "stunned and a little frightened." The targeting of WikiLeaks was yet another catalyst for politicizing Anonymous; some key participants and organizers active today jumped aboard at a momentous time.

By 2011, both Anonymous and WikiLeaks were recognized as staunch — albeit controversial — advocates for free speech. Both were ready to pounce into action, in distinct ways, in the face of censorship. Prompted by the Tunisian government's blocking of WikiLeaks, on January 2, 2011, AnonOps released a video launching OpTunisia. The campaign was initially spearheaded by one person, who corralled a group of participants, some of whom became moderators (they helped "keep order" on the public IRC channel by keeping the conversation on-topic and kicking trolls off the channel). A technical team of hackers attacked Tunisian government websites and undermined software the dictatorial regime was using to spy on citizens. Many others aided by translating information, writing manifestos and crafting publicity videos.

Although Anonymous initially intervened to stamp out censorship, the same team continued to lend a helping hand as country after country in the region underwent revolution. Individuals organized in a dedicated AnonOps chat room, and the operations became collectively known as the "Freedom Ops." For several months, they teamed up with local activists and hackers in Libya, Egypt, Algeria and Syria. Although many participants have since moved

on or simply vanished, some forged relationships and connections that continue to this day.

By this time, Anonymous had become multitudinous, prolific and unpredictable. In January 2011, AnonOps was buzzing with activity, making it impossible for one person to stay abreast of all the developments. The IRC network housed dozens of distinct chat channels for other ongoing operations to support the environment, student movements in Latin America and WikiLeaks, among other causes.

Then, early in February 2011, an impromptu operation — targeting the corporate security firm HBGary — fundamentally and dramatically reconfigured the political culture of AnonOps. Participants transitioned from covert to public forms of hacking, such as Web defacing. Hacking, always a tool but often used more clandestinely, became a public act, wielded for multiple purposes: vengeance, turf protection, technological assistance, theatrics, exposing security vulnerabilities, searching for information to leak and for the lulz.

Much like the formation of Chanology, this transition wasn't planned. It was a spontaneous act of revenge prompted by the actions of Aaron Barr, CEO of HBGary. Barr boasted that his firm had compromised Anonymous, claiming to a reporter that it had allegedly discovered the real identities of top operatives and was ready to hand them over to the FBI; a spreadsheet of names had been found and circulated online. In response, an AnonOps crew took the initiative to locate security vulnerabilities on HBGary servers and search for information to leak. A small group of hackers commandeered Barr's Twitter account. They hacked HBGary servers, downloaded 70,000 emails and deleted files. They purportedly wiped out Barr's iPhone and iPad, and then published the company's data alongside Barr's private communications. They sent the following cocky rationale to a reporter for the Tech Herald, who had covered their actions for many months:

> Let us teach you a lesson you'll never forget: you don't mess with Anonymous. You especially don't mess with Anonymous simply because you want to jump on a trend for public attention. You have blindly charged into the Anonymous hive, a hive from which you've tried to steal honey. Did you think the bees would not defend it? Well here we are. You've angered the hive, and now you are being stung. It would appear that security experts are not expertly secured. (quoted in Ragan, 2011)

Anonymous unearthed a damning document entitled "The WikiLeaks Threat," which outlined how HBGary, in conjunction with the US Chamber of Commerce, the Bank of America, Palantir Technologies and other security companies, could undermine WikiLeaks by submitting fake documents to the organization. Anons also found evidence of plans to tarnish the reputations of WikiLeaks supporters, including journalists such as Glenn Greenwald. Celebrated by Anonymous at large for restocking the lulz, this operation inspired a team of technological elites to break away and devote themselves to the pursuit of mischief, unambiguously proclaimed in their choice of name: LulzSec. "When you get over nine thousand PM's [private messages on IRC] asking to help in some random 'op'" explained one member, "it's a case of 'the hell with this, I want to go have some fun.'"Although the press usually equated LulzSec with Anonymous, the hacker crew attempted to distance itself from the larger collective due to their freewheeling attitude and their indiscriminate choice of targets. In contrast to Anonymous, for instance, LulzSec went after the

press, who had been totally off limits, even among the networks such as AnonOps that favoured illegal direct action tactics.

It is likely for this reason that the infamous Sony PlayStation hack, executed between April 17 and 19, 2011, was often retroactively (and, as far as we know, incorrectly) attributed to LulzSec and, at the time of the hack, to Anonymous, as LulzSec had yet to come into being. The massive breach forced Sony to shut down the network for a prolonged period of time, leading to significant financial loss and scores of irate gamers around the world. To this day, while a handful of LulzSec members have been prosecuted for hacking, including against Sony Pictures, no one has been either indicted or prosecuted for the PlayStation Network outage.[4]

With constant news coverage detailing their 50-day spree, hackers and hacking groups became the public (and notorious) face of Anonymous, even if other operations were ongoing and LulzSec had, for the time being, proclaimed its independence from Anonymous. On May 13, 2011, LulzSec declared on Twitter: "Must say again: we're not AnonOps, Anonymous, a splinter group of Anonymous, or even an affiliate of Anonymous. We are #Lulzsec :D" (LulzSec, 2011). The team provoked a measure of controversy among Anons for being such a loose cannon. Although LulzSec and Anonymous shared common principles, a common culture and even some personnel, there was still enough ideological distance between the two that many Anons, along with security professionals, geeks, activists and hundreds of thousands of Twitter followers, either seemed to genuinely enjoy their antics and support them, or were at least compelled enough to watch the wild show LulzSec put on as it targeted PBS, Fox News, Sony Pictures and EVE Online, along with dozens more.

