

LIMN NUMBER EIGHT HACKS, LEAKS, AND BREACHES

Edited by E. Gabriella Coleman and Christopher Kelty



- 2 Preface**
- 6 Hacktoids**
- 9 The spy who pwned me** by Matt Jones
- 18 The public interest hack** by Gabriella Coleman
- 24 The political meaning of hacktivism** by Ashley Gorham
- 28 Survival of the cryptic** by Sarah Myers West
- 33 Interview with Mustafa Al-Bassam**
- 36 Hacking/Journalism** by Philip Di Salvo
- 39 Refuse and resist** by Joan Donovan
- 44 Half-lives of hackers and the shelf life of hacks** by Luca Follis and Adam Fish
- 50 The illicit aura of information** by Molly Sauter
- 57 The logic of leaks** by Naomi Colvin
- 64 Interview with Lorenzo Franceschi-Bicchierai**
- 68 Can you secure an iron cage?** by Nils Gilman, Jesse Goldhammer, and Steven Weber
- 75 Power down** by David Murakami Wood and Michael Carter
- 81 When GhostSec goes hunting** by Robert Tynes
- 86 The paradoxical authority of the Certified Ethical Hacker** by Rebecca Slayton
- 90 On reusable pasts and worn-out futures** by Sara Tocchetti
- 96 Utopian hacks** by Götz Bachmann
- 102 I am not a hacker** by Paula Bialski
- 107 Interview with Kim Zetter**
- 111 The extortion stack** by Finn Brunton
- 116 Hacker madness** by Tor Ekeland
- 120 Who's hacking whom?** by Renée Ridgway
- 127 What is to be hacked?** by Claudio ("nex") Guarnieri
- 131 Car wars** by Cory Doctorow.

Preface

ISSUE 08 | HACKS, LEAKS, AND BREACHES

WAY BACK IN SEPTEMBER 2016, DURING THAT PERIOD when the media was reporting on Cozy Bear and Fancy Bear and Guccifer 2.0, security researcher Dino Dai Zovi posted this exemplary tweet:



As Dai Zovi's tweet suggests, "hacker" clearly means many different things—from adolescent boys to criminals on the "Dark Web" to nation-state spies. And one might add: from makers of Free Software to certified information security researchers to cool television characters like Eliot Alderson, to wardens of privacy and promoters of encryption to those helping secure the work of journalists and dissidents. All these and more are hackers. Some are hacking, some are leaking, some are breaching—and it does not always mean just the same thing. What used to be an "underground" subculture, is now part of a new regime of offensive and defensive state action, a robust domain of criminal exploration, and the site of ever more powerful political activism.

In 2017, it is nearly impossible to open a newspaper and not stumble upon something about hacks, leaks, or breaches. Everyday some new angle of a seemingly endless story about alleged Russian hacking of the US Presidential election assaults us; every day, there are computers hacked, frozen by ransomware, or phished by criminals and state actors alike; every day, there are breaches of massive numbers of records, from email address and passwords to the complete dossiers of every federal employee to the medical records of innocent patients. Some of these events seem to be state-sponsored, some seem to be criminal actions, and others are related to activism of some kind.

So, *has* hacking jumped the shark? For this issue of *Limn*, we asked contributors to help us puzzle out the different meanings and implications of hacks, leaks, and breaches. In particular,

we wanted to know: *what's changed?* Not just technically or legally, but in a more general *political* sense. Why are hackers and hacking—despite existing in different forms for close to 50 years—suddenly something that is being taken seriously at every level? Are leaks changing in relation to hacking—and when did this happen? Are breaches a form of espionage, or kind of crime, or a new form of warfare?

The answers here take many forms, and the issue can be read in a number of different ways (we offer the reader below some of the many different "phases" this issue takes). Perhaps most obvious is that with the dramatic increase in online activity over the last decade, new forms of vulnerability and insecurity have become ever-more apparent. There are clear links to previous work that *Limn* has undertaken (e.g. with our issues on "Systemic Risk", "Ebola's Ecologies" and "Public Infrastructures/Infrastructural Publics") concerning the increasing interdependence of technical infrastructures and the new forms of governance, resistance, and insecurity this state of affairs has brought about.

But this is much more than just a technological change, it is also cultural and political. The rise of hacktivism, especially in its chief avatar of Anonymous, has changed the meaning of hacking and leaking. As Coleman points out in her piece ("the public interest hack" on page 18), the idea of a "public interest hack" by which a hack results in a politically effective leak of important information is a novel combination—innovated in large part by Anonymous groups like LulzSec—that goes part of the way towards explaining why the DNC email *leaks* have been routinely referred to as *hacks* of the US election.

Similarly, while the revelations of Edward Snowden came as a shock to many in 2012, the "Golden Age of SIGINT"—as Matt Jones calls it (9)—was taking place from the 1990s onwards, as military and intelligence officials debated the fine points of "enabling" and "affecting" (terms hackers might replace with "rooting" or "owning") vast numbers of devices around the world. Cases like the Office of Personnel Management *breach*, detailed in this issue by Gilman, Goldhammer and Weber (68), are referred to as "honourable espionage work" (attributed to the Chinese),



while something like the May 2017 WannaCry Ransomware attack is labelled “criminal” even though it relied on the hoarding of tools and exploits by spy agencies who used them for purposes we may never discover.

For a long time now, those of us who study hacking and hackers have been arguing for more precision and better terminology—there are “genres” of hackers (Coleman and Golub 2008) as well as different historical periods, regional differences, specific and precise changes to the laws and technologies at stake, and larger political changes that implicate some hackers and not others. Hackers are frequently misunderstood precisely because we lack this precision in our public discourse and debate. But they aren’t only misunderstood—sometimes the shifting meanings are a sign of significant technical and political change.

When media and public attention (and that of “hackers” as well) waxes and wanes; or when the meaning of hacking shifts to a different register, to a different definition, or to a different and distinct set of actors, it is a good sign that other elements of contemporary politics and culture are also changing. The shifting meaning of hacking, leaking and breaching seems to follow patterns, not unlike the phases of the moon: when the moon is waxing or waning different parts of it are visible. There is the dark side that we can never see, but then there are the parts that are lit up when it is full, or crescent, or gibbous. Definitions of hackers are kind of like these phases: in some periods the light is shining on the criminals and the spammers; in others, on the Free Software hackers, and in yet others on hacktivists like Anonymous. These groups never disappear completely, but they do slip into an obscurity generated by a lack of (or shift in) public discourse and interest or a momentary ebbing of certain kinds of activity (Kelty 2017).

But like the moon itself, the existence of hackers and the complex tools, techniques and infrastructure, doesn’t often change substantially. Hacking exists: whether it is referred to as leaking or breaching; whether it involves state actors, criminals or anarchist activists; whether it seems to disrupt an election, protest a corporation or government, or steal funds; whether it is about making software in a different way, or breaking it in a new way, hacking is a here to stay, whether we

want it or not, and we learn more about it, the more carefully we look at and study it. We have much to learn about how hackers and hacking operate—whether that refers to the actions of state actors, hacktivists, free software developers, hacker-entrepreneurs, hack-driven leakers and journalists, criminal extorters of bitcoin, or information security researchers in search of a safer internet. We ought to peer at hacking more closely, and with a lot more care. With any luck, this issue of *LIMN* is a telescope for those interested in seeing what hacking looks like up close, in all its phases.

PHASE 1: HACKERS, WTF ARE THEY?

Just what is a hacker? Who calls themselves hackers, and who rejects the label? The articles by Sara Tocchi (90), Goetz Bachmann (96), Ashley Gorham (24), Paula Bialski (103), Sarah Myers West (28), Rebecca Slayton (86), Tor Ekeland (116) and Robert Tynes (81) all present different faces of hackers. There are the 1990s “cyberpunks” who form the background to any contemporary understanding of the importance of cryptography today; there are “biohackers” of synthetic biology who borrow explicitly but mostly unimaginatively from the history of computer hacking; there are “corporate hackers” who disavow the label but engage in recognizable acts of hacking; there different types of hacktivists whose distinct ethical orientations around truth and opinion are brought to bear through classical political philosophy; there are “certified ethical hackers” who take courses and tests in order to gain employment and status; there are rogue hackers engaged in global activist struggles against ISIS; and there are “radical engineers” who hack not just things, but possibly our imagination of what things there could be. There will never be just one definition of “hacker”—but there are definitely better and worse ways to understand what a hacker can and cannot be, and these pieces chart that space of possibility.

PHASE 2: LEAKS AND THEIR (DIS)CONTENTS

2016 was the year the leak changed. Gone is the revered past of Pentagon Papers and inside sources, this was the year that leaking went bananas. From the Panama Papers to the DNC leaks,

more private email entered public discourse in 2016 than ever before—and more of it entered the public domain suddenly—and totally unfiltered—than ever before. One reason the leak has been in the news is that the news depends on leaks—and when they change form, or cross a threshold it is not just hackers who notice, but journalists as well, as Philip Di Salvo recounts (36). Finn Brunton (111) reminds us that the idea of the leak as a powerful force in and of itself was captured long ago in a 1975 story (popular with hackers) by John Brunner called *The Shockwave Rider*—and he uses that idea to explore the Ashley Madison hack of 2015. That case combines elements of the hack—a defaced website and a threat, with a breach (stolen private information), with the political leak (who was using the affair-brokering service?) and finally, with criminal extortion (users were required to pay to “scrub” their names from the database).

After the DNC leaks of 2016, it also became clear that leaking gigabytes of unfiltered emails represented a new category of political problem. Adam Fish and Luca Follis (44) explore the speed of new and old leaks and ask whether their temporality matters to their effects. Molly Sauter (51) asks a similar question about the illicit aura of hacked material, and whether it matters if it is processed by journalists, or dumped on us willy-nilly. And Naomi Colvin (57) generously responded to both of these pieces by urging us not to lose sight of the political effectiveness of leaks, even if they seem to have become messier and more uncontrollable. Into this debate, Joan Donovan lobs some trash: what is it (legally and technically) that differentiates dumpster diving from finding or leaking online information?

More than anything, however, the question of how hacking and leaking are related has been thrown into relief here. Gabriella Coleman (18) gives us a sharp attempt to define what’s changed about hacking—leaking today; she explores the legacy of Anonymous’ in the history of what she dubs “the public interest hack” and how we might understand it as a significant and unique disturbance in our political atmosphere.

PHASE 3: THE CYBER: STATES, FEDS, ESPIONAGE AND WAR

If there is a good indication of hacking “jumping the

shark” it may well be the resurgence of “cyber”-prefixed words: cyberspace, cyberwar, cybercrime, cybersecurity. Not since the 1990s has “the cyber” seen so much grammatically-challenged love. It is also a very good sign that we are paying attention anew to a brand of statecraft that, like many things transformed by becoming-digital, is now clearly here to stay. Matt Jones article provides perhaps the best characterization of how the line between espionage and warfare is blurring and how the practices of the NSA and the technology of hacking disturb the laws of war and the fourth amendment. Nils Gilman, Jesse Goldhammer and Steven Weber (68) take a close look at the 2015 Office of Public Management Hack—widely reported to be Chinese Espionage—and diagnose it as also a problem enabled by bureaucratic government systems. David Murakami Wood and Michael Carter (75) explore the claims about “infrastructure hacking” and distinguish extreme cases like the StuxNet virus from the now ubiquitous problems with “Internet of Things” devices all around us. Kim Zetter, author of the best book on StuxNet, also reflects here on the status of “hybrid attacks” and the ability to combine general and specific forms of expertise (107). Not to be outdone, the FBI is also involved in hacking—and not just in breaking open iPhones: Renee Ridgway (120) recounts the story of the FBI’s alleged subpoena-hacking in a case related to Tor, the Silk Road, and anonymity online.

PHASE 4: KNOW, DON’T REPEAT: SOME HISTORIES OF HACKING

Because hackers re-enter the public eye regularly, and because they are crafty, wily, hidden, shadowy— it is all too easy to forget what they have been in the past, and how we got to where we are today. Technology that seems new sometimes turns out to be very old, like the phone and the dumpster—as Joan Donovan (39) reminds us—and sometimes it is the practice of hacking that matters, not the technology. Hackers pride themselves on not being suits—but this doesn’t mean they don’t want to be legitimate. Rebecca Slayton’s (86) history of the seemingly paradoxical idea of a “certified ethical hacker” shows us how information security researchers are tangled up with hackers, military and espionage units around the world— but at the end of the day, they still need resumes to get hired.

Goetz Bachmann (96) returns to some of the most sagely of the early hackers (Douglas Engelbart and Alan Kay) in an attempt to make sense of what “radical engineers” are doing today. Sarah Myers West (28) reminds us of just how long the question of encryption of email and data has been obsessing hackers in her brief history of the Cypherpunks; and Matt Jones (9) gives us an unprecedented look into the 25 year-long development of “computer network exploitation” and the blankspeak of security agencies like the NSA who speak of “enabling” and “affecting” computers at scale around the world. Coleman (18) asks us to look past the obviousness (or obvious state) of hacking to leak documents to question how and when this tactic stabilized. And David Murakami Wood and Michael Carter (75) also looks to the recent past and near future in order to situate the events of today related to past infrastructure protection and hacking.

PHASE 5: INTERVIEWS, OPEN LETTERS AND SCREEDS

Finally, this issue of *Limn* includes the voices of the people most closely involved in hacks, leaks, and breaches: hackers themselves, journalists, defense lawyers. Interviews with journalists Kim Zetter (107) and Lorenzo Franschesci-Biccherai (64) give us an inside look at some of the problems facing those who communicate with and report on the actions of hackers as they try, in their own ways, to make sense of the thresholds we’ve crossed. Mustafa Al Bassam (33), aka “tflow”, was a member of the now famous LulzSec hacking crew, and has since gone on to become a security researcher and PhD student interested in cryptography and blockchains. He offers some insight here into the nature of the problems that LulzSec exploited, and the difficulty in fixing them. Of all our authors, none has been as close to both hackers and their persecutors as defense attorney Tor Ekeland (116), who offers us here a screed about the hysteria surrounding hackers, the completely oversized image of them projected by Federal prosecutors in the US, and the waste of time and money that has—so far—surrounded investigation of the wrong people. As we move further into the rabbit hole of national security and intelligence agencies’ hacking, we will no doubt

end up longing for a time when the worst thing a hacker did was to alter a few choice words on a website. Rounding out this collection of practitioners is a hopeful one: Claudio “nex” Guarnieri (127) has issued an impassioned call for hackers—especially those in the information security and research world—to join him in securing civil society against actors big and small. Whether it be dissidents hounded by repressive governments, or journalists spied upon by mercenary hacker firms, or civilians who just need to be reasonably safe from basic security flaws—nex’s project (called “Security Without Borders”) provides an historically novel place from which to rethink our duties and our responsibilities in the world we’ve made.

THE DARK SIDE: SCIENCE FICTION AND HACKER FACTS

We complete the issue with a *Harpers’ Magazine* inspired set of “Hacktoids”—curious facts about hacking that will edify and outrage. And then there is a science fiction story by renowned author Cory Doctorow (131). It’s a speculative piece about hacking autonomous cars, but not just in the way you might expect. If you read it at the end, after all these different perspectives, it might give you a chill. On the one hand you might think: *we are so fucked*. But on the other, it is only by our own commitment to understanding, speculating, revising and revisiting as scholars, writers, makers, researchers, and of course, as *hackers*, that we might be able to see—and to think—what we are doing today, if not tomorrow.