This small crew of hackers, embroiled in their own dramas, eventually retired on June 25, 2011, but many of the same individuals subsequently banded under "Operation Antisec." Unlike LulzSec, Antisec loudly and proudly branded itself as an Anonymous operation. While not forsaking deviant humour (which had been a core feature of LulzSec's public persona), Antisec adopted a more militant tone. This was largely attributable to two hackers: Jeremy Hammond, a political radical who is currently in jail awaiting sentencing, and Hector Xavier Monsegur, known as "Sabu," who worked with Anonymous, LulzSec and Antisec. Soon after being arrested on June 7, 2011, Sabu also cooperated with law enforcement as a FBI informant. Soon after, he became the public face of Antisec through his popular Twitter account, where he specialized in 140-character tirades against the group's main targets: the government, security firms, the police and corporations.

While Antisec was busy at work over the summer of 2011, several stable and distinct entities were operating simultaneously: AnonOps; Chanology; Cabin Cr3w (a small team that had formed, in part, to poke fun at Antisec, but conducted its own legal and illegal operations); a new network known as VoxAnon (which initially formed in opposition to AnonOps); as well as regional networks in Brazil, India and elsewhere. With few exceptions, media accounts of Anonymous have tended to focus on hacking, which has now become a convenient shorthand to describe Anonymous' activities; however, many of Anonymous' operations, past and present, have little to do with hacking. Anonymous' effectiveness stems, in part, from its tactical diversity. Operation BART (OpBart) provides a striking case.

4 See Charles Arthur (2013), "LulzSec: The Unanswered Questions," *The Guardian*, May 16, available at: www.guardian.co.uk/technology/2013/may/16/lulzsec-unanswered-questions.

Once again, Anonymous took action in response to an act of censorship: In August 2011, the San Francisco Bay Area Rapid Transit (BART) decided to disable mobile phone reception on station platforms in order to thwart planned protests against police brutality. Anonymous naturally publicized the well-attended street demonstrations they helped organize. A couple of individuals also hacked into BART's computers and released customer data in order to garner media attention. An illicit, semi-nude photo of BART's official spokesperson, Linton Johnson, was republished on the "bartlulz" website, with the following brazen rationalization: "If you are going to be a dick to the public, then I'm sure you don't mind showing your dick to the public" (Bartlulz, 2011).

Soon after OpBart, activity on AnonOps once again came to a halt. Its IRC network was often taken offline by a rogue hacker's DDoS attack. VoxAnon provided another home base, but it often came under attack as well, and it had yet to pull off a major operation. In the fall of 2011, many Anons turned their attention to the Occupy protests sweeping North America and Europe. Even before Occupy officially began on September 17, 2011, Anonymous had churned out many videos and images, essentially acting as an informal — but vital — public relations (PR) wing of the movement and drumming up support. Some Anons chose to encamp with the protesters, while others provided technological assistance. At the camps, individuals without any prior connection to Anonymous' Internet-based networks sported plastic Guy Fawkes masks.

In the winter of 2011-2012, Anonymous' online activity roared again. In late December, Antisec announced that it had hacked the global intelligence firm Stratfor. It initially used customers' credit cards to donate to charities — à la Robin Hood — in honour of "Lulzxmas," and eventually handed off company emails to WikiLeaks. By this time, a number of Twitter accounts, such as Your Anonymous News, AnonyOps and AnonymousIRC, had amassed hundreds of thousands of followers. The largest, Your Anonymous News, currently has over one million subscribers and roughly 25 individual contributors. This trend demonstrates that while Anonymous relies on the media to amplify its actions and amass support, it is not wholly dependent on corporate media to get word out or issue calls to action.

The Stratfor affair was followed by a flurry of widespread participatory protest activity between January and March 2012. This activity largely emanated out of AnonOps and VoxAnon, with wide support on Twitter and other forums. First, there were protests against a looming copyright bill, the Stop Online Piracy Act (SOPA), the passage of which unravelled due to a massive and elaborate outpouring of dissent. The linchpin was a "blackout day," a Web-based protest of unprecedented scale. By raising awareness about SOPA and publicizing the blackout day, Anonymous' contribution was notable. On January 17, 2012, non-profits, some prominent Web companies, public interest groups and thousands of individuals temporarily removed their websites from the Internet to voice their opposition to the bill. Thousands of citizens called or emailed their political representatives to voice their concerns.