GABRIELLA COLEMAN and CHRISTOPHER M. KELTY
JUNE 2017

BIBLIOGRAPHY

- Coleman, E. Gabriella and Golub, Alex. 2008. “Hacker practice: Moral genres and the cultural articulation of liberalism.” *Anthropological Theory*, 8(3):255-277.
- Kelty, Christopher M. forthcoming. “Every Era Gets the Internet it Deserves (or, the Phases of Hacking).” In *Exotic No More: Anthropology on the Front Lines*, 2nde. Ed. Jeremy MacClancy.



HACKTOIDS (OR, THE LIMN INDEX)

Limn tapped its extensive network of underground operatives to bring you this extraordinary list of facts about hacks, leaks, and breaches.

4 Number of U.S. Presidents who were also painters.

23 Number of U.S. Presidential paintings released by hackers?¹

2 Number of U.S. Presidential nude self-portrait paintings released by hackers.²

1 Number of FBI moles urging LutzSec to hack the Icelandic parliament to provide the FBI with the perfect excuse to visit Iceland so that they could investigate WikiLeaks?³

8 or 9 Number of FBI agents kicked out of Iceland by the prime minister.⁴



A HANDFUL
Number of phone phreakers threatened with arrest in 1962.⁵

ONE Number of phone phreakers threatened with arrest in 1962 who went on to become any Ivy League professor and famous information designer.⁶

21 Number of times Sony was **pwned** in 2011.⁷



\$171m
Cost to Sony of 2011 PlayStation Hack.⁸

0 Number of people arrested for the 2011 Playstation hack.

7,000 Number of pages in Pentagon Papers leak.⁹

“more than 700,000” Number of documents in Manning/WikiLeaks leak.¹⁰





NOT ENOUGH TO WARRANT SHOOTING UP COMET PING PONG.

Number of times "spirit cooking" and "pizza" were referenced in DNC/Podesta hacks.



774 Number of Computer Fraud and Abuse Act cases filed against individuals between 2011-2016.¹³

0 Number of Computer Fraud and Abuse Act cases filed against corporations since the CFAA's inception in 1984.



FEWER THAN 10

Number of times the word HACKER was used in *The New Yorker* before 2008.

MORE THAN A THOUSAND

Number of times the word HACKER was used in *The New Yorker* after 2008.¹⁴

0

Number of poems about hacking in *The New Yorker* in 1991.

10

Number of poems about hacking in *Phrack* 36 (1991).¹⁵ Here's one of them:

```
\=====/
Hack
/=====\
```

[Sung to the tune of Stand by REM]

Hack in the place where you live
Now dial out
Think about telnet, wonder why you
have it now

Hack in the place where you work
Now dial up
Think about tymnet, wonder why you
have it
If you are real board hack with SUN
Carry a lap-top to help along

A PAD is there to move you around
If You're not careful your hands will
be bound

Hack in the place where you live
Now dial out
Think about telnet, wonder why you
have it now
Hack in the place where you work

Now dial up
Think about tymnet, wonder why you
have it

A PAD is there to move you around
If you're not careful your hands will
be bound

If accounts were trees
Trees would be falling

Listen to reason
Foley is calling

(repeat an (X) amount of times)
Now Hack!



33 million Number of phone

calls AT&T monitored to search for phreaks & fraud between 1964 and 1970.¹⁶

1.5 million Number of calls recorded for the

same purpose over the same time period.¹⁶

3

Number of times an electrical grid has been paralyzed by hackers since 1902.



PHOTO: CHRISTOPH SCHOLZ

952

Number of times an electrical grid has been paralyzed by squirrels since 1902.¹⁷



HACKTOIDS FOOTNOTES

- 1 Panganiban, Roma. N.d. "4 Presidents Who Painted for Fun and Profit" <http://mentalfloss.com/article/50089/4-presidents-who-painted-fun-and-profit>
- 2 Smoking Gun. 2013. "Audacious Hack Exposes Bush Family Pix, E-Mail," The Smoking Gun, February 7. <http://www.thesmokinggun.com/documents/bush-family-hacked-589132> See also: Read, Max. 2013. "These New George W. Bush Paintings May Herald a 'Cat Period,'" Gawker, August 27. <http://gawker.com/these-new-george-w-bush-paintings-may-herald-a-cat-pe-1209373403> There were 3 in the original leak on The Smoking Gun website, but a few weeks after Gawker published 6 new paintings, and then 12 others, and then a final 2, claiming each time they were also from Guccifer (other websites say that with all the positive attention the first 3 paintings got, it is maybe Bush himself who "leaked" the next paintings to Gawker). Including the Gawker leaks, the total number of leaked paintings would be 23. Guccifer accessed the pictures by simply breaking into Bush's daughter AOL Mail account.
- 3 Poulsen, Kevin. 2013. "WikiLeaks Volunteer Was a Paid Informant for the FBI," *Wired*. June 27. <https://www.wired.com/2013/06/wikileaks-mole/>
- 4 Carr, David and Ravi Somaiya. 2014. "Assange, Back in News, Never Left U.S. Radar." *New York Times*. June 24. <http://www.nytimes.com/2013/06/25/world/europe/wikileaks-back-in-news-never-left-us-radar.html?pagewanted=2&r=2>
- 5 Lapsley Phil. 2013. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell*. New York: Grove Press.
- 6 You Tube. 2013. "Edward Tufte on Aaron Swartz, JSTOR downloads and his own hacking," *YouTube*. January 21. https://www.youtube.com/watch?v=NSNVUt_5BkM
- 7 Security Curmudgeon. 2011. "Absolute Sownage: A concise history of recent Sony hacks," *Attrition.org*, June 4. http://attrition.org/security/rant/sony_aka_sownage.html
- 8 Tassi, Paul. 2011. "Sony Pegs PSN Attack Costs at \$170 Million, \$3.1B Total Loss for 2011," *Forbes*. May 23. <http://www.forbes.com/sites/insertcoin/2011/05/23/sony-pegs-psn-attack-costs-at-170-million/#6ebfc0b712ba>
- 9 Sheehan, Neil. 1971, "Vietnam Archive: Pentagon Study Traces 3 Decades of Growing U. S. Involvement," *The New York Times*, June 13. http://www.nytimes.com/1971/06/13/archives/vietnam-archive-pentagon-study-traces-3-decades-of-growing-u-s.html?_r=0
- 10 Lewis, Paul. 2013. "Bradley Manning given 35-year prison term for passing files to WikiLeaks," *The Guardian*. August 21. 2013, <https://www.theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence>
- 11 The Internet Archive, <https://archive.org/web/>
- 12 Debczak, Michele. n.d. "IKEA to Roll Out Hackable Furniture in 2018". *Mental Floss*. <http://mentalfloss.com/article/91702/ikea-roll-out-hackable-furniture-2018>
- 13 US Courts' Federal Judicial Caseload Statistics. <http://www.uscourts.gov/statistics-reports/analysis-reports/federal-judicial-caseload-statistics>
- 14 <http://www.newyorker.com/search>
- 15 Homey the Hacker. 1991. "Hack," *Phrack Magazine* vol. 3, no. 36 <http://phrack.org/issues/36/8.html#article>
- 16 Lapsley Phil. 2013. *Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell*. New York: Grove Press.
- 17 <http://cybersquirrel1.com/>



THE SPY WHO

HOW DID WE GET TO STATE-SPONSORED HACKING?
MATT JONES TRACES THE LEGAL AUTHORITIES AND
TECHNICAL CAPACITIES THAT HAVE TRANSFORMED THE
POWER OF THE NATION-STATE SINCE THE 1990S.

PWNED ME



U.S. INTELLIGENCE OFFICERS DISCUSS

Chinese espionage in dramatically different terms than they use in talking about the Russian interference in the U.S. presidential election of 2016. Admiral Michael Rogers, head of NSA and U.S. Cyber Command, described the Russian efforts as “a conscious effort by a nation state to attempt to achieve a specific effect” (Bocugno 2016). The former director of NSA and subsequently CIA, General Michael Hayden, argued, in contrast, that the massive Chinese breach of records at the U.S. Office of Personnel Management was “honorable espionage work” of a “legitimate intelligence target” (American Interest 2016; Gilman et.al 2017). Characterizing the Chinese infiltration as illegal hacking or warfare would challenge the legitimacy of state-sanctioned hacking for acquiring information and would upset the norms permitting every state to hack relentlessly into each other’s information systems.

The hairsplitting around state-sanctioned hacking speaks to a divide between the doctrinal understanding of intelligence professionals and the intuitions of non-professionals. Within intelligence and defense circles of the United States and its close allies, peacetime hacking into computers with the primary purpose of stealing information is understood to be radically different than using hacked computers and the information from them to cause what are banally called “effects”—from breaking hard drives or centrifuges, to contaminating the news cycles of other states, to playing havoc with electric grids. One computer or a thousand, the size of a hack doesn’t matter: scale doesn’t transform espionage into warfare. Intent is key. The Chinese effort to steal information: good old espionage, updated for the information age. The Russian manipulation of the election: information or cyber warfare.

Discussing the OPM hack, Gen. Hayden candidly acknowledged,

If I as director of CIA or NSA would have had the opportunity to grab the equivalent [employee records] in the Chinese system, I would not have thought twice... I would not have asked permission. I would have launched the Starfleet, and we would have brought those suckers home at the speed of light.¹

Under Hayden and his successors, NSA has certainly brought suckers home from computers worldwide. Honorable computer espionage has become multilateral, mundane, and pursued at vast scale.²

In February 1996 John Perry Barlow declared to the “Governments of the Industrial World,” that they “have no sovereignty where we gather”—in cyberspace (Barlow 1996). Whatever their naivety in retrospect, such claims in the 1990s from right and left, from civil libertarians as well as defense hawks, justified governments taking preemptive measures to maintain their sovereignty. Warranted or not, the fear that the Internet would weaken the state fueled its dramatic, mostly secret, expansion at the beginning of the current century. By understanding the ways state-sponsored hacking exploded from the late 1990s onward, we see more clearly the contingent interplay of legal authorities and technical capacities that created the enhanced powers of the nation-state.

How did we get a mutual acceptance of state-sanctioned hacking? In a legal briefing for new staff, NSA tells a straightforward story of the march of technology. The movement from telephonic and other communication to the mass “exploitation” of computers was “a natural transition of the foreign collection mission of SIGINT” (signals intelligence). As communications moved from telex to computers and switches, NSA pursued those same communications” (NSA OGC n.d.). Defenders of NSA and its partner agencies regularly make similar arguments:

anyone unwilling to accept the necessity of government hacking for the purposes of foreign intelligence is seen as having a dangerous and unrealistic unawareness of the threats nations face today. For many in the intelligence world today, hacking into computers and network infrastructures worldwide is, quite simply, an extension of the long-standing mission of “signals intelligence”—the collection and analysis of communications by someone other than the intended recipient.

Contrary to the seductive simplicity of the NSA slide, little was natural about the legalities around computer hacking in the 1990s. The legitimization of mass hacking into computers to collect intelligence wasn’t technologically or doctrinally pre-given, and hacking into computers didn’t—and doesn’t—easily equate to earlier forms of espionage. In the late 1990s and 2000s, information warfare capacities were being developed, and authority distributed, before military doctrine or legal analysis could solidify.³ Glimpsed even through the fog of classification, documents from the U.S. Department of Defense and intelligence agencies teem with discomfort, indecision, and inter-necine battles that testify to the uncertainty within the military and intelligence communities about the legal, ethical, and doctrinal use of these tools. More “kinetic” elements of the armed services focused on information warfare within traditional conceptions of military activity: the destruction and manipulation of the enemy command and control systems in active battle. Self-appointed modernizers demanded a far more encompassing definition that suggested the distinctiveness of information warfare and, in many cases, the radical disruption of traditional kinetic warfare.

The first known official Department of Defense definition of “Information Warfare,” promulgated in an only recently declassified 1992 document, comprised:

1 In conversation with Gerard Baker, June 15, 2015. Available at link.

2 For the current state of international consensus on cyber espionage among international lawyers, see Schmitt 2017, rule 32.

3 See Berkowitz 2003:59-65; Rattray 2003; Rid 2016:294-339 and Kaplan 2016

Authority to conduct CNE

- (S) EO 12333 assigns NSA the Signals Intelligence (SIGINT) Mission, **which includes COMINT and in turn CNE.**
- (U) CNE evolved as a natural transition of the foreign intelligence collection mission of SIGINT. As communications moved from telex to computers and switches, NSA pursued those same communications.
- (U) 2 type of CNE activities:
 - (U) Collection Activities- designed to acquire foreign intelligence information from the target computer system.
 - (S) Enabling Activities- designed to obtain or facilitate access to the target computer system for possible later CNA, or force use of alternate communication systems.

Classification TOP SECRET//COMINT//Ref 4
EYES//2029123

FIGURE 1: "Authority to Conduct CNE."
(NSA OFFICE OF GENERAL COUNSEL, N.D.8)

and dissemination of information has been a stumbling block in gaining understanding and acceptance of the concepts surrounding information warfare" (Kuehl 1997). Information warfare had to encompass collection of intelligence, deception, and propaganda, as well as more warlike activities such as deletion of data or destruction of hardware. Exploitation had to become peaceful.

Around 1996, a new doctrinal category, "Computer Network Exploitation" (CNE), emerged within the military and intelligence communities to capture the hacking of computer systems to acquire information from them.⁵ The definition encompassed the acquisition of information but went further. "Computer network exploitation" encompassed collection and enabling for future use. The military and intelligence communities produced a series of tortured definitions. A 2001 draft document offered two versions, one succinct,

Intelligence collection and enabling operations to gather data from target or adversary automated information systems (AIS) or networks.

and the other clearer about this "enabling":

Intelligence collection and enabling operations to gather data from target or adversary automated information systems or networks. CNE is composed of two types of activities: (1) enabling activities designed to obtain or facilitate access to the target computer system where the purpose includes foreign intelligence collection; and, (2) collection activities designed to acquire foreign intelligence information from the target computer system (Wolfowitz 2001:1-1).

The competition of opposing information systems to include the exploitation, corruption, or destruction of an adversary's information system through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information systems from such attacks (DODD TS 3600.1 1992:1).

Under this account, warfare included "exploitation": the acquiring of information from an adversary's computers whether practiced on or by the United (ibid.:4).⁴ A slightly later figure (Figure 2) illustrates this inclusion of espionage in information warfare.

According to an internal NSA magazine, information warfare was "one of the new buzzwords in the hallways" of the Agency by 1994 (Redacted 1994:3). Over the next decade, the military services competed with NSA and among themselves over the

definition and partitioning of information warfare activities. One critic of letting NSA control information warfare worried about "the Intelligence fox being put in charge of the Information Warfare henhouse" (Rothrock 1997:225).

Information warfare techniques were too valuable only to be used in kinetic war, a point Soviet strategists had long made. By the mid-1990s, the U.S. Department of Defense had embraced a broader doctrinal category, "Information Operations" (DODD S-3600 1996). Such operations comprised many things, including "computer network attack" (CNA) and "computer network defense" (CND) as well as older chestnuts like "psychological operations." Central to the rationale for the renaming was that information warfare-like activities did not belong solely within the purview of military agencies and they did not occur only during times of formal or even informal war. One influential strategist, Dan Kuehl, explained, "associating the word 'war' with the gathering

4 Drawn from the signals intelligence idiolect, "exploitation" means, roughly, making some qualities of a communication available for acquisition. With computers, this typically means discovering bugs in systems, or using pilfered credentials, and then building robust ways to gain control of the system or at least to exfiltrate information from it.

5 Computer Network Exploitation (CNE) was developed alongside two new doctrinal categories emerging in 1996: more aggressive "Computer Network Attack," (CNA) which uses that access to destroy information or systems, and "Computer Network Defense" (CND). For exploitation versus attack, see (Owens et. al. 2009; Lin 2010:63).