The next day, federal authorities orchestrated the takedown of the popular file-sharing site MegaUpload. The company's controversial founder, Kim Dotcom, was arrested. Anonymous activists were outraged at the government's pre-emptive takedown of this popular website: it seemed to confirm that if bills like SOPA became law, Internet censorship would become commonplace. Although Kim Dotcom had not yet been found guilty of piracy, his property was confiscated and his website shut down.

In the wake of these events, Anonymous coordinated its largest DDoS campaign to date. This time, it did not reach out to the public at large to take part; it relied on its own (or rented) botnets. Anonymous targeted a slew of websites, including the homepages of Universal Music, the FBI, the US Copyright Office, the Recording Industry Association of America and the Motion Picture Association of America, all of which experienced downtime.

Anonymous reappeared in Europe a few weeks later, as massive on- and offline demonstrations were unfolding to protest ACTA, another international copyright law. After the Polish government agreed to ratify ACTA, Anonymous took down a slew of government websites and publicized the street protests that were sweeping Krakow. Soon after, as part of a self-conscious publicity stunt and with no connection to Anonymous groups, members of the left-leaning Palikot's Movement political party concealed their faces with paper-cut-out Guy Fawkes masks during a parliamentary session to protest ACTA. The European Union scrapped ACTA in July 2012.

According to a *Wall Street Journal* article from February 21, 2012, weeks after the flurry of protests, the US National Security Agency (NSA) labelled Anonymous an imminent threat to national security, claiming that Anonymous "could have the ability within the next year or two to bring about a limited power outage through a cyber attack" (Gorman, 2012). Subsequent news reports quoted Anonymous activists and security experts who dismissed the NSA's claims as fear mongering.[5] For all of its legal and illegal tactics, to date, Anonymous had never publicly called for such an attack, and there is no evidence to suggest that it had even considered doing so.

On March 5, 2012, one of the core Antisec hackers, Jeremy Hammond, was arrested by the FBI. The next day, Fox News broke the story that one of the most prominent Anonymous hackers, Sabu, had been working as an FBI informant subsequent to his arrest in June 2011. This confirmed the long-standing suspicion that informants had infiltrated Anonymous and that Antisec had been at least partly manipulated by government interests. Mistrust, which had always hung over the Anonymous networks, began to give way to a bleaker, ominous paranoia. Many wondered whether this would put an end to Anonymous.

Antisec's hacking activity subsided for a period of time, but in March 2012, hackers and others helped erect a new leaking platform, Par:AnoIA (Potentially Alarming Research). Hackers have expressed the need to re-shift internal security practices in order to protect individuals from ongoing government infiltration.

Anonymous-led activity picked up again over the summer of 2012 with a flurry of international ops. OpQuebec, which defaced provincial police websites, gained momentum in May 2012 after the passage of Bill 78, a law curtailing protest activity. Organized in June 2012, OpIndia rallied on the streets; activists took down a state-owned Internet service provider website for blocking file-sharing sites.

In early 2013, Anonymous hackers launched Operation Last Resort and once again initiated a string of Web defacements and hacks, this time in memory of the activist and hacker Aaron Swartz. Many believe that Swartz committed suicide due to his ongoing legal battles with the American Department of Justice and the prospect of facing decades in jail for downloading a large cache of

5 See Sam Biddle (2012), "No, Idiots, Anonymous Isn't Going to Destroy the Power Grid," February 21, available at: http://gizmodo.com/5886995/no-idiots-anonymous-isnt-going-to-destroy-the-power-grid.

academic journal articles from JSTOR, the scholarly archive.

The Logics of Anonymous

Relying on a fairly predictable script, most commentators — including journalists and academics alike — usually introduce Anonymous as an evasive and shadowy group of hackers. This description distorts sociological reality. Although Anonymous is certainly a home to hackers, a great many Anons are neither hackers nor difficult to find. If you want to talk with some participants, simply log onto one of their IRC networks.

Invented in 1989, IRC is still used by geeks and hackers to develop software and (as its name suggests) to chat. IRC is unlike other media we are familiar with today — it is entirely text-based, generally free of candy-coloured icons or cute noises and conducted with its own mix of text commands and norms of communication. By today's standards, IRC provides bare-bones functionality, but its staying power and appeal likely lies in this simplicity. Ideal for real-time communication and coordinating operations, many Anons settle onto various stable IRC networks, where they converse on public or private channels. In many regards, it functions like an online social club open 24 hours a day. This is where lulzy humour flourishes and intimate bonds of fellowship are formed. Anons aren't required to use IRC, though; some prefer to act alone, while others turn to Web forums, Twitter and/or other chat protocols. Illegal activities are orchestrated on invite only, encrypted communication channels.