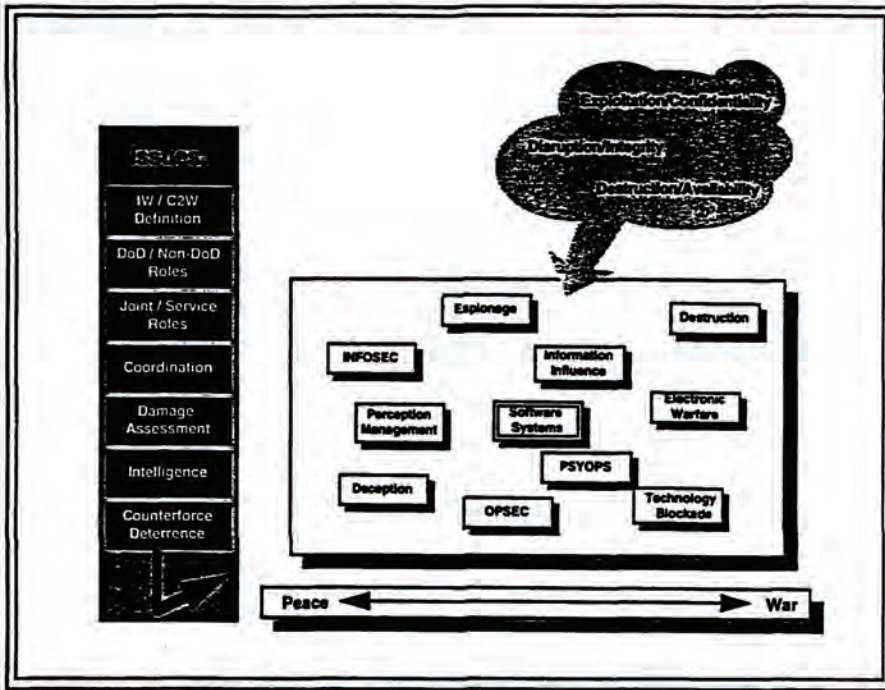


FIGURE 2: "Information Warfare."

(FIELDS AND MCCARTHY 1994: 27)

FIGURE 3 (BELOW): Information warfare is different.

(ANDREWS 1996:3-2).

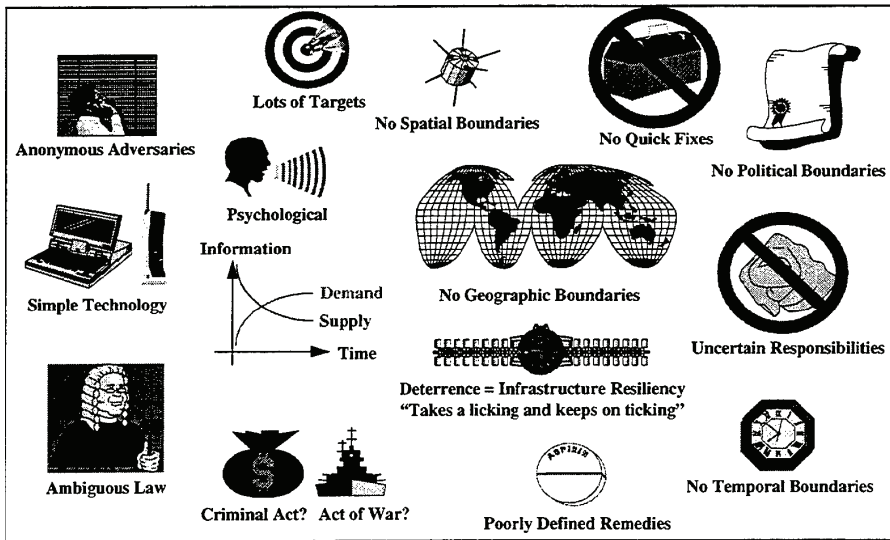
category, "enabling" was hived off from *offensive warfare*, to clarify that exploiting a machine—hacking in and stealing data—was not an attack. It was espionage, whose necessity and ubiquity everyone ought simply to accept.

The new category of CNE subdued the protean activity of hacking and put it into an older legal box—that of espionage. The process of hacking into computers for the purpose of taking information and enabling future activities during peacetime was thus grounded in pre-existing legal foundations for signals intelligence. In contrast to the flurry of new legal authorities that emerged around computer network attack, computer network exploitation was largely made to rest on the hoary authorities of older forms of signals intelligence.⁶

A preliminary DoD document captured this domestication of hacking in 1999:

The treatment of espionage under international law may help us make an educated guess as to how the international community will react to information operations activities. . . . international reaction is likely to depend on the practical consequences of the activity. If lives are lost and property is destroyed as a direct consequence, the activity may very well be treated as a use of force. If the activity results only in a breach of the perceived reliability of an information system, it seems unlikely that the world community will be much exercised. In short, information operations activities are likely to be regarded much as is espionage—not a major issue unless significant practical consequences can be demonstrated (Johnson 1999:40; emphasis added).

In justifying computer espionage, military and intelligence thinkers rested on a Westphalian order of ordinary state



Enabling operations were carefully made distinct from *affecting* a system, which takes on a war-like demeanor. Information operations involved "actions taken to affect adversary information and information systems, while defending one's own information and information systems" (CJCSI 3210.1A 1998). CNE was *related to* but was not in fact an informa-

tion "operation." A crucial 1999 document from the CIA captured the careful, nearly casuistical, excision of CNE from Information Operations: "CNE is an intelligence collection activity and while not viewed as an integral pillar of DoD IO doctrine, it is recognized as an IO-related activity that requires deconfliction with IO" (DCID 7/3 2003: 3). With this new

⁶ Especially NSCID-6 and Executive Order 12,333. The development of satellite reconnaissance had earlier challenged mid twentieth century conceptions of espionage. For a vivid sense of the difficulty of resolving these challenges, see (Falk 1962: 45-82).

relations with long standing norms. At the very moment that the novelty of state-sanctioned hacking for information was denied, however, a range of strategists and legal thinkers expounded how the novelty of information warfare would necessitate a radical alteration of the global order.

BEYOND WESTPHALIA

Mirroring Internet visionaries of left and right alike, military and defense wonks in the 1990s detailed how the Net would undermine national sovereignty. An article in RAND's journal in 1995 explained,

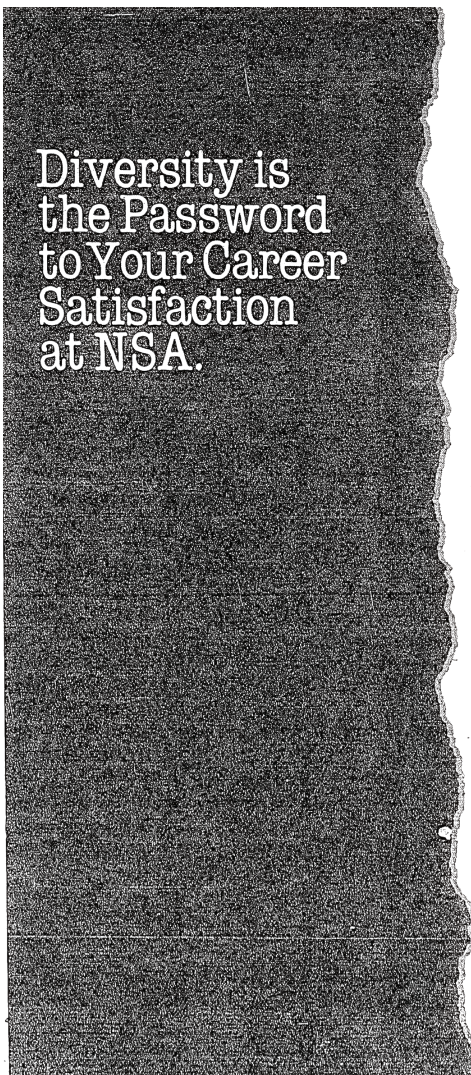
Information war has no front line. Potential battlefields are anywhere networked systems allow access—oil and gas pipelines, for example, electric power grids, telephone switching networks. In sum, the U.S. homeland may no longer provide a sanctuary from outside attack

(Rand Research Review 1995; emphasis added.)

In this line of thinking, a wide array of forms of computer intrusion became intimately linked to other forms of asymmetric dangers to the homeland, such as biological and chemical warfare.

The porousness of the state in the global information age accordingly demanded an expansion—a hypertrophy—of state capacities and legal authorities at home and abroad to compensate. The worldwide network of surveillance revealed in the Snowden documents is a key product of this hypertrophy. In the U.S. intelligence community, the challenges of new technologies demanded rethinking Fourth Amendment prohibitions against unreasonable search and seizure. In a document intended to gain the support of the incoming presidential administration, NSA explained in 2000,

Make no mistake, NSA can and will perform its missions consistent with the Fourth Amendment and



Diversity is the Password to Your Career Satisfaction at NSA.

all applicable laws. But senior leadership must understand that today's and tomorrow's mission will demand a powerful, permanent presence on a global telecommunications network that will host the 'protected' communications of Americans as well as the targeted communications of adversaries

(NSA 2000:32).

The briefing for the future president and his advisors delivered the hard truths of the new millennium. In the mid- to late 1990s, technically minded circles in

Engineers...Computer Scientists...Mathematicians... Language Specialists

Unparalleled diversity in the technologies of the future and in all types of assignments awaits you at the National Security Agency. At NSA, we're charged with the unique missions of collecting, analyzing and assessing foreign signals, as well as with safeguarding our government's vital communications and securing its massive computer systems. To carry out these unique missions, we continually develop the most sophisticated technologies and advanced techniques, often years in advance of their commercial use. At NSA, you'll find the kind of equipment, support facilities and technical assistance that many companies and private labs dream about, including a computer complex so vast that it's measured in acres.

NSA's diversity of 21st century technologies also gives you the opportunity to move freely among a wide variety of organizations and assignments within the Agency and for resultant rapid career advancement.

We currently have positions available for individuals with interests and experience in the following areas:

Electrical Engineering

(Minimum of BS/EE required)

Electrical Engineers work across the technological and functional spectrum. Opportunities range from fundamental research through advanced development, small to large system design and prototype development, developmental test and evaluation, field installation and operational support.

- | | |
|---|---------------------------------|
| Computer Security and Networking | Signals Analysis and Processing |
| Hardware and Software | RF and Microwave Systems |
| Design, Development and Interface | Speech Processing |
| Microprocessor Implementation and Programming | Logic Design |
| LSI/VLSI | Contract Management |
| Analog and Digital Design | CAID/AM |
| Secure Communications | Systems Acquisition |
| Communications Systems Design and Analysis | Optics |
| | EW |
| | Systems Architecture and Design |

Computer Science

(Minimum of BS in Computer Science required)

Our Computer Scientists work with Electrical Engineers and Mathematicians across the frontier of finite state machine development and applications.

- | | |
|-------------------|-----------------------------|
| Computer Security | Systems Design and Analysis |
| Applications | Software Engineering |
| Graphics | Operating Systems |
| | DBMS |

Mathematics

(Minimum of BA/BS in Math required)

Work in a challenging research environment using a variety of mathematical concepts, including algebra, probability theory, statistics, Galois theory and group theory.

- | | |
|-----------------------|--------------------------|
| Cryptanalysis | Computer Architecture |
| Cryptography | Operations Research |
| Algorithm Development | Mathematical Engineering |

Languages

(Minimum of BA in specified language or native proficiency)

As a Language Specialist, you'll be transcribing, translating, analyzing or reporting on material that involves matters of utmost concern to the security of the United States.

- | | |
|----------------|-----------|
| • Slavic | • Asian |
| • Near Eastern | • African |

In addition to the challenges and career rewards of diverse projects, NSA offers competitive salaries and benefits plus, most importantly, the opportunity to make your own crucial contribution to an informed and secure environment for our nation's policymaking. Discover your password to job satisfaction today. Send your resume to:



Unheard of Career Opportunities

NATIONAL SECURITY AGENCY
ATTN: M323 (1AD)
Fort Meade, MD 20778-6000

U.S. citizenship required
We are an equal opportunity employer

the Departments of Defense and Justice, in corners of the Intelligence Community, and in various scattered think tanks around Washington and Santa Monica began sounding the call for a novel form of homeland security, where military and law enforcement, the government and private industry, and domestic and foreign surveillance would necessarily mix in ways long seen as illicit if not illegal. Constitutional interpretation, jurisdictional divisions, and the organization of bureaucracies alike would need to undergo dramatic—and painful—change. In a remarkable draft “Road Map for National Security” from 2000, a centrist bi-

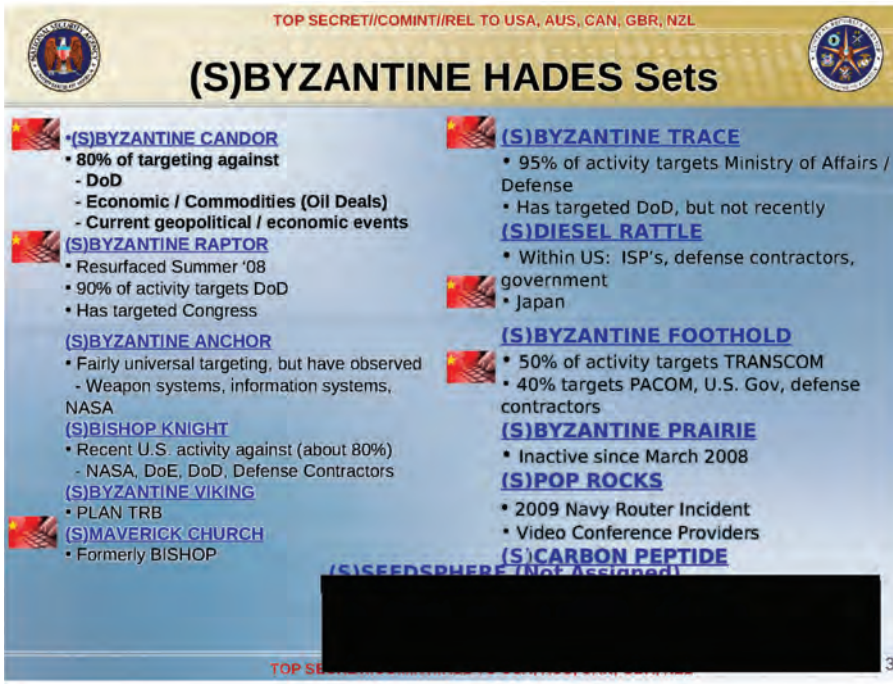


FIGURE 4: NSA's list of major Chinese CNE efforts, called "BYZANTINE HADES." (REDACTED-NTOC 2010).

perspective (i.e., low cost of entry, few tangible observables, a diverse and expanding target set, increasing amounts of 'freely available' information to support target development, and a flexible base of deployment where being 'in range' with large fixed field sites isn't important) present a particularly difficult problem for the defense... before you get too excited about this 'target-rich environment,' remember, General Custer was in a target-rich environment too! (Redacted 1997: 9; emphasis added).

The Air Force and NSA pioneered computer security from the late 1960s: their experts warned that the wide adoption of information technology in the United States would make it the premier target-rich environment (Hunt 2012). NSA's capacities developed as China, Russian, and other nations dramatically expanded their own computer espionage efforts (see figure 4 for the case of China c. 2010).

By 2008, and probably much earlier, the Agency and its close allies probed computers worldwide, tracked their vulnerabilities, and engineered viruses and worms both profoundly sophisticated and highly targeted. Or as a key NSA hacking division bluntly put it: "Your data is our data, your equipment is our equipment—anytime, anyplace, by any legal means" (SID Today 2006: 2).