Nevertheless, compared to spheres of hacker activity where contributions (and often respect) require technical skills, Anonymous is more participatory, which sustains its dynamism and flexibility. In order to be part of Anonymous, one need simply self-identify as Anonymous. No particular abilities are required. To be sure, hackers (including programmers, security researchers and system administrators) are essential to Anonymous' networks. They erect and maintain communication infrastructure, and infiltrate servers to expose weak security or in their hunt for information to leak. Given the mass media's frenzied obsession with hackers, their actions invariably nab a majority of the headlines. While hackers obviously wield more technical power and their opinions carry weight, they don't erect entrance barriers nor control the evolution of Anonymous. Individuals without technical skills can participate by collectively writing press communiqués, giving media interviews on IRC, designing propaganda posters, editing videos and mining information that is publicly available but difficult to access. To get the word out and attract new volunteers, participants have developed best practices. Back in 2010 and for much of 2011, it was common for a small dedicated team to constantly flood 4chan with propaganda material to recruit participants. Today individuals running large Anonymous Twitter accounts coordinate to spark a "Twitter storm" with established hash tags to publicize an issue in the hopes it will trend. Organizers thus emerge to advise, inspire and corral troops, and some even broker between different groups and networks; brokering is vital for the formation of inter-network ad hoc teams.

No single group or individual can dictate the use of the name or iconography of Anonymous, much less claim legal ownership of its names, icons and actions. It has now become the quintessential anti-brand brand. Naturally, this has helped Anonymous spread across the globe. Although Anonymous may at times appear to be chaotic, participants rarely choose targets randomly. Operations tend to be reactive; existing local, regional and international events and causes can trigger action from Anonymous. Leaking and exposing security vulnerabilities are two common proactive interventions.

All types of operations can usually be linked to a particular IRC network, such as AnonOps, AnonNet or Voxanon or a Twitter account dedicated to the operation, such as @OpLastResort. Although individuals on these networks generally take credit for their operations, they sometimes deny their participation. Naturally, regional issues command the attention of regional networks. To date, and with a few exceptions, regional operations have garnered scant academic or media attention; they may prove impossible to study retrospectively.

Only a handful of actions performed under the banner of Anonymous have been atypical, such as the lone anti-abortion hacker who targeted Britain's largest abortion clinic.[6] While predictions of chaos unleashed by evil or maladjusted hackers loom large in the state's anxieties about Anonymous, they remain largely unrealized. To date, no Anonymous operation has been diabolical and no existing node has ever expressed the desire to do something as rash as taking down the power grid (as the NSA once predicted). That's not to say that all of Anonymous' operations are laudable, or effective. Indeed, since the character and tactics of each Anonymous operation are distinct, blanket moral judgments are hard to make and tend to be overly simplistic. In some cases, targeted individuals and organizations have suffered some combination of harm to their reputation and finances. (From Anonymous' point of view, this is the desired outcome.) Given its unpredictability, past actions are no basis for predicting the future. Still, reckless operations meant to endanger lives have, thus far, never been part of Anonymous' moral calculus or tactical repertoire.

The majority of individual Anons never break the law; however, since Anonymous can't generally police participants, it's possible that some may. Certain factions have certainly done so (and over 100 individuals across the globe have been arrested for their alleged participation). Any vulnerability will be exploited, any advantage generally leveraged. A handful of Anons have used tactics such as doxing, that is, leaking someone's Social Security number and home address or other personal information. This tactic was used against BART's official spokesperson and against numerous police officers who pepper-sprayed Occupy protesters.

Journalists highlight these controversial acts, which invariably boosts Anonymous' profile. Unlike criminal groups who want to remain hidden, Anonymous seeks the limelight. Partly because of its maverick image and transgressive antics, Anonymous has attracted significant attention, sometimes admiration and sometimes fear. As an entity though, Anonymous is often slippery, evasive and invisible. Its organizing principle — anonymity (or technically pseudonymity) — makes it difficult to tell how many people are involved overall. Although core participants exist and chat channels are dedicated to reporters, Anonymous has a shifting cast of characters. Some individuals routinely change their online nicknames. If a participant leaves for a few months, catching up can prove frustrating and certainly time consuming, even more so for an observer.

Misinformation about Anonymous abounds. Some of it is self-sown, but some has been foisted upon the movement. Journalists, even those reporting for reputable news outlets, have at times incorrectly cast

6 See Ben Quinn (2012), "Anti-abortion activism escalating, warns clinic targeted by vigil," March 13, *The Guardian*, available at: www.guardian.co.uk/world/2012/mar/13/anti-abortion-activism-clinic-vigil.

DDoS campaigns as a subspecies of hacking.[7] In fact, the servers that bear the brunt of DDoS attacks are not hacked into and do not suffer any permanent damage or data loss. A successful DDoS blocks access to an Internet domain (often a very large one), but it does not affect an organization's internal computer system. If companies follow basic security best practices, their financial payment processing, trading networks and other core infrastructure won't be sitting wide open on the Internet, vulnerable to an attack. DDoS tactics are political stunts. The sites that are the most vulnerable to these attacks tend to be symbols of important infrastructure, not the infrastructure itself.

To disguise itself further, Anonymous also seeds false information, thereby pulling the wool over the eyes of the media, and even confounding participants. As one organizer put it, "so much of Anon[ymous] relies on smoke and mirror tactics." For example, an Anonymous-based group may take credit for a hack, actually given to them by some other hacker or team; Anonymous relies on botnets to knock a website offline, but it won't advertise this in its press releases. It can be hard, at times, to distinguish fib from fact, truth from lies. This obfuscation adds to Anonymous' mystique and, thus, to its power.