While the internal division for hacking was named "Tailored Access Operations," its work quickly moved beyond the highly tailored—bespoke—hacking of a small number of high priority systems. In 2004, the Agency built new facilities to enable them to expand from "an average of 100–150 active implants to simultaneously managing thousands of implanted targets" (SID Today 2004a:2). According to Matthew Aid, NSA had built tools (and adopted easily available open source tools) for scanning billions of digital devices for vulnerabilities; hundreds of operators were covertly "tapping into thousands of foreign computer systems" worldwide (Aid 2013). By 2008, the Agency's

partisan group argued, "in the new era, sharp distinctions between 'foreign' and 'domestic' no longer apply. We do not equate national security with 'defense'" (U.S. Commission on National Security 2001). 9/11 proved the catalyst, but not the cause, of the emergence of the homeland security state of the new millennium. The George W. Bush administration drew upon this dense congeries of ideas, plans, vocabulary, constitutional reflection, and an overlapping network of intellectuals, lawyers, ex-spies, and soldiers to develop the new homeland security state. This intellectual framework justified the dramatic leap in the foreign depth and domestic breadth of the acquisition, collection, and analysis of communications of NSA and its Five Eyes partners, including computer network exploitation.

THE GOLDEN AGE OF SIGINT

In its 2000 prospectus for the incoming presidential administration, the NSA included an innocent sounding clause: "in close collaboration with cryptologic and Intelligence Community partners, establish tailored access to specialized communications when needed" (National Security Agency 2001: 4). Tailored access

meant government hacking—CNS. In the early 1990s, NSA seemed to many a cold-war relic, inadequate to the times, despite its pioneering role in computer security and penetration testing from the late 1960s onward. By the late 2010s, NSA was at the center of the "golden age of SIGINT" focused ever more on computers, their contents, and the digital infrastructure (NSA 2012: 2).

From the mid 1990s, NSA and its allies gained extraordinary worldwide capacities, both in the "passive" collection of communications flowing through cables or the air and the "active" collection through hacking into information systems, whether it be the president's network, Greek telecom networks during the Athens Olympics, or in tactical situations throughout Iraq and Afghanistan (see Redacted-Texas TAO 2010; SID Today 2004).

Prioritizing offensive hacking over defense became very easy in this context. An anonymous NSA author explained the danger in 1997:

The characteristics that make cyber-based operations so appealing to us from an offensive



FIGURE 5: Worldwide SIGINT/Defense Cryptologic Platform, n.d., (HTTPS://ARCHIVE.ORG/DETAILS/NSA-DEFENSE-CRYPTOLOGIC-PLATFORM.)

forms of metadata such as calling records from legal protection stems from the intelligence value of studying metadata at scale. The collection of the metadata of one person, on this view, is not legally different from the collection of the metadata of many people, as the U.S. Foreign Intelligence Surveillance Court has explained:

[so] long as no individual has a reasonable expectation of privacy in meta data [sic], the large number of persons whose communications will be subjected to the . . . surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur.⁷

Yet metadata is desired by intelligence agencies just because it is revealing at scale. Since their inception, NSA and its Commonwealth analogues have focused as much on working with vast databases of “metadata” as on breaking cyphered texts. NSA’s historians celebrate a cryptographical revolution afforded through “traffic analysis” (Filby 1993). From reconstructing the Soviet “order of battle” in the Cold War to seeking potential terrorists now, the U.S. Government has long recognized the transformative power of machine analysis of large volumes of metadata while simultaneously denying the legal salience of that transformative power.

As in the case of metadata, U.S. legal work on hacking into computers does not consider scale as legally significant. Espionage at scale used to be tough going: the very corporeality of sifting through physical mail, or garbage, or even setting physical wiretaps, or other devices to capture microwave transmissions scale only with great expense, difficulty, and potential for discovery (Donovan 2017).

distributed XKeyscore database and search system offered its analysts the option to “Show me all the exploitable machines in country X,” meaning that the U.S. government systematically evaluated all the available machines in some nations for potential exploitation and catalogued their vulnerabilities. Cataloging at scale is matched by exploiting machines at scale (National Security Agency 2008). One program, *Turbine*, sought to “allow the current implant network to scale to large size (millions of implants)” (Gallagher and Greenwald 2014). The British, Canadian, Australian partner intelligence agencies play central roles in this globe-spanning work.

THE DISANALOGY WITH ESPIONAGE

The legal status of government hacking to exfiltrate information rests on an analogy with traditional espionage. Yet the scale and techniques of state hacking strain the analogy. Two lawyers associated with U.S. Cyber Command, Col. Gary Brown and Lt. Col. Andrew Metcalf, offer two examples: “First, espionage used to be a lot more difficult. Cold Warriors did not anticipate the wholesale plunder of our industrial secrets. Second, the techniques of cyber espionage and cyber attack are often identical, and cyber espionage is usually a necessary prerequisite for cyber attack” (Brown and Metcalf 1998:117).

The colonels are right: U.S. legal work on intelligence in the digital age has tended to deny that scale is legally significant. The international effort to exempt sundry

Scale provided a salutary limitation on surveillance, domestic or foreign. As with satellite spying, computer network exploitation typically lacks this corporeality, barring cases of getting access to air-gapped computers, as in the case of the StuxNet virus. With the relative ease of hacking, the U.S. and its allies can know the exploitable machines in a country X, whether those machines belong to generals, presidents, teachers, professors, jihadis, or eight-year olds.

Hacking into computers unquestionably alters them, so the analogy with physical espionage is imperfect at best. A highly-redacted Defense Department “Information Operations Policy Roadmap” of 2003 underscores the ambiguity of “exploitation versus attack.” The document calls for clarity about the definition of an attack, both against the U.S. (slightly redacted) and by the U.S. (almost entirely redacted). “A legal review should determine what level of data or operating system manipulation constitutes an attack” (Department of Defense 2003:52). Nearly every definition—especially every classified definition—of computer network exploitation includes “enabling” as well as exploitation of computers. The military lawyers Brown and Metcalf argue, “Cyber espionage, far from being simply the copying of information from a system, ordinarily requires some form of cyber maneuvering that makes it possible to exfiltrate information. That maneuvering, or ‘enabling’ as it is sometimes called, requires the same techniques as an operation that is intended solely to disrupt” (Brown and Metcalf 1998:117) “Enabling” is the key moment where the analogy between traditional espionage and hacking into computers breaks down. The secret definition, as of a few years ago, explains that enabling activities are “designed to obtain or facilitate access to the target computer system for possible later” computer network attack. The enabling function of an implant placed on a computer, router, or printer is the preparation of the space of future battle: it’s as if every time a spy entered a locked room to plant a bug, that bug contained a nearly unlimited capacity to materialize a bomb or other

7 Quotation from secret decision with redacted name and date, p. 63, quoted in Amended Memorandum Opinion, No. BR 13-109 (Foreign Intelligence Surveillance Court August 29, 2013).

device should distant masters so desire. An implant essentially grants a third-party control over a general-purpose machine: it is not limited to the exfiltration of data. Installing an implant within a computer is like installing a cloaked 3-D printer into physical space that can produce a photocopier, a weapon, and a self-destructive device at the whim of its master. One NSA document put it clearly: “Computer network attack uses similar tools and techniques as computer network exploitation. If you can exploit it, you can attack it” (SID Today 2004b).

In a leaked 2012 Presidential Policy Directive, the Obama administration clarified the lines between espionage and information warfare explicitly to allow that espionage may produce results akin to an information attack. Amid a broad array of new euphemisms, CNE was transformed into “cyber collection,” which “includes those activities essential and inherent to enabling cyber collection, such as inhibiting detection or attribution, even if they create cyber effects” (Presidential Policy Directive (PPD)-20: 2-3). The bland term ‘cyber effects’ is defined as “the manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.” Espionage, then, often will be attack in all but name. The creation of effects akin to attack need not require the international legal considerations of war, only the far weaker legal regime around espionage. With each clarification, the gap between actual government hacking for the purpose of obtaining information

and traditional espionage widens; and the utility of espionage as a category for thinking through the tough policy and legal choices around hacking diminishes.

SURVEILLING IRONY

By the end of the first decade of the 2000s, sardonic geek humor within NSA revealed in the ironic symbols of government overreach. A classified NSA presentation trolled civil libertarians: “Who knew that in 1984” an iPhone “would be big brother” and “the Zombies would be paying customers” (Spiegel Online 2013). Apple’s famous 1984 commercial dramatized how better technology would topple the corporatized social order, presaging a million dreams of the Internet disrupting wonted order. Far from undermining the ability of traditional states to know and act, the global network has created one of the greatest intensifications of the power of sovereign states since 1648. Whether espoused by cyber-libertarians or RAND strategists, the threat from the Net enabled new authorities and undermined civil liberties. The potential weakening of the state justified its hypertrophy. The centralization of online activity into a small number of dominant platforms—Weibo, Google, Facebook, with their billions of commercial transactions, has enabled a scope of surveillance unexpected by the most optimistic intelligence mavens in the 1990s. The humor is right on.

Signals intelligence is a hard habit to break—civil libertarian presidents like Jimmy Carter and Barack Obama quickly found themselves taken with being able to peek at the intimate communications of friends and foes alike, to know their negotiating positions in advance, to be three

steps ahead in the game of 14-dimensional chess. State hacking at scale seems to violate the sovereignty of states at the same time as it serves as a potent form of sovereign activity today. Neither the Chinese hacking into OPM databases nor the alleged Russian intervention in the recent US and French elections accords well with many basic intuitions about licit activities among states. If it would be naïve to imagine the evanescence of state-sanctioned hacking, it is doctrinally and legally disingenuous to treat that hacking as entirely licit based on ever less applicable analogies to older forms of espionage.

As the theorists in the U.S. military and intelligence worlds in the 1990s called for new concepts and authorities appropriate to the information age, they nevertheless tamed hacking for information by treating it as continuous with traditional espionage. The near ubiquity of state-sanctioned hacking should not sanction an ill-fitting legal and doctrinal frame that ensures its monotonic increase. Based on an analogy to spying that ignores scale, “computer network exploitation” and its successor concepts preclude the rigorous analysis necessary for the hard choices national security professionals rightly insist we must collectively make. We need a ctrl+alt+del. Let’s hope the implant isn’t persistent. ■

MATTHEW L. JONES teaches history of science and technology at Columbia. He is the author, most recently, of *Reckoning with Matter: Calculating Machines, Innovation, and Thinking about Thinking* from Pascal to Babbage. (Chicago, 2016).

BIBLIOGRAPHY

- Aid, Matthew M. 2013. “Inside the NSA’s Ultra-Secret China Hacking Group,” *Foreign Policy*. June 10. http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group?page=full
- American Interest. 2015. “Former CIA Head: OPM Hack was ‘Honorable Espionage Work.’” *The American Interest*. June 16. <https://www.the-american-interest.com/2015/06/16/former-cia-head-opm-hack-was-honorable-espionage-work/>
- Andrews, Duane. 1996. “Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D),” December.
- Barlow, John Perry. “A Declaration of the Independence of Cyberspace.” *Electronic Frontier Foundation*, February 8, 1996. <https://www.eff.org/cyberspace-independence>
- Berkowitz, Bruce D. 2003. *The New Face of War: How War Will Be Fought in the 21st Century*. New York: Free Press
- Boccagno, Julia. 2016. “NSA Chief speaks candidly of Russia and U.S. Election.” *CBS News*. November 17. <http://www.cbsnews.com/news/nsa-chief-adm-michael-rogers-speaks-candidly-of-russias-use-of-wikileaks-in-u-s-election/>
- Brown, Gary D. and Andrew O. Metcalf. 1998. “Easier Said Than Done: Legal Reviews of Cyber Weapons,” *Journal of National Security Law and Policy* 7.
- CJCSI 3210.01A. 1998. “Joint Information Operations Policy,” Joint Chiefs, November 6. https://archive.org/details/CJCSI3210_01A
- DCID 7/3. 2003. “Information Operations and Intelligence Community Related Activities.” Central Intelligence Agency, June 5. <https://fas.org/irp/offdocs/dcid7-3.pdf>

- Department of Defense. 2003. "Information Operations Roadmap," October 30. http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf
- DODD TS 3600.1. 1992. "Information Warfare (U)," December 21. <https://archive.org/details/14F0492Doc01DirectiveTS3600.1>
- DODD S-3600.1, 1996. "Information Operations (IO) (U)," December 9. https://archive.org/details/DODD_S3600.1
- Donovan, Joan. 2017. "Refuse and Resist!" *Limn* 8, February. <http://limn.it/refuse-and-resist/>
- Falk, Richard A. 1962. "Space Espionage and World Order: A Consideration of the Samos-Midas Program," in *Essays on Espionage and International Law*. Akron: Ohio State University Press.
- Fields, Craig, and James McCarthy, eds. 1994. "Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," October. <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA286745>
- Filby, Vera R. 1993. *United States Cryptologic History, Sources in Cryptologic History*, Volume 4, *A Collection of Writings on Traffic Analysis*. Fort Meade, MD: NSA Center for Cryptological History.
- Gallagher, Ryan and Glenn Greenwald. 2014. "How the NSA Plans to Infect 'Millions' of Computers with Malware," *The Intercept*. March 12. <https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/>
- Gilman, Nils, Jesse Goldhammer, and Steven Weber. 2017. "Can You Secure an Iron Cage?" *Limn* 8, February. <http://limn.it/can-you-secure-an-iron-cage/>
- Hunt, Edward. 2012. "U.S. Government Computer Penetration Programs and the Implications for Cyberwar," *IEEE Annals of the History of Computing*. 34(3):4-21.
- Johnson, Philip A. 1999. "An Assessment of International Legal Issues in Information Operations," 1999, 40. <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADB257057>
- Kaplan, Fred M. *Dark Territory: The Secret History of Cyber War*. New York: Simon & Schuster, 2016.
- Kuehl, Dan. 1997. "Defining Information Power," *Strategic Forum: Institute for National Strategic Studies*, National Defense University, no. 115 (June). <https://web.archive.org/web/20050208041218/http://www.ndu.edu/inss/strforum/SF115/forum115.html>
- Lin Herbert S. 2010. "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy*, 4.
- National Security Agency/Central Security Service. 2000. "Transition 2001" December. <http://nsarchive.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf>
- National Security Agency. 2008 "XKEYSCORE." February 25. https://www.eff.org/files/2014/04/09/20130731-guard-xkeyscore_training_slides.pdf
- National Security Agency. 2012. "(U) SIGINT Strategy, 2012-2016," February 23. <https://archive.org/details/NSA-SIGINT-Strategy>
- NSA Office of General Counsel. n.d. "(U/FOUO) CNO Legal Authorities," slide 8. https://www.aclu.org/sites/default/files/field_document/CNO%20Legal%20Authorities_0.pdf
- Owens, William, Kenneth W. Dam, and Herbert S. Lin. 2009. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington D.C.: National Academies Press.
- Presidential Policy Directive (PPD)-20: "U.S. Cyber Operations Policy," October 16, 2012. <https://www.fas.org/irp/offdocs/ppd/ppd-20.pdf>
- Rand Research Review. 1995. "Information Warfare: A Two-Edged Sword." *Rand Research Review: Information Warfare and Cyberspace Security*. Ed. A. Schoben. Santa Monica: Rand. https://www.rand.org/pubs/periodicals/rand-review/issues/RRR-fall95-cyber/infor_war.html
- Rattray, Gregory J. 2001. *Strategic Warfare in Cyberspace*. Cambridge, Mass: MIT Press.
- Redacted. 1994 "Information Warfare: A New Business Line for NSA," *Cryptolog*. July.
- Redacted. 1997. "IO, IO, It's Off to Work We Go . . . (U)," *Cryptolog*. Spring.
- Redacted-NTOC, V225. 2010, "BYZANTINE HADES: An Evolution of Collection," June. https://www.eff.org/files/2015/02/03/20150117-spiegel-byzantine_hades_-_nsa_research_on_targets_of_chinese_network_exploitation_tools.pdf
- Redacted-Texas TAO/FTS327. 2010. "Computer-Network Exploitation Successes South of the Border," November 15. https://www.eff.org/files/2013/11/15/20131020-spiegel-mexican_president.pdf
- Rid, Thomas. *Rise of the Machines: A Cybernetic History*. New York: W. W. Norton & Company, 2016.
- Rothrock, John. 1997. "Information Warfare: Time for Some Constructive Criticism," in *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt. Santa Monica: Rand.
- Schmitt, Michael N., ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. 2nd ed. Cambridge: Cambridge University Press. DOI:10.1017/9781316822524.
- SID Today. 2004. "Another Successful Olympics Story," October 6, 2004. <https://www.eff.org/document/20150928-intercept-another-successful-olympics-storypdf>
- SID Today. 2004a. "Expanding Endpoint Operations." September 17. <https://www.eff.org/document/20150117-spiegel-document-about-expansion-remote-operations-center-roc-endpoint-operations>
- SID Today. 2004b. "New Staff Supports Network Attack." October 21. <https://theintercept.com/snowden-sidtoday/3676084-new-staff-supports-network-attack/>
- SIDToday. 2006. "The ROC: NSA's Epicenter for Computer Network Operations," September 6. https://www.eff.org/files/2015/01/23/20150117-spiegel-document_explaining_the_role_of_the_remote_operations_center_roc.pdf
- Spiegel Online. 2013. "Spying on Smartphones," *SPIEGEL ONLINE*, September 9. <http://www.spiegel.de/fotostrecke/fotostrecke-101201.html>
- United States Commission on National Security/21st Century. 2001. *Road Map for National Security: Imperative for Change*. January 31. Final Draft. <https://www.hsdl.org/?abstract&did=2079>
- Wolfowitz, Paul. 2001. "Department of Defense Directive 3600.1 Draft," October.

the public interest hack

How are hacking and leaking related?
Gabriella Coleman introduces us to the “public interest hack” and explains how it emerged.



ILLUSTRATION: AMISHA GADANI

IN WINTER OF 2014, AN INQUIRY FROM A JOURNALIST LANDED IN MY email inbox. His message opened innocently: “how can I can safely and effectively get plugged into the hacker community?” He continued with a hypothetical explanation: “my sense is that folks in particular hacker circles might be interested to know that a reporter is digging on topic X because they too are eager to see a spotlight thrown there.” Further discussion revealed he was interested in how hackers chose targets, a query prompted by the recent spate of Anonymous-led hacks and document leaks. After reminding him it was illegal to seek hacking aid of any sort, I told him that, as far as I knew, the hackers themselves had initiated these computer infiltrations and subsequent document exfiltrations. There was no indication they were ever prompted by a journalist or other citizen—as it should be, I stressed.

I was satisfied I had relayed to him (and any snoopers listening in) my unambiguous objections to such a scheme; but at the time, I overlooked the historical benchmark furnished by his inquiry. That he was interested in how hackers went about landing documents to publish signaled that a new strategy—what I am calling the public interest hack—had, by this historical juncture, become fully imaginable and established. To define it in its simplest terms: a public interest hack (PIH) entails a computer infiltration for the purpose of leaking documents that will have political consequence. Rather than perpetrating a hack just for

hacking’s sake, as hackers have always done, the PIH is a hack that will *interest the public* (even if, as we have seen with the DNC hacks and the Macron hack, it is not necessarily ‘in the public interest’ in some simply positive sense). This tactic can resemble traditional forms of leaking and whistleblowing, like the Pentagon Papers, insofar as both are high-risk activities leading to the release of publicly relevant documents. But they are distinct: because the PIH conjoins a computer intrusion—advertised as such—with a particular type of leak. The PIH has also taken on two distinct forms. In one class, many of the most prominent cases of the last five years—the hacks against security or intelligence firms like HBGary, Stratfor, Hacking Team, and FlexiSpy were orchestrated by hacktivists who explicitly sought to expose wrongdoing. Another class—like the Guardians of Peace hack of Sony Pictures and Guccifer 2.0’s hack of the Democratic National Convention—were carried out by mysterious crews who, in contrast, have obscured their intentions but still released data and documents that spurred extraordinary public attention and inquiry (See table 1).

When I have told hackers or technology journalists of my hunch—that the PIH strategy did not really quite exist prior to 2007 and was largely indebted to Anonymous—none of them believed me. In fact, I did not believe it myself. It is why I tapped these experts in the first place seeking to find the esoteric or

overlooked cases when hackers had infiltrated a system, snatched documents, and published them widely, triggering substantial news or inquiry about the hack *and* the documents. But all they could offer, along with their skepticism, were many cases of hacktivist interventions (“how about the NASA Wank Worm?” they might charge back, among *many* other cases). None, however, quite fit the mold of this relatively new political strategy. What then distinguishes the PIH from other varieties of hacks, leaks, and whistleblowing? And why did it come into being only between 2007 and 2011, when it was conceivable—ideologically and materially—for it to have emerged much earlier?

Prior to the emergence of the PIH, various kinds of hack-leak combinations and hacktivist techniques were common. Indeed, most of these can qualify as both political and of interest to the public; but as proposed here, the PIH is a more distinctive and a more singular category that excludes the great majority of hacks, leaks and breaches. For instance,

hackers have long infiltrated systems for all sorts of reasons—for fun, learning, and showmanship—and in the process swiped data and documents but never released them. For decades, hackers have also acquired and published credentials: passwords, log ins, and credit card numbers. But such leaked information can only be mobilized in the narrow form of consumer security advocacy. It is a distinct strategy for hackers and security researchers to use high profile breaches to urge corporate executives or government officials to invest more resources into digital fortifications. Other hacktivist techniques, like website defacements, distributed denial of service (DDoS) attacks, and even hacks of sabotage (like deleting files), don’t entail document acquisition; thus they fail to qualify as a public interest hack. Finally, some black hat hackers were known to shame enemies by acquiring a victim’s email spool and publishing it; but these events tended to be personal revenge skirmishes, with the emails never meant for wider uptake. Many examples

TABLE 1:
Public Interest
Leaks

TARGET	MATERIALS	HACKERS	YEAR
Hal Turner	limited emails leak	Unknown	2008
Sarah Palin	screen shots of emails	David Kernell	2008
Climatic Research Unit at University of West Anglia	emails	Unknown	2009
HBGary Federal	emails	Anonymous	2011
Stratfor Intelligence	emails	Anonymous	2011
Syrian Government	emails	RevoluSec	2012
Gamma Group	technical documentation and software	Phineas Phisher	2013
Hacking Team	emails	Phineas Phisher	2014
Peruvian government	emails	Anonymous/Lulzsec	2014
Sony Pictures	emails, documents, movies	Guardians of Peace	2014
CIA Director John Brennan	emails	Cracka’s with Attitude	2015
Turkish AKP leaks	emails	Phineas Phisher and others	2016
Bradley Foundation hack	emails	Anonymous Globo	2016
Democratic National Convention	emails	Guccifer 2.0	2016
Colin Powell	emails	Guccifer 2.0	2016
John Podesta	emails	Guccifer 2.0	2016
Cellebrite	documents and circumvention tools	Unknown	2017
Retina and FlexiSpy	source code, HR documents, and other files	Decepticons	2017
Emmanuel Macron campaign staff	emails	Unknown	2017

of this class of hacks may well exist, but most have never pierced public consciousness.

There are likely cases—and I know of one—whereby a hacker leaked documents to the public or a journalist but did so without advertising the source of the material as a hack. I’ve identified one occurrence in this style, but had to venture deeply to recover it: in the mid-1990s, amid trenchant critiques of the Church of Scientology voiced on a popular Usenet mailing list, a hacker accessed Scientology servers, siphoned some documents and released them to the list. Still, measuring this early hacking case by my criteria, this hack-leak fails to qualify as a public interest hack because the hacker never advertised how he or she obtained the material. If we compare this instance with those hacks and leaks orchestrated by Phineas Phisher—who after hacking the Italian firm Hacking Team, published a “Hack Back” manual (2016) seeking to galvanize others to emulate him—we can identify the precise historical period when hackers publicized this strategy and thus positioned it for adoption and replication.

The PIH stabilized only in 2011, an exceptional year of political ferment characterized by waves of street-based demonstrations and the ascendancy of the hacker as a major geopolitical force. With Anonymous and WikiLeaks, hackers pushed the levers of power in new and far more consequential ways, making hacks and leaks the stuff of foreign policy briefs and international relations debates. In this period, Anonymous hackers twice stumbled upon newsworthy documents that they then published on accessible platforms like the Pirate Bay or WikiLeaks. Their conspicuous brand of hacking—accompanied by catchy digital posters and videos—lured in media professionals who boosted Anonymous’ profile and by extension raised the profile of this mode of disclosure, ensuring that scattered instances of this method would crystallize into a template for emulation. But before we turn to Anonymous proper and the stabilization of this tactic, let’s start with the pre-history of this method.

A BRIEF GENEALOGY OF THE PUBLIC INTEREST HACK

Roughly five years before hackers executed one of the first instances of the public interest hack, there are two borderline cases that prefigure the tactic: the acquisition of digital documents from the voting machine company Diebold; and the publication of emails from the now-defunct energy giant Enron. Even if these materials were not obtained by hacks, these two cases drew a hermeneutic circle, making it apparent that such digital information might be out there for the taking. The events also signaled that releasing digitally-hosted or digitally-compiled data, like emails, could potentially serve a democratic function by exposing or corroborating wrongdoing.

The Diebold case began in 2002 when Seattle resident Bev Harris learned that her county had purchased touchscreen voting machines and she flung herself into research on software vulnerabilities. While seeking technology experts online who could answer her litany of concerns, she found something more consequential: the source code, hardware schematics, internal mailing list archives, passwords, and documents for vote-counting software. Her initial attempt to hand over the documents to journalists by sending “more than 100,000 bulletins directly to the appropriate editors and producers,” proved ineffectual (Harris 2003: 158). Later in the year, spurred by research enabled by the documents, the *New York Times* finally ran an exclusive story on “the stunning research flaws” in the Diebold system (Schwartz, 2003).

In same period, a large corpus of corporate emails—over 600,000 emails written by Enron employees—were published for the first time on the internet. The responsible party was not a reckless hacker, WikiLeaks (an organization not yet in existence), nor the Russian government, but an obscure American government agency: the Federal Energy Regulatory Commission (FERC). At the time, Enron had been embroiled in scandal with its top corporate executives under investigation for fraud. According to a later report by the *Wall Street Journal*, the FERC published the corpus “to help the public better understand whether Enron helped to create—and then profit from—an energy shortage in California during 2000 and 2001” (Berman, 2003). In spite of FERC’s intentions, the contents of the emails attracted scant journalistic scrutiny; the *Wall Street Journal* rebuffed the release at the time, citing privacy violations. Not long after, another journalist defended the publication of the emails for offering a glimpse—into the “soul” as he put it—of the corrupt organizational culture of Enron (Grieve, 2003).

A few years later in 2007, a retributive attack orchestrated by anonymous 4chan users marked one of the first instances of a hack where information found in exfiltrated emails was publicized to damage the reputation of a targeted individual and picked up by organizations well outside of the technology and hacker community. It all began when Anonymous trolls prank called Hal Turner, a white supremacist radio host. When he made the grave error of doxing the callers, a group of 4chan anons decided to dox him right back: broadcasting Turner’s home phone number, previous places of residence, and criminal records. As the doxing feud escalated, online allegations swirled that Turner was an FBI mole, sleuthing for the government to out white supremacists. The ostensible source of the accusation came from emails acquired by anonymous (not Anonymous) hackers. While the emails have since vanished, and didn’t at the time spark any stories in the mainstream press, they became public knowledge, as groups like the Southern Poverty Law Center posted news of the hack and emails on their website (Potok, 2008). Due to this hack and leak, Hal Turner—once a beloved public personality among hard-core racists—became a pariah.

Another similar incident was executed in 2008 by David Kernell and was directed against then-presidential candidate Sarah Palin. Kernell, revealed to be the son of a Democratic representative, hacked Palin’s Yahoo email account and posted to 4chan proof of the intrusion, an explanation of why and how he carried out the hack, and his fears of getting caught (his hunch proved founded: he was arrested not long after). Sharing a few screenshots he lamented, “there was *nothing* there, nothing incriminating, nothing that would derail her campaign as I hoped” (Schor, 2008). Even though he found nothing to publish, the case signals that by 2008, hackers were openly pursuing this game plan; and unlike the Hal Turner incident, the mainstream press picked up the Sarah Palin hack, with Gawker and WikiLeaks



republishing the screenshots. The wide coverage likely worked to sow the idea for future uptake.

Another two years would pass before Anonymous would strike again with a hack leading to a newsworthy email disclosure. In 2010, they managed to publish a large email cache thanks to a technical bungle by a company targeted by Anonymous hackers for other reasons. In September 2010, an Anonymous activist node by the name of AnonOps launched a pro-piracy campaign by hammering a slew of copyright industry websites with DDoS attacks. One target was ACS:Law, a British law firm under fire for sending thousands of notices to British citizens threatening them with lawsuits unless they ponied up a lump sum for their alleged piracy. ACS:Law's emails were obtained when, in the midst of being thrashed with a DDoS attack, ACS:Law removed their website from the internet. Upon restoring it, a misconfiguration meant all their email was on deck, available for the taking. Anonymous snapped up the digital assets and re-directed the emails to The Pirate Bay. Various parties waded into material, including Ars Technica reporter Nate Anderson, who provided an in-depth exposition of the emails, laying out the company's workings—and how many of their threats to supposed pirates were recklessly targeted (Anderson, 2010). "If there's one great theme running through these letters," highlighted Anderson, it's the poverty of the respondents" (ibid). Ultimately, the consequences of this hack and email disclosure were as direct as they were substantial: the government levied fines against the firm for its poor security and failure to protect sensitive personal data, and the firm was forced to close.

From the ACS:Law leak onwards, it became clear that the act of publishing exfiltrated digital content would garner public attention and—depending on the nature of the content—could serve particular political interests, in this case defending ordinary people from aggressive anti-piracy corporations. Hackers affiliated with Anonymous—and eventually others—at this moment became more deliberate: directing their finely-honed skills towards intelligence gathering of leakable information. For instance, in January 2011, some of the same hackers who published the ACS:Law emails squirreled into the Tunisian Prime Minister's email servers, hoping to find damning material that if released could turbo-boost the popular revolt gripping the nation. Their jaunt proved unsuccessful and they had to remain satisfied with the consolation prize of various website defacements.

That is, until two weeks later when the same platoon hacked Aaron Barr, the CEO of federal intelligence firm HBGary Federal. Barr was on a quest

HB Gary
CEO Aaron
Barr on The
Colbert
Report,
2011.



to infiltrate and dox Anonymous hackers. After the *Financial Times* published a piece detailing Barr's crackpot plan to publicly identify the core leaders driving the hacking operations (Menn, 2011), these hackers snarled back at Barr (whose 'intel' was wrong) with their own merciless brand of "infiltration." In one evening, Anonymous hackers snaked their way into HBGary Federal computer systems, hauled away the company's emails, posted them on The Pirate Bay, and gutted whatever else remained on the system.