WEAPONS OF THE GEEK

While certainly unique in its bombast and capriciousness, Anonymous is part of a wellspring of hackers and geeks taking political matters into their own hands to make their voices heard, to orchestrate protests over a range of issues, in particular civil liberties, and to transform policy and law. Anonymous signals the growing importance of what I call "weapons of the geek," in contrast to "weapons of the weak" — the term anthropologist James Scott (1985) uses to capture the unique, clandestine nature of peasant politics. While weapons of the weak is a modality of politics among disenfranchised, economically marginalized populations who engage in small-scale illicit acts — such as foot dragging and minor acts of sabotage — that don't appear on the surface to be political, weapons of the geek is a modality of politics exercised by a class of privileged and visible actors who often lie at the centre of economic life. Among geeks and hackers, political activities are rooted in concrete experiences of their craft — administering a server or editing videos — skills channelled toward bolstering civil liberties, such as privacy. Unlike peasants, who seek to remain inconspicuous and anonymous, geeks and hackers, even Anonymous, indisputably call attention to themselves via their volatile, usually controversial, legal and transgressive political acts. They are testing new possibilities and legal limits for digital civil disobedience.

Hackers and geeks, diverse in skills, political sensibilities and national backgrounds, are naturally intervening in equally diverse ways. For instance, hackers have crafted a legal mechanism to side-step traditional copyright regulations: copyleft, a class of licenses that can be applied to software to render it open source. Since the early 1990s, hackers have coded and used privacy and encryption tools such as Pretty Good Privacy and Tor (originally short for The Onion Router) to provide technical protection from state and corporate snooping. Dozens of other examples of geeks engaging in diverse genres of collective action come to mind, from the chartering of new political parties such as the Pirate Party in Europe, to the astonishing proliferation of informal

7 For example, in March 2013, an article in the *Los Angeles Times* issued a correction after incorrectly stating in a post that an indictment charged Anonymous with what amounted to hacking. See Matt Pearce (2013), "Wisconsin man indicted in Anonymous attack of Koch Industries," *Los Angeles Times*, March 27 Available at: http://articles.latimes.com/2013/mar/27/nation/la-na-nn-anonymous-koch-hack-20130327. The correction appears near the end of the article.

workshops, such as hacker labs and spaces, around the world, to the rise of policy geeks educating politicians and staff technologists advising lawyers in advocacy groups.

Hackers and technologists have also been at the forefront of the dramatic resurgence of whistle-blowing. These activities are, in part, the result of the efforts of Julian Assange, who chartered WikiLeaks in 2006, and US solider Chelsea Manning (formerly Bradley Manning),[8] who provided WikiLeaks with its most explosive material. Anonymous would eventually take the baton of leaking by targeting security firms and governments. To date, the most significant leak has come from Edward Snowden, an ex-NSA employee and system administrator. In June 2013, he confirmed what Anonymous, privacy activists and journalists have been claiming for years: the NSA not only has vast capabilities to intercept, store and analyze the digital traces and footprints of citizens and foreigners alike, but in so doing has broken numerous laws and lied to Congress.

Within this diverse and expanding ecology of hacker-based activity — one might even view it as an emerging digital environmentalism — Anonymous specializes in acts of disobedience, defiance and protest. It is adept at magnifying issues, boosting existing (and usually oppositional) movements and converting amorphous discontent into a tangible form. Individuals who live at great distances from each other, without hefty financial resources, band together under recognizable names and symbols to direct attention on and thus judge — often quite swiftly — the actions of individuals, corporations and governments. To do so, they often exploit a feature of our collective digital predicament: corporations and governments have collected and stored a vast sea of digital data, often insecurely on unencrypted servers, which can at times be legally accessed, and in other cases illegally procured, but once leaked, is nearly impossible to contain and sequester.[9]

Since Anonymous' forte is publicity, it can create a PR nightmare for its targets. This reflects an important aspect of the contemporary media and information environment: the reputations of institutions or individuals are now more vulnerable to credible critiques and leaks, as well as false smear campaigns. Even if information is not featured on the evening news, it may still spread like wildfire if enough individuals circulate it on social media.

Still, Anonymous stands apart for the unparalleled degree to which it injects suspense, drama and intrigue into existing or self-generated events. Sometimes it merely pens a manifesto, other times it ignites a large-scale protest. Each intervention is distinct, but all benefit from Anonymous' formidable PR machine. The machine churns out homemade videos, manifestos and images via Twitter, IRC channels or Web forums, usually generating some degree of spectacle. In a more general register, its iconography — Guy Fawkes masks and headless suited men — symbolically and spectacularly asserts the idea of anonymity, which they embody in deed and words. Anonymous' particular elixir of spectacle is especially nourished by its aforementioned unpredictability and mystery: Who exactly are the men and women behind the mask? What will they do next? How will police react to their calls for justice and their threats to release the names of alleged perpetrators? It thus works to air and

8 On August 22, 2013, Chelsea Manning announced that she considers herself a woman and had changed her name.

9 See "35% of Companies Worldwide Don't Use Encryption to Safeguard Business Data" (2013), Kaspersky Lab, March 14, available at: www.kaspersky.com/about/news/virus/2013/35_of_companies_worldwide_dont_use_encryption_to_safeguard_business_data.

dramatize a panoply of issues that might otherwise have remained hidden, elusive or underreported.