Owing in part to the irony of a ragtag band of hackers taking down a security firm with minimal effort, and the damning plot discovered in the emails, Operation HBGary became legendary among hackers and security professionals. The emails were full of fascinating information—including a PowerPoint concocted by Barr in partnership with Palantir and Berico employees, detailing plans to thwart and destroy WikiLeaks and its associates using dubious and illegal methods. One of the more reprehensible tidbits of their plan was to slander journalist Glenn Greenwald who, according to their assessment, would halt supporting WikiLeaks if his career was put under jeopardy.

Because the email contents and the logistics of the hack were juicy, shocking, and newsworthy—tailor-made for our contemporary media environment—the HBGary hack and leak dominated the news cycle for days. And like ACS:Law before it, airing the emails had an impact far beyond the shame it bestowed upon Aaron Barr. Disgraced, he was forced to resign; and not long after, HBGary Federal was itself dismantled. In the euphoria of victory, these hackers were emboldened to hack even more, which is precisely the path they took: first with a breakaway group Lulzsec and later with Antisec.

The gale of Anonymous hacking in 2011 brought seasoned hacktivist Jeremy Hammond out of retirement. Chartering a militant crew, Antisec, Hammond ensured that under his tutelage Anonymous would continue to prowl servers for the acquisition of incriminating evidence destined for wider distribution. After a string of hacks, one audacious exfiltration finally resulted in his arrest by the FBI. Rolled out against an intelligence firm Stratfor, the hack landed Strafor's emails, which Hammond sent to WikiLeaks. Journalists then mined them for evidence, pointing to the corporate spying against activists. Unlike the HBGary hacks, here Hammond and his teammates were not triggered by revenge—acting merely reactively—but were instead proactively seeking information.

Before the HBGary and the Stratfor hacks, hackers had certainly started to intrude systems for the purpose of extracting the sort of information the public or journalists might deem important. But the few successful instances of such an approach were scattershot or obscure. From this moment on in 2011, a time period when hacktivism itself had soared into the geopolitical stratosphere, this tactic gained momentum and seemed to settle into political pattern. The HBGary and Stratfor hacks were a sign a new threshold had been reached, at least in North American, European, and Latin American regions,' but it was not entirely clear whether the PIH would survive after law enforcement arrested scores of hackers who were responsible for these types of hacks.

The answer came in 2014 when other hacktivists executed exceptionally visible and high-impact public interest hacks. In Peru, the government nearly dissolved after a two-person Anonymous hacktivist crew, Lulzsec Peru,

distributed hacked emails from the Department of the Interior—correspondence teeming with evidence of corruption. After a flurry of press coverage, the issue forced a vote and the count was one vote shy from forcing a change in leadership. In 2014 and 2015 another hacktivist, Phineas Phisher, hacked in the service of data leaks by striking against two firms, Gamma Group and Hacking Team—firms suspected of selling surveillance software to totalitarian regimes. Like previous cases discussed here, his liberation of Hacking Team’s emails served as an evidential anchor by confirming suspected wrongdoing. This was put well to me by Lorenzo Franceschi-Bicchierai who covered the hack for VICE Motherboard: “Before Phineas Fisher broke into the servers of Hacking Team, we already suspected, based on extensive and detailed research, that they were selling [spyware] to oppressive regimes. But his hack gave us the ultimate proof.”² A year after the hack, Hacking Team lost its license to export spyware outside of the EU.

Up until 2014, public interest hacks were solely the domain of hacktivists. But in the summer of 2014, a distinct and more mysterious species of hacker would deploy this tactic. Unlike hacktivists who transparently express their objectives, these actors advertised their hacks, but never disclosed their true intent.

The first hack to unfurl in this new guise struck like a tempest in 2014, when a mysterious hacker group, Guardians of Peace (GOP), ransacked and pillaged Sony’s servers, dropping company emails into the public. It was an attack characterized by security and government officials as “unprecedented”—largely, I would suggest, for its PIH characteristics. Eventually the GOP specified that their actions were taken in vengeance for a Hollywood film—*The Interview*—that poked fun at the North Korean dictator. The journalistic analysis, which was gargantuan, largely concentrated on the intrusion, extortion, motivations, and forensics of the hack rather than the content of the emails. Still, some journalists excavated the material for salacious gossip about celebrities written by executives, while others used it for social commentary: uncovering disparities in earnings by gender and race. What was already known was made explicit, with exact financial figures suddenly made available.

While the US government blamed the North Korean government, the hack baffled many security experts; some of whom insisted the claim rested on shaky, inconclusive evidence (Zetter 2014). Determining whether or not the North Korean government masterminded the hack or only later piggybacked on its coattails may prove unimportant; this hack offered another public statement that conveyed in effect that a government or other entity *could* use this method for a motley array of purposes, such as retribution, a raw display of aggression and power, or other geopolitical machinations.

It appears that at least one powerful nation has since heeded the lesson. Nearly two years later, a similar hack—similar insofar as the ulterior motive was concealed—was leveled against the Democratic National Committee (DNC), leading to the disclosure of multiple email caches. The hacker-in-chief laying claim to intrusion went by Guccifer 2.0. In contrast to the Sony hack, different sectors of the security community were nearly unanimous in their assessment: everything about the hack—from forensic to

other geopolitical evidence—pointed to Russian intelligence.

This hack and leak leapfrogged past the GOP Sony hack to become the single most controversial PIH to date. The fallout from the hack was volcanic, with raging disputes spewing to this day about its source, impact, and meaning: scores of liberals were dismayed that the emails might have thwarted Hillary Clinton election bid; Bernie Sander’s supporters were livid that the correspondence demonstrated the DNC failed to play fair; and some pundits and journalists harrumphed that the emails contained no meaningful material whatsoever (see Sauter, Colvin, Fish and Follis, and Gorham in this issue for contrasting takes). Some information liberation advocates were upset that WikiLeaks chose to publish the emails at all, while others supported the embattled organization—asserting that truth is not distorted by its messengers. Elsewhere, various pundits: wished the material had been published only after the election; forecasted the start of new cold war with then President Obama shortly thereafter booting thirty-five Russian diplomats from the US; maintained the Russian hysteria was overly-hysterical; and used the emails as raw ingredients to cook up the dangerously weird conspiracy theory, Pizzagate.

The DNC hack/leak, thoroughly defined along numerous fault lines, unfurled over time with divergent consequences. The DNC emails were used by some journalists to break stories. But the material could also be used to unleash a thicket of confusion or, what might be better called (with a nod to the fog of war) the fog of hacking—a hack and leak designed to distract, confuse, and seed doubt in the public.

CONCLUSION

The history of the PIH may be remarkably recent but it seems here to stay. Indeed, 2017 has already seen a number of high-profile instances, such as the hack of Cellebrite, an Israeli mobile firm, with the hacker first channeling some documents directly to a journalist and subsequently publicly dumping the firm’s circumvention tools. Another even more notable example is the gargantuan hack against Retina and FlexiSpy—software companies marketing “stalkerware” to other firms and individuals for monitoring employees or children. Entering and then swiping source code, HR documents, and other files, the hackers leaked this information, which became the basis for a series of investigative pieces detailing how this spying software is used by “lawyers, teachers, construction workers, parents, jealous lovers” (Franceschi-Bicchierai and Cox 2017). Clearly following the path blazed by hacktivist predecessors, these hackers, going by name the Decepticons, also published a “How-to guide for aspiring hackers” with a respectful shout out to Phineas Phisher, noting: “we’d be remiss if we didn’t include Phineas Phisher’s articles, which are fantastic introductions. They cover things like how to stay safe and many of the basics, including many techniques we used to compromise FlexiSpy/Vervata/etc. So read them and soak them up” (Decepticons, 2017).

Some might be wondering whether the Shadow Brokers’ April 2017 dump of NSA hacking tools qualifies as a PIH under the rubric proposed here. Given available information, it’s hard to say. Journalists certainly mined the leaked data and tools to unveil

1 A more comprehensive history of the PIH would also need to examine other regions, such as Asia and the Middle East and especially Turkey home to a prolific hacktivist group, RedHack.

2 Personal Communication with the author.

Hack Back!

A DIY Guide



Artwork from Phineas Phisher's "HackBack: A DIY Guide."

new details about the use of exploits and malware by US intelligence, but evidence as to whether the data was acquired from a hack or by some other means remains circumstantial. According to Edward Snowden, this group—likely composed of nation state-backed hackers—infiltrated a staging server (itself a hacked server where the NSA would host and launch their tools) where they discovered

the tools left for the taking. This hack would not be “unprecedented.” But what is unprecedented is the publicness, the style of “publication,” as Snowden put it, of the material (2016).

That there is a connecting thread between Anonymous, Phineas Phisher, and the Decepticons is obvious, confirmed by the actors themselves—each subsequent hacktivist paying homage to their predecessor. In contrast, it is impossible to say definitively whether groups like Guardians of Peace, Guccifer 2.0, or Shadow Brokers were overtly or directly influenced by Anonymous. What is evident—and the recent hack and leak of Macron staff email provides another nugget of proof—is hackers will continue to rely on but also experiment with this method. And experimentation invariably leads to mutations. The PIH will continue to be used as it has been in the last few years: as an instrument for left-leaning hacktivism, statecraft, revenge and extortion, and geopolitical machinations; but as journalists develop new norms for reporting on leaks and as hackers become more sophisticated at launching and staging attacks—for instance, by successfully implanting false information in the leaks—the form will continue to surprise us with its myriad political effects and consequences. ■

E. GABRIELLA COLEMAN holds the Wolfe Chair in Scientific and Technological Literacy at McGill University. She is the author of *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton University Press, 2012) and *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Verso, 2014).

BIBLIOGRAPHY

- Anderson, Nate. 2010. “The ‘legal blackmail; business: inside a P2P settlement factory.” *Ars Technica*, September 29. Available at link.
- Berman, Dennis K. 2003. “Government Posts Enron’s E-Mail: Amid Power-Market Minutiae, Many Personal Notes Remain.” *Wall Street Journal*, October 6. Available at link.
- Decepticons. 2017. “Flexidie: brought to you by LeopardBoy and the Decepticons.” *Pastebin*. Available at link.
- Franceschi-Bicchierai, Lorenzo and Joseph Cox. 2017. “Inside the ‘Stalkerware’ Surveillance Market, Where Ordinary People Tap Each Other’s Phones.” *MotherBoard*, April 18 Available at link.
- Grieve, Tim. 2003. “The decline and fall of the Enron empire.” *Salon*, October 14. Available at link.
- Harris, Bev, 2003. *Black Box Voting Book*. <http://blackboxvoting.org/black-box-voting-book/>
- Menn, Joseph. 2011. “Cyberactivists warned of arrest.” *Financial Times*, February 4. Available at link.
- Phisher, Phineas. 2016. “Hack Back! A DIY Guide.” *Pastebin*. Available at link.
- Potok, Mark. “Neo-Nazi Threatmaker Accused of Working for FBI.” *Southern Poverty Law Center Hatewatch*, January 11. Available at link.
- Schwartz, John. 2003. “Computer Voting Is Open to Easy Fraud, Experts Say.” *New York Times*, July 24. Available at link.
- Schor, Elana. 2008. “US election: Tennessee politician’s son indicted for hacking into Palin’s email.” *The Guardian*, October 8. Available at link.
- Snowden, Edward (Snowden). “The hack of an NSA malware staging server is not unprecedented, but the publication of the take is. Here’s what you need to know: (1/x)”. 16 Aug 2016, 11:40 UTC. Tweet. Available at link.
- Zetter, Kim. 2014. “Experts Are Still Divided on Whether North Korea Is Behind Sony Attack.” *WIRED*, December 23. Available at link.

**the
political
meaning of
hacktivism**



Philosopher-kings or Fawkes masks? Ashley Gorham explores the truth-telling zeal of WikiLeaks and the lulzy opinions of Anonymous

IN LESS THAN A DECADE, hackers have gone from marginal political actors to talking points at presidential debates. Hillary Clinton's emails and Donald Trump's 400-pound hacker are only the most recent evidence of hacking's ascendance in the political sphere. Hacking's popularity has verged on infamy at times. Fears of foreign spying, "unpatriotic" leaks, and cybercrime abound. Accounts of WikiLeaks and Anonymous, two of the most famous hacktivist forces, have been colored by these concerns. Contrary to these negative accounts, hacktivism can be a legitimate and effective form of political action. However, not all hacktivism is the same. In this article, I seek to differentiate the hacktivism of WikiLeaks from that of Anonymous by articulating the models of politics the two forms of digital activism represent. WikiLeaks's fetishization of truth begets a technocratic politics, while Anonymous's emphasis on opinion encourages a more democratic practice. Understanding this distinction helps to illuminate the particular implications of their political action, which are obscured by the conflation of the two hacktivist groups.

The connection between truth and technocracy is at least as old as Plato. Plato's philosopher-kings's rule is based on their knowledge of the "Forms." Knowledge of the Form of the Good allows for knowledge of all observable things as worldly manifestations of the invisible Forms. To approach such knowledge, philosophers require a rigorous and technical education, which includes arithmetic, geometry, astronomy, and dialectic. Those who achieve knowledge of the Forms gain access to the Truth, which is superior to "mere opinion" because it is eternal and unchanging. It is self-sufficient and does not require input from "the people." Knowledge of the Forms offers a kind of blueprint for ruling; in the *Republic*, Socrates suggests, "there is no way a city can ever find happiness unless its plan is drawn by painters who use the divine model" (Plato 2004:500e1-e3). Plato compares the political leader to "the physician, weaver, and artist," all technocrats in the literal sense as it refers to "craftsmen," or "artists"

working with "passive material receptive to the impress of the Idea" (Wolin 2004:43). In the words of Hannah Arendt, "the philosopher-king applies the ideas [Forms] as the craftsman applies his rules and standards; he 'makes' his City as the sculptor makes a statue" (1958:227).¹

While Plato idealizes the technocratic regime of Truth of the philosopher-kings, he identifies "mere opinion" with "disorder" (Wolin 2004:35). According to Nadia Urbinati, Plato understood opinion as "the name of a view or a belief that cannot pass the bar of philosophical analysis" (2014:29). Suspicion of opinion runs throughout the canon of Western philosophy. Alexis de Tocqueville and John Stuart Mill caution against opinion's oppressive power, which Mill called the "yoke of opinion" (2006:14). Arendt is unusual among political thinkers in her defense of opinion. Arendt was critical of the "despotic character" of truth, writing:

The trouble is that factual truth, like all other truth, peremptorily claims to be acknowledged and precludes debate, and debate constitutes the very essence of political life. The modes of thought and communication that deal with truth, if seen from the political perspective, are necessarily domineering; they don't take into account other people's opinions, and taking these into account is the hallmark of all strictly political thinking (1993:241).

Unlike truth, opinion is fallible, but this is its value for Arendt because it makes room for democratic discourse and debate.

Although they do not rule according to their knowledge of the Truth, like Plato's philosopher-kings, WikiLeaks understands politics in terms of truth. There are at least three kinds of truth involved in WikiLeaks's politics: theoretical, mathematical, and political. WikiLeaks's political action centers on the "leak," or the transmission of classified, private, or otherwise secret information. Their model of leaking is rooted in the "cypherpunk" philosophy of their founder, Julian Assange.² In Assange et al.'s (2012) *Cypherpunks: Freedom and the Future of the Internet*, cypherpunks are described as "advocate[s] for the use of cryptography and similar methods as ways to achieve societal and political change" (2012:v). For WikiLeaks, cypherpunk thought represents a kind of theoretical truth; it is a blueprint for political action, which the organization seeks to implement technically through its "innovative, secure and anonymous" leaking submission system (WikiLeaks 2011). Assange believes his work with WikiLeaks has "given political currency to the traditional cypherpunk juxtaposition:

1 Plato's philosopher-kings are certainly not conventional technocrats. They do not possess a narrow expertise; in fact, they are by definition "lovers of wisdom."

2 For a description of the evolution of cypherpunk thought, see Levy (2001).

‘privacy for the weak, transparency for the powerful’” (Assange et al. 2012:7). Cryptography is itself grounded on mathematical truth; Assange has said, “it just happens to be a fact about reality, such as that you can build atomic bombs, that there are math problems that you can create that even the strongest state cannot break ... So there is a property of the universe that is on the side of privacy, because some encryption algorithms are impossible for any government to break, ever” (Assange et al. 2012:61–62).³ Finally, WikiLeaks views the content of the leaks themselves as political truths. In his article “Don’t Shoot Messenger for Revealing Uncomfortable Truths” (2010), Assange makes this point explicit, writing of WikiLeaks, “The idea ... was to use internet technologies in new ways to report the truth.” These three truths represent the idea behind, enabling form, and content of WikiLeaks’s leaks. The organization’s technocratic implementation of the theoretical truth of cypherpunk thought, based as it is on mathematical truth, facilitates the leaking of political truth in pursuit of “privacy for the weak, transparency for the powerful.”

Like WikiLeaks, Anonymous is also concerned with truth, but unlike WikiLeaks, their hacktivism reflects the centrality of opinion to politics. Although it is discussed far less than their commitment to free speech, opposition to censorship, and love of “the lulz,” opinion is the substance of both their internal communication and external actions.⁴ Before, during, and after operations, “Anons” correspond with one another almost continuously on IRC (internet relay chat), and through their discussions they form a community, as many become known to one another by their hacker handles. Multiple IRC networks and channels and Twitter accounts are active at all times. Hanna Pitkin once criticized Arendt’s concept of “the political” with its idealization of Athens by quipping, “what is it that they talk about together, in that endless palaver in the *agora*?” (1981:336). Online members of Anonymous seem to have created an unembellished version of this ideal as their continuous conversations run the gamut from the not serious at all to the extremely serious (and often both at the same time). The absence of official dogma allows for the coincidence of multiple and at times conflicting opinions.

Anonymous has staged protests against Scientology, Sony, and BART, and in support of WikiLeaks, the “Arab Spring,” and Occupy, among many others. In carrying out their operations, Anonymous employs a variety of tactics, including distributed denial of service (DDoS) attacks, website defacement, data dumps,

physical protest, press releases, consciousness-raising through videos, hacks, leaks, and various kinds of pranks (see Coleman 2014; Norton 2012). While they may not rise to the level of discourse, such tactics are expressive. They are better understood as expressions of opinion and prods to opinion formation and reformation than as edicts of truth. Both internally and externally, Anonymous is constantly undertaking the work of opinion formation and expression rather than allowing truth to do the work of politics for them. In this way, Anonymous engages in democratic *praxis*.

It is not that WikiLeaks’s hacktivism is incompatible with democracy; leaking can expose wrongdoing and often leads to positive change. Factual truth is essential to politics for a number of reasons, not least of which is that “facts inform opinions,” which means that “freedom of opinion is a farce unless factual information is guaranteed and the facts themselves are not in dispute” (Arendt 1993:238).⁵ The problem is that the technocratic fetishization of truth can have antidemocratic effects. Truth has, in Arendt’s words, a “despotic character” like that of the philosopher-kings: its rule is absolute (1993:241).⁶ By contrast, in “matters of opinion ... validity depends upon free agreement and consent; they are arrived at by discursive, representative thinking; and they are communicated by means of persuasion and dissuasion” (Arendt 1993:247).⁷ Arendt notes that “the shift from rational truth to opinion implies a shift from man in the singular to men in the plural” (1993:235). While opinion entails community, truth requires only a single representative. Thus, when politics is understood primarily in terms of truth, the *demos* may be devalued.

This danger echoes in the internal politics of WikiLeaks itself. Famously, Assange is alleged to have suspended Daniel Domscheit-Berg from WikiLeaks for “disloyalty, insubordination and destabilization [sic] in a time of crisis” (Domscheit-Berg and Klopp 2011:227). When WikiLeaks volunteer Herbert Snorrason questioned Domscheit-Berg’s suspension, Assange is said to have responded, “I am the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier and all the rest. If you have a problem with me, piss off” (Zetter and Poulsen 2010). Elsewhere, Assange has admitted to considering himself “a bit of a vanguard” (Assange et al. 2012:84).

Anonymous’s emphasis on opinion



3 Incidentally, as Arendt notes, “Plato...believed that mathematical truth opened the eyes of the mind to all truths” (1993:230).

4 Gabriella Coleman defines “the lulz” as “a deviant style of humor and a quasi-mystical state of being” (2014:2).

5 That truth is necessary in politics amounts to a truism, and yet “No one has ever doubted that truth and politics are on rather bad terms with each other” (Arendt 1993, 227). The rise of “alternative facts” is a reminder of just how important, and fraught, the relationship is.

6 Interestingly, Assange has described Plato as “a bit of a fascist” (Baird 2013).

7 “Representative” thinking involves “considering a given issue from different viewpoints,” which requires “being and thinking in my own identity where actually I am not” (Arendt 1993:241).

helps to insulate the collective against the tyranny of philosopher-kings. Opinion is dependent on a community (both real and imagined) for its validity; lacking the “force of truth,” it relies on consent (Arendt 1993:240). In this way, opinion entails a community by consent. Understood in terms of voluntary engagement rather than consensus, Anonymous can be said to be such a community by consent. Gabriella Coleman has described Anonymous as a “wily hydra”—a loosely coordinated collective of changing (and at times conflicting) associations without “a stable hierarchy or a single point of control” (2014:48,75). It is perhaps best understood as a “do-ocracy,” or a system “rule[d] by sheer *doing*,” in which “Individuals propose actions, others join in (or not), and then the Anonymous flag is flown over the result” (Norton 2012; see also Coleman 2014:75). As Coleman points out, “some Anons are more active and influential than others—at least for limited periods” (2014:75). However, no one could ever say that he or she was “the heart and soul of this organization, its founder, philosopher, spokesperson, original coder, organizer, financier and all the rest” in reference to Anonymous. Opinion’s communal nature demands as much.

There is a way in which WikiLeaks and Anonymous are both technocratic and both democratic: both embrace technological expertise and have expressed a commitment to democracy. These similarities help explain why the two are so frequently grouped together and the distinctions between them collapsed. Yet, while both WikiLeaks and Anonymous have technocratic and democratic elements, their participation in the categories is not uniform. Their differing relationships to truth and opinion mark a definitive divide between the groups. The two can function well together, working to temper each other’s excesses, but from the perspective of democracy, WikiLeaks’s excesses are more troubling than those of Anonymous. The pitfalls of WikiLeaks’s model of politics surfaced during the recent U.S. presidential election, as the organization’s leaks appeared to target only one of the candidates, thus implicitly endorsing the other. While both Anonymous and WikiLeaks seek to influence democratic discourse, WikiLeaks approaches politics from a position outside of the *demos*, in the role of truth-teller. Eliding the influence of its own curatorial opinions on its truths, WikiLeaks opens itself up to the charge of manipulation. The inability, or unwillingness, of WikiLeaks to recognize

the relationship between its truths and its opinions leads the organization to risk harming the system it claims to serve. ■



ASHLEY GORHAM is a doctoral student in political science at the University of Pennsylvania.

BIBLIOGRAPHY

- Arendt, Hannah. 1958. *The Human Condition*. Chicago, IL: University of Chicago Press.
- . 1993. “Truth and Politics.” In *Between Past and Future: Eight Exercises in Political Thought*, pp. 227–264. New York: Penguin.
- Assange, Julian. 2010. “Don’t Shoot Messenger for Revealing Uncomfortable Truths.” *The Australian*, December 8. <http://www.theaustralian.com.au/in-depth/wikileaks/dont-shoot-messenger-for-revealing-uncomfortable-truths/story-fn775xjq-1225967241332>
- Assange, Julian, Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann. 2012. *Cypherpunks: Freedom and the Future of the Internet*. New York, NY: OR Books.
- Baird, Julia. 2013. “Assange as Tyrant?” *New York Times*, September 14. <http://www.nytimes.com/2013/09/15/opinion/sunday/assange-as-tyrant.html>
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York, NY: Verso Books.
- Domscheit-Berg, Daniel, and Tina Klopp. 2011. *Inside WikiLeaks: My Time with Julian Assange at the World’s Most Dangerous Website*. Translated by Jefferson Chase. New York, NY: Crown.
- Levy, Steven. 2001. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. New York, NY: Viking.
- Mill, John Stuart. 2006. *On Liberty and The Subjection of Women*. Edited by Alan Ryan. New York, NY: Penguin.
- Norton, Quinn. 2012. “How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down.” *Wired*, July 3. https://www.wired.com/2012/07/ff_anonymous/
- Pitkin, Hanna Fenichel. 1981. “Justice: On Relating Private and Public.” *Political Theory* 9(3):327–352.
- Plato. 2004. *Republic*. Translated by C. D. C. Reeve. Indianapolis, IN: Hackett.
- Urbinati, Nadia. 2014. *Democracy Disfigured: Opinion, Truth, and the People*. Cambridge, MA: Harvard University Press.
- WikiLeaks. 2011. “About: What is WikiLeaks?” May 7. <https://wikileaks.org/About.html>
- Wolin, Sheldon S. 2004. *Politics and Vision: Continuity and Innovation in Western Political Thought*. Princeton, NJ: Princeton University Press.
- Zetter, Kim, and Kevin Poulsen. 2010. “Unpublished Iraq War Logs Trigger Internal WikiLeaks Revolt.” *Wired*, September 27. <http://www.wired.com/2010/09/wikileaks-revolt/>

SURVIVAL OF THE

In January 1993, as then-President Elect Clinton was preparing to take office, a now-familiar Pennsylvania Avenue nemesis reared its ugly head: the email scandal. A young, exuberant presence during the campaign, Clinton's administration promised to inaugurate a new era for the White House. Technology would be centrally implicated in this new phase: the Clinton Administration would be the first to have its own website, the first to use email to communicate with the public. But though the White House didn't start using the internet in earnest until 1992, White House staffers had been using email to communicate internally since the Reagan era. And the Bush Administration did not want to leave records of its emails on computers that would be used by Clinton staffers.

Judge Charles B. Richey issued a restraining order preventing the Bush White House from destroying its records, shooting down a memo from the President's counsel saying they had the authority to do so. White House staffers framed the issue as a problem of resources: they needed to open up hard drive space for the new administration's files on White House computers. But it was quickly dismissed by Richey, who said, "As a practical matter, one does not need to know much about computers to know that saving this information is not going to bring the government to its knees" (Gerstenzang, 1993). Though the law prohibiting destruction of presidential records doesn't cover ephemera like scratch pads, informal notes, and visitor logs, by issuing the order Richey designated email a part of the public record of the administration (Bearman, 1994). "History is full of instances where the outgoing president has decided to erase, burn or destroy all or substantially all presidential or Executive Office of the President records before the end of his term," Judge Richey wrote in his forceful statement issuing the order (New York Times News Service, 1993).



At its heart, the legal battle over email was about secrecy: Should the private communications of public officials be transparent to the public, and thus their political opponents? The conflict in the 1990s built upon a series of email scandals from previous administrations. As early as 1986, only a few years after the White House started using email, John Poindexter and Oliver North destroyed 5,000 email messages in an attempt to cover up the Iran-Contra scandal. The FBI found back-up copies and used them to piece together the affair; these emails became a key part of the evidence evaluated by the Tower Commission. In 1989, on President Reagan's last day in office, the National Security Archive filed a lawsuit to prevent the White House from deleting its email backup tapes. They were successful in doing so, and followed their suit with a case against President Bush toward the end of his administration. The Archive expanded its petition to the Court this time, asking them to formally rule that email falls within the jurisdiction of laws that require presidential administrations to hold on to their records (National Security Archive, 1995).

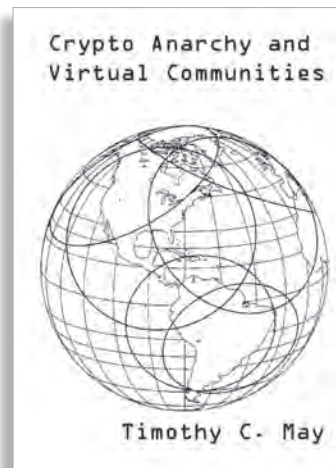
These early cases established that White House

John Poindexter and Oliver North destroyed 5,000 email messages in an attempt to cover up the Iran-Contra scandal

Should we have privacy for the weak and transparency for the powerful? Sarah Myers West reminds us that we've been agonizing over this question since at least the 1990s, when the cypherpunks first started discussing it.

CRYPTIC

THE CYPHERPUNKS
Wired Magazine,
May/June 1993.



CRYPTO ANARCHY AND VIRTUAL COMMUNITIES
Tim May's classic manifesto from 1994

The "cypherpunks" sought to bring into being a world in which it would be possible to share and spread information about government activities while remaining secret

emails generally fall within the bounds of public records laws. But the leaks, hacks, and scandals that marred the 2016 presidential elections suggest the underlying debate over the function of secrecy within a democratic government is ongoing. The elections raised many important questions about state secrecy: Should cabinet officials handling sensitive information be allowed to use private servers for their emails? Should the FBI announce when a presidential candidate is under investigation days before an election? How do we make sense of the practices of strategic leaking that are endemic to Beltway politics?

One of the leaks in particular has persistently remained at the center of the post-election debate: the penetration of the Democratic National Committee's (DNC) server by the hacker Guccifer 2.0, leading to the release of the DNC emails through WikiLeaks. The DNC hack made visible the inner workings of a political party, raising questions about whether its secret machinations are compatible with the tenets of liberal democracy. At first, the leak seemed to force accountability within the Democratic Party for how it selects presidential candidates. But the months following have

led to murkier questions over the true identity of the leaker and possible motivations behind the hack. As intelligence officials, congressional leaders, and journalists grapple with the fallout, the public is left grasping for a clearer view of what really transpired. Rather than making the secrets of government transparent and legible, in the end the DNC leak rendered them all the more opaque.

These questions about transparency and secrecy were central to the workings of a group of technologists in the early 1990s, and perhaps by looking at their debates we might make sense of our current situation.

The "cypherpunks," as they called themselves, sought to bring into being a world in which it would be possible to share and spread information about government activities while remaining secret, using public key encryption to verify their authenticity while protecting the identity of the leaker.

Debates among the cypherpunks during the Bush email scandal suggests this group of technologists was at the vanguard of thinking through the challenges of government secrecy. Though they don't reach any firm conclusions—and in fact differed considerably



in opinions on which mechanisms for transparency would be preferable—at the advent of the White House’s adoption of the internet the cypherpunks were already teasing out the nuances of the implications of networked technologies for the proper functioning of government. These nuances prefigure many of the tensions that reached a climax during the 2016 elections as a result of the DNC hack.

PRIVACY FOR THE WEAK, TRANSPARENCY FOR THE POWERFUL

In his *Crypto Anarchist Manifesto*, Timothy C. May, cofounder of the cypherpunks, remarked, “Computer technology is on the verge of providing the ability for individuals and groups to interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other.... These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation” (May 1992). Reacting to repeated attempts by state officials throughout the 1970s and 1980s to mask the inner workings of government—including those of the officials involved in the Iran–Contra scandal—May

envisaged the development of a trade in national secrets, making it possible for whistleblowers to uncover corruption in government without risking harm to their physical selves.