Anonymous, already infamous, is hard to sully further, especially due to its relatively minimal funding requirements. Unlike WikiLeaks, Anonymous has no salaries to dole out or rent to pay. Costs are largely confined to hosting IRC servers and renting botnets. As a result, Anonymous, as an entity, has little to lose and, combined with no allegiance to a master plan or set of goals, this affords them tremendous experimental freedom in thought and action.

Even if shielded from shocking or degrading information about its participants or operations, charges of terrorism or overly deviant and reckless behaviour have, on occasion, been levelled against the group by government officials and journalists. These attempts to discredit Anonymous have neither stuck as a dominant narrative, nor become prevalent, likely because they strike as hyperbolic because these activists have not engaged in violent terroristic behaviours.

The bottomless appetite the press has for sensationalism has made Anonymous' notoriety an ideal subject for coverage. Fuelling the fire of media hype, as Anonymous often does, may be celebrated, denounced or (fatalistically) accepted, depending on one's views about the hotly debated nature of journalism. Should the media strive for cool and contained objectivity? Or for a public that is already accustomed to some degree of entertainment with its news, might an element of fantasy, intrigue, humour and gravitas captivate more attention? Whatever one's opinion, Anonymous has become a central fixture in the media because it aligns so well with the prevailing journalistic culture of sensationalism.

One might justifiably ask if Anonymous' provocations and publicity, whether self-generated or delivered via the media, can lead to large-scale structural change or policy reform. While many of Anonymous' operations solely generate publicity, many others have focussed on yielding other outcomes, although often coupled with a savvy media strategy of engagement. For example, during the Arab Spring, Anonymous provided technological assistance to activists on the ground; many of its leaks have given a rare glimpse into the inner workings of private security companies seeking to land coveted government contracts for surveillance or propaganda. Anonymous has exposed grave human rights abuses, for example, in Burma with OpRohingya, and has instigated numerous street demonstrations. However, Anonymous is ill-equipped for self-directed policy reform or targeted engagement with Internet governance. If participants were to unmask, "clean up" their act and come out to state or national capitals to pitch their causes, they would no longer be recognizable as Anonymous.

Nevertheless, Anonymous was so notable in the anti-SOPA demonstrations that I received a call from a famous venture capitalist involved with organizing these protests. He wanted to learn whether its participants could be harnessed a little more directly, for the purposes of rallying around Internet reform. The beauty and frustration of Anonymous lies in its unruly and unpredictable spontaneity — as its members like to boast, with a commonly stated refrain, "We are not your personal army." This inability to harness Anonymous directly prevents their assimilation and neutralization by established institutional actors. But the venture capitalist's intuition — that Anonymous is an important part of the mix — was correct. Some Internet advocacy employees have also told me they cannot publicly support nor work with Anonymous, but are cheering them on from the sidelines (many hackers are less than enthused, seeing Anonymous as too juvenile or irrational for their taste). A number of Anons have also had numerous behind the scenes discussions with more traditional activists and advocates over

Internet governance and other policy issues. There are, nevertheless, limits to Anonymous' ability to intervene in policy reform and it is best viewed as a multifaceted protest ensemble.

Still, the broader effectiveness and success of Anonymous is contingent on the vibrancy and diversity of its wider political milieu. Anonymous is a niche in a broader ecosystem of geek- and hacker-oriented activism, which includes policy reform, participation in Internet governance and whistle-blowing. Social change requires a diverse tool kit, including fine-tuned interventions targeting policy to rowdy and subversive tactics. In the fight for digital rights and civil liberties online, Anonymous exists alongside, although not directly working with, advocacy organizations such as the Electronic Frontier Foundation (EFF).

Distinct modalities need not compete or be mutually exclusive; they can and do cross-pollinate to form a broad-based, internally diverse movement. A functioning democracy requires investigative journalists who spend years piecing difficult puzzles together, advocacy groups with lawyers and policy specialists who strategize for legal reform, whistle-blowers who take on individual risk and protest movements open to the citizenry at large.

Some predict that Anonymous' wily, irreverent and at times illegal tactics (such as DDoS campaigns and hacking) may lead governments to restrict the civil liberties that Anons have so passionately been clamouring to protect. Government officials and law enforcement may be quick to paint Anonymous as imaginary goblins to paraphrase the American journalist H. L. Mencken (2008) who famously quipped "the whole aim of practical politics is to keep the populace alarmed (and hence clamorous to be led to safety) by menacing it with an endless series of hobgoblins, most of them imaginary." However, this prediction loses its legs when one contextualizes Anonymous historically. Long before Anonymous rose to prominence, national governments around the world aspired to control the Internet, and implemented statutes eroding civil liberties. Indeed, state secrecy and surveillance are so well entrenched that even if Anonymous were to vanish tomorrow, or if it had never existed in the first place, it is unlikely the expansion of the surveillance state and the post-9/11 curtailment of civil liberties in the United States would be deterred. Although Anonymous' actions will likely be used to justify further restrictions on liberty, Anonymous should be seen as a reaction to these trends, not simplified as a primary cause.

In the face of trends like increasing state surveillance and secrecy, silence and inaction from the public might actually be more dangerous than any legislation justified in the name of Anonymous' actions. Anonymous counters political disengagement and passivity, acting as a gateway for some individuals to engage in direct action. Spectators can join in, follow along and get their daily dose of news. Organizations like the EFF have a narrowly defined set of opportunities for participation: financial support, reading and circulating weekly email alerts, political campaign advocacy and attending yearly benefit events. Anonymous, on the other hand, provides individuals with avenues for personal and collective participation. While Anonymous might not appeal to everyone — no political movement ever can or will — it functions as a wide-open platform for discrete microprotests. Participants need not fill out forms, make donations, or in this case, even provide their legal names. By participating, individuals become a part of something larger than themselves. They acquire diverse skills. Some will likely dedicate years of their lives to activism.

Anonymous has awoken and cultivated political sensibilities for some citizens. Dissent of the sort Anonymous specializes in allows citizens to exercise

their rights and demonstrate on behalf of the causes they embrace. This lesson was reinforced through a recent conversation with one young European participant, a talented and prolific video editor. In February 2013, he revealed how fundamentally he had been transformed by Anonymous:

> Well Anonymous changed a fkg lot in my life, it changed 99 [percent] of my life…before Anonymous, I was a regular student at school, doing stuff like playing pc games. I viewed the USA as a dream land, especially because Obama pulled back soldiers from Afghanistan...My dream was to become a architect or policemen, a doctor. But ever since I got involved in Anonymous, and accessed different types of information from reading twitter news, I saw how governments "saw" justice, I started to see things from another perspective. Everyday I see the value of free speech. I work with people I didn't even know and work with them for people who can't always speak for themselves.

Early in May 2013, this Anon completed a video for Operation Guantanamo. Opening with a montage of news clips featuring President Obama's repeated promises to close down the prison on Guantanamo Bay, the video highlights the hypocrisy of a president who ran a campaign on a promise that he has thus far failed to keep. This young Anon has already made over 90 videos for Anonymous. In May 2013, he finished high school.

CONCLUSION

In 1996, a group of RAND researchers published a seminal book on netwar. They defined it as "an emerging mode of conflict (and crime)" in which actors rely on small teams and flexible networked organizational forms lacking a "precise central command" or a rigid hierarchy (Arquilla and Ronfeld, 1996). Although netwar is often identified with criminal activity or digital networked politics, the RAND authors emphasized its diversity. Netwar can emerge online or offline. It can be initiated for criminal, religious, ethnic or civil society purposes. Many of the authors' insights still ring true today. However, several examples heralded as flexible, ad hoc, peer-to-peer and non-institutional formations, from MoveOn.org to open source production, are now fairly stable formations with fleshed-out strategies and doctrines; over time, they routinized and became institutions in their own right.

Anonymous, on the other hand, has steadfastly resisted routinization. With its flexibility, dynamism and ad hoc autonomous groups, Anonymous may epitomize netwar even to the extent that protagonists celebrate and theorize its core features. Still, it is worth noting that a few of Anonymous' tactics, notably hacking and DDoS campaigns, rely on a logic of command and control. For instance, although an Anonymous DDoS attack may be widely participatory and its target may be chosen by consensus, the majority of the actual network traffic required to perform the attack is controlled by a smaller group. These elite participants must possess the technical skills to wield botnets. This reveals an element of a more traditional top-down hierarchy. In fact, a private channel on one of Anonymous' biggest IRC networks, where targets were chosen and hacks discussed in secret, was actually called "#command." Nevertheless, the simultaneous existence of different types of operations as well as multiple backroom cabals, some at war with each other, many experiencing internal feuds, prevents a calcified and stable seat of concentrated power from forming.

Networked and flexible forms of online activism and dissent like Anonymous have arisen in lockstep with the vast collection of information and software that can algorithmically harvest data for real-time surveillance and behaviour prediction. With a great degree of accuracy and sophistication, this data can forecast consumer preferences, map social relationships, predict sexual orientation based on one's friends online and potentially even warn military or commercial institutions that a staff member is "likely" to become a whistle-blower and leak sensitive information to the public.[10]

Anonymous is all the more interesting for its ability to escape the orbit of big data analysis, inquiry often marshalled for the purpose of anticipating behaviour patterns. Even basic sociological treatment of Anonymous is difficult, although not impossible. This elusive entity is devilishly hard to track and predict. Significant time and resources are required simply to follow the arc of a single Anonymous operation, let alone the social life and history of an IRC network such as AnonOps. Its symbolism is pervasive, yet much of Anonymous remains opaque and undecipherable — an increasingly rare state of existence today; thus, it acts as a vital counterweight to the state of surveillance.

The inability to divine its future, much less form a consistent and comprehensive account of Anonymous at present, is most likely what is so unsettling and threatening to governments and corporations alike. Nevertheless, law enforcement has poured significant resources into finding and apprehending hacker suspects. In the United States, two LulzSec hackers have been sentenced. Antisec hacker Jeremy Hammond plead guilty in September 2013 to nine acts of hacking, including the Stratfor hack, and is awaiting sentencing. In the United Kingdom, four individuals involved with Anonymous were sentenced in May 2013 and received punishments ranging from community service to 20 to 32 months in jail. Earlier in January 2013, two men in the United Kingdom were sentenced to jail, one for seven months, the other for 18 months for their role in the DDoS campaign against PayPal. In Ireland, two young men pleaded guilty to defacing a website of the Fine Gael, an Irish political party, for which the judge noted the only harm was embarrassment. She fined them 5,000 euros each and has ordered them to complete a restorative justice program and to return to court in October 2013.

So far, judges on both sides of the Atlantic have treated these activities as purely criminal, unwilling to entertain the idea that the actions may have be principled dissent. One key difference between sentencing in Europe and the United States is that in the United States, punishments are usually accompanied by astronomical fines. Both LulzSec hackers in the United States were fined over US$600,000, while no one in the United Kingdom was fined and in Ireland the largest fine has, thus far, not exceeded 5,000 euros.

Due to its lack of transparency, labyrinthine sociology and bountiful secrecy, Anonymous may not be the best model for democracy; in a few instances, operations creep uncomfortably close to vigilantism. It has, however, also revealed current impasses and limits to democracy, the sort of critique offered by Anonymous is an essential feature of the democratic process. While Anonymous has not proposed a programmatic plan to topple institutions or change unjust laws, it has made evading laws and institutions seem desirable. It has enabled action at a time when many feel that existing channels for

10 See Ryan Gallagher (2013), "Software that Tracks People on Social Media Created by Defence Firm," *The Guardian*, February 10. available at: www.guardian.co.uk/world/2013/feb/10/software-tracks-social-media-defence.

change are either beyond their reach or too corrupt. One core organizer captured this sentiment after I asked him why he joined the more militant wing of Anonymous, Anonops: "I was sold on the raids [DdoS, black faxes, etc.] because I'd been an activist for years before I got involved in Anon, like about four-five years, and I'd just experienced that once vested interests have made a government decision, lobbying by ordinary people won't get it changed back without scaring them a little."By unpredictably fusing conventional activism with transgression and tricksterism, Anonymous has captured the attention of a diverse cornucopia of admirers and skeptics. Many are watching, recognizing the power of the mask as a potential force to unmask corruption, hypocrisy, and state and corporate secrecy.

WORKS CITED

Anonymous (2007). "Dear Fox News." YouTube video. Available at: www.youtube.com/watch?v=RFjU8bZR19A.

——— (2008). "Message to Scientology." YouTube video, January 21. Available at: www.youtube.com/watch?v=JCbKv9yiLiQ.

Arquilla, John and David Ronfeld (1996). *The Advent of Netwar*. RAND Corporation.

Bartlulz (2011). "Linton Johnson — The Face of BART." August 24.

Cheng, Jacqui (2010). "Anonymous Targets Australian Government Over Porn Filters." *Arts Technica*. February 10. Available at: http://arstechnica.com/tech-policy/2010/02/anonymous-targets-australian-government-over-porn-filters/.

Christman, Tory (2012). "Tory Christman ex Scientologist and Declared SP Shares Her Experiences @ Dublin Offline." YouTube video, August 15. Available at: www.youtube.com/watch.

Fox News (2009). "4Chan: The Rude, Raunchy Underbelly of the Internet," April 8. Available at: www.foxnews.com/story/0,2933,512957,00.html.

Gorman, Siobhan (2012). "Alert on Hacker Power Play," *The Wall Street Journal*, February 21. Available at: http://online.wsj.com/article/SB10001424052970204059804577229390105521090.html.?v=SZzQUV6JUr0&list=PLC311FA5229AC4B73&index=9.

LulzSec (2011). Available at: https://twitter.com/LulzSec/status/69051330660007936.

Mencken, H. L. (2008). *In Defense of Women*. Rockville, MD: Arc Manor. First published 1918 by Philip Goodman.

Ragan, Steve (2011). *Report: HBGary Used as an Object Lesson by Anonymous*. February 7. Available at: www.thetechherald.com/articles/Report-HBGary-used-as-an-object-lesson-by-Anonymous/12723/.

Scott, James (1985). *Weapons of the Weak: Everyday forms of Peasant Resistance*. New Haven: Yale University Press.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on four themes: the global economy; global security; the environment and energy; and global development.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

CIGI MASTHEAD

57 Erb Street West
Waterloo, Ontario N2L 6C2, Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org