May and other cypherpunks were inspired by texts like the 1985 science fiction novel *Ender’s Game* by Orson Scott Card. In the book, two children post political essays anonymously to a global communication system under the pseudonyms Demosthenes and Locke, winning over policy experts and ascending to the world stage despite their youth. Anonymity enabled them to overcome the disparities in power and reputation accorded to their age: it leveled the playing field such that arguments were judged based on the content of their information rather than by the reputation of the speaker. May’s vision builds upon this by seeking to establish a market in information separated from its institutional context. In so doing, May thought anonymous leaks could check the power of institutions like governments and corporations, redistributing it back to individuals.

Though Card’s vision is very nearly an embodiment of Habermasian discourse, May’s interpretation is more akin to a capitalist marketplace of ideas than a rationalized public sphere. “Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put

TWO IMAGES OF HEROIC SILENCE
Left: Ollie North Shreds for America (provenance unknown);
Right: “If you talk too much, this man may die.” U.S. Office of War Information, 1943.

“The burden should not be on individuals to constantly be open to scrutiny to demonstrate their innocence”

into words and pictures,” he said, leaving it up to the invisible hand of the market to define the value of that material (May 1992).

May extended these principles to the debate over White House emails. In an email to the cypherpunk listserv about the Bush administration case, he declared, “Individuals, corporations, clubs, and perhaps even government agencies should have the right to secure and private communications. The only caveat with the “perhaps” for the government is that it, in theory, belongs to ‘us’” (Cypherpunk listserv, January 21, 1993). Though this statement is suggestive of some sort of carve-out for transparency in his philosophy for encryption, he quickly closed up that loophole: “I find it unsettling when people of one political party are screaming for access to the private diaries and papers of members of the other party. Citing Ollie North’s crimes is no excuse” (Cypherpunk listserv, January 21, 1993). The vision May has articulated across these texts is suggestive of a philosophy not of mandated transparency, but of a marketplace of secrets, one in which the onus is on the secret-holder to maintain their own privacy through the use of encryption, and woe to those who wield it ineffectively.

Other cypherpunks proffered different views, however, raising a number of caveats in their discussion of the Bush emails that tease out nuances in the debate over government secrecy or transparency. Most turned to principles of liberal democracy and the concept of the social contract as justifications for a constraint on government secrecy: though institutions (individuals, groups of individuals, and companies) should have the right to private communication, they argued, those who act upon the consent of the governed must have some degree of transparency to ensure they stay accountable to the public.

As Eric Fogleman put it in a post on the Cypherpunk listserv, a mailing list through which the network of technologists communicated, “The right of government employees to private communication is limited by one important factor: many of these individuals are empowered to use force against citizens, and they responsible [sic] for justifying the use of this force.... Anyone given this kind of power has a heavy burden of proof and had better be able to prove beyond a shadow of doubt that their actions are justified. The burden should not be on individuals to constantly be open to scrutiny to demonstrate their innocence, but on those with the power to suspend individual rights” (Cypherpunk listserv, January 21, 1993). Fogleman’s statement is akin to an early version of a maxim frequently stated by fellow cypherpunk Julian Assange: “Privacy for the weak, transparency for the powerful.”

Many cypherpunks seemed to agree with this view but, as later emails suggest, at this point in time these cypherpunks’ views fit within democratic frameworks of accountability rather than the kind of radical transparency Assange later espoused. Few cypherpunks at that moment built upon May’s expressed vision for a stateless market in the trade of secrets. Responding to May’s email, Dave Deltorto wrote that though Oliver

North should have access to strong cryptography, he should be required to open his files if under criminal investigation. Deltorto later elaborated on this argument, saying that while documents produced by public officials on public time and in pursuit of public policy should be subject to scrutiny, their private communications on their own time should be excluded from this rule. He added, “HOWEVER, if such persons then turn around and abuse this freedom by abusing the public trust in those contexts (i.e., if Ollie North started communicating with NSA officials through CompuServe to order illegal shipments of money to CIA agents in Peruvian cocaine cartels), they should, by virtue of their positions of public trust be subject to the same (presumably high) levels of scrutiny as they are now—Congressional, OMB, GSA, FBI investigations, etc.” (Cypherpunk listserv, January 21, 1993). Deltorto’s argument relies upon the existence of government institutions to ensure officials act ethically, reforming from within rather than from without.

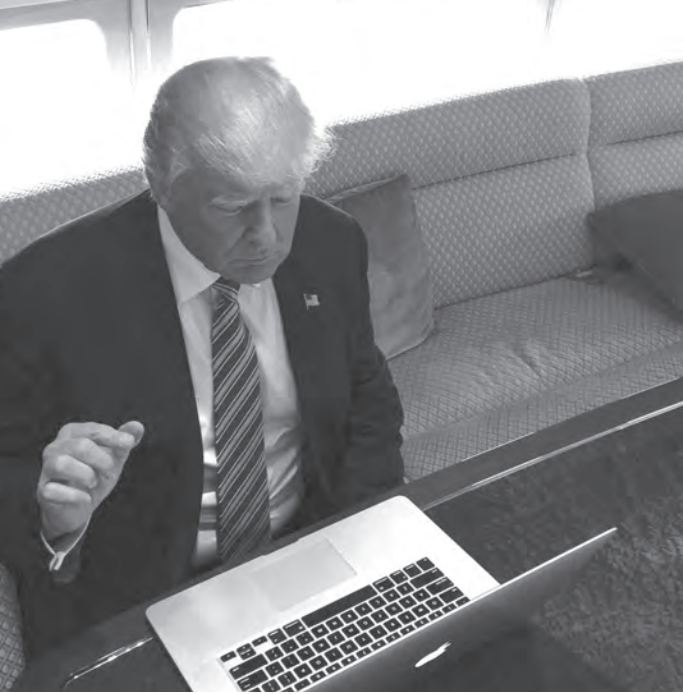
Or, as a cypherpunk going by the handle Lefty put it, “A *private* institution should have a right to *private* communications. The White House is *not* a *private* institution” (Cypherpunk listserv, January 22, 1993).

SURVIVAL OF THE CRYPTIC

May later elaborated on his vision in a post to the Cypherpunk listserv titled “Introduction to BlackNet.” “BlackNet is in the business of buying, selling, trading and otherwise dealing with *information* in all its many forms,” May said. “We buy and sell information using public key cryptosystems with essentially perfect security for our customers. Unless you tell us who you are (please don’t!) or inadvertently reveal information which provides clues, we have no way of identifying you, nor you us” (Cypherpunk listserv, August 17, 1993).

The concept of the BlackNet was particularly amenable to a trade in state secrets, encouraging whistleblowers in government to adopt anonymity to render government more transparent through strategic leaks. Moreover, it would create an impetus for government officials to think about the protection of their privacy: “BlackNet believes it is solely the responsibility of a secret holder to keep that secret—not the responsibility of the State, or of us, or of anyone else who may come into possession of that secret. If a secret’s worth having, it’s worth protecting,” May wrote. Technical savvy thus becomes both a means of facilitating transparency and a precondition for secrecy, a Machiavellian kind of survival of the cryptic.

The DNC leaks are in many respects a realization of May’s ideas: the DNC hack demonstrated in stark relief the consequences of public officials’ ignorance about their digital security. And in a sense, the organization WikiLeaks, which aided in the distribution of the DNC emails, is an embodied version of the BlackNet, with the notable difference that it doesn’t operate purely on market logic. WikiLeaks’ choice to act strategically in the timing of the emails’ release resulted in an outcome that ran counter to May’s expressed intentions:



the leaks asserted the dominance of geopolitical power rather than subverting it. The fingerprints of state-linked teams of hackers, not individual vigilantes, appear to be behind the hacks, which fit into a campaign of disinformation intended to sway the results of the election. The outcome was a diminution of individual agency, rather than its enhancement: a far cry from the vision May outlined in his manifesto.

SECRETS AND THE STATE

In “Sociology of Secrecy and of Secret Societies” (1906), Georg Simmel anticipated the morass that could surround government secrecy: “Secrecy secures, so to speak, the possibility of a second world alongside of the obvious world, and the latter is most strenuously affected by the former” (Simmel 1906: 462). Secrecy conveys on the secret-holder an exceptional position, he said, because of the fallacy that everything secret is somehow essential and significant. “Just as the moment of the disappearance of an object brings out the feeling of its value in the most intense degree,” he said

(Simmel 1906: 465), the revelation of secret knowledge can convey a sense of importance that may be outsized compared with the content of the information itself, a dynamic leveraged by the strategic use of leaks by actors seeking to sway the results of the election.

Simmel was adamant that in and of itself, secrecy “has nothing to do with the moral valuations of its contents” (1906: 462); it can be used by the benevolent to embrace their highest virtues, even as it is used by the malevolent to hide the darkest of evil acts. But he predicted that too much secrecy would make modern life intolerable: the realm of conspiracy, where truth could not be separated from fiction with any kind of objectivity, would be an undesirable state for any society to be in. As such, democracies are bound to regard transparency as a favorable condition, Simmel argued, following from the idea that every citizen is responsible for informing themselves about their government as a precondition for participating in it.

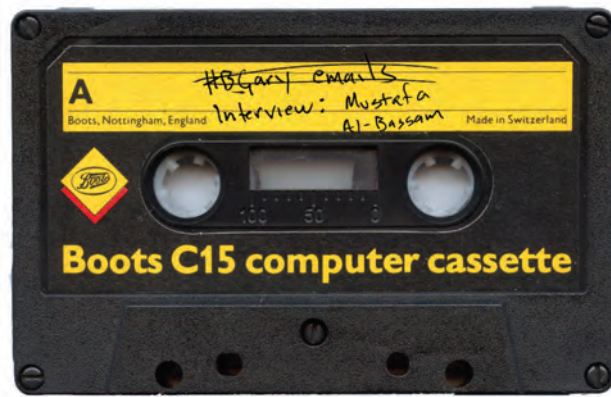
A decade before the formation of WikiLeaks and two decades before the DNC hack, the cypherpunks were already putting Simmel’s sociological predictions to the test, anticipating how government secrecy and transparency would be transformed in a networked age. Despite their differences, the cypherpunks shared a vision of the redistribution of power through technology away from institutions and back to individuals.

The DNC leaks make clear that this vision has not been realized just yet: the strategic revelation of government information made the workings of political officials more opaque, rather than legible to the public. Both the hacks by Guccifer 2.0 and strategic leaks by government officials contributed to this opacity. This is an indication of the limits of transparency: while it remains a favorable condition for democracy, whether or not it will effectively aid the public in democratic deliberation depends very much upon by whom and for whom transparency is working. ■

SARAH MYERS WEST is a PhD Candidate and the Wallis Annenberg Graduate Research Fellow at the USC Annenberg School for Communication and Journalism.

BIBLIOGRAPHY

- Bearman, D. (1994). “The Implications of *Armstrong v. the Executive Office of the President* for the Archival Management of Electronic Records.” In *Electronic Evidence: Strategies for Managing Records in Contemporary Organizations*, (pp 118-144). Pittsburgh, PA: Archives & Museum Informatics.
- National Security Archive. (1995). “White House E-mail”. *National Security Archive*, November 22. http://nsarchive.gwu.edu/white_house_email/#LIST
- Gerstenzang, J. (1993). “White House Told to Copy Records: Archives: In Fight over Computer Files, Appellate Panel Wants Bush’s Staff to Back Up Notes and Memos before Erasing Anything.” *Los Angeles Times*, January 16. http://articles.latimes.com/1993-01-16/news/mn-1353_1_white-house
- May, Timothy. C. (1992). “The Crypto Anarchist Manifesto.” *Cypherpunk Mailing List*. <http://www.activism.net/cypherpunk/crypto-anarchy.html>
- New York Times News Service. (1992). “Administration Aides May Destroy Telephone Logs, Counsel Maintains.” *The Baltimore Sun*, November 21. http://articles.baltimoresun.com/1992-11-21/news/1992326024_1_bush-white-white-house-telephone-logs
- Simmel, Georg. (1906). “The Sociology of Secrecy and of Secret Societies.” *American Journal of Sociology* 11(4):441-498.
- Young, John. (2013). “Cypherpunks Archive 1992-1998.” *cpunks.org*, September 6. <https://lists.cpunk.org/pipermail/cypherpunks/2013-September/000741.html>



Interview: Mustafa Al-Bassam

Limn talks with security expert **Mustafa Al-Bassam** (a.k.a “**tflow**”) about the responsibility for information security, the incentive problems it creates and the available solutions.

Gabriella Coleman: Based on what you’ve seen and reported do you think we (not just lay people, but experts on the subject) are thinking clearly about vulnerability? Is our focus in the right place (e.g. threat awareness, technical fixes, bug bounties, vulnerabilities disclosure), or do you think people are missing something, or misinterpreting the problem?

Mustafa Al-Bassam: Based on the kind of vulnerabilities that we [LulzSec] were exploiting at Fortune 500 companies, I don’t think that there is a lack of technology or knowledge in place to stop vulnerabilities from being introduced, but the problem is that there is a lack of motivation to deploy such knowledge. We exploited extremely basic vulnerabilities such as SQL injection, in companies like Sony, that are quite easy to prevent.

I believe the key problem is that most companies (especially those that are not technology companies – like Sony) don’t have much of an incentive to invest money in making sure their systems are vulnerability-free, because security isn’t a key value proposition in their business model, it’s merely an overhead cost to be minimized. Sony fired their entire security team shortly before they got hacked over 30 times in 2011. For such companies, security only becomes a concern for them when it becomes a PR disaster. So that’s what LulzSec did: make security a PR disaster.

We’ve seen this before: when Yahoo! was breached in 2014, the CEO made the decision not to inform customers of the breach. Because it would have been a PR disaster for them, that may have seen them lose customers to their competitors, causing them to lose money.

That begs the question: how can we expect companies to do the right thing and inform customers of breaches, if doing the right thing will cause them to lose money? And so, why should companies bother to invest in keeping their systems free of vulnerabilities, if they can simply brush compromises under a carpet? After all, it is the customer that loses from having their information compromised, rather than the company, as long as the customer keeps paying.

So I think if we can incentivize companies to be more transparent about their security and breaches, customers can make better-informed decisions about which products and services to use, making it more likely for companies to invest in their security. One way this might happen in the future is through the rise of cybersecurity insurance; more and more companies are signing up to cybersecurity insurance. A standard cybersecurity insurance claim policy should require the company to disclose to its customers when a breach occurs. That way, it makes more economic sense for a company to disclose breaches and also invest in security to get lower insurance premiums or avoid PR disasters.

GC: I wanted to ask about the rise of cybersecurity insurance and whether major firms all already have purchased policies, what the policies currently look like, and whether they actually prevent good security since the companies rely on insurance to recoup their losses?

Christopher Kelty: Yes, I don’t actually understand what cybersecurity insurance insures against— does

it insure brand equity? Does it insure against government fines? Lawsuits against a corporation for breach of duty? all of these things? Just curious.

GC: Exactly, I don't think many of us have a sense of what this insurance looks like and if you can give us a picture, even a limited picture of what you know and how the insurance works, that would be a great addition to our issue.

MAB: The current cybersecurity insurance market premium is \$2.5 billion but it's still early stages because insurance companies have very little data on breaches to be able to calculate what premiums should be (Joint Risk Management Section 2017: 9). As a result, premiums are quite high and too expensive for small and medium sized businesses, and this will continue to be the case until cybersecurity insurance companies get more data about breaches to properly calculate the risks.

Cybersecurity insurance has been used in several high-profile breaches, most notably Sony Pictures which received a \$151 million insurance payout for its large internal network breach alleged to be by North Korea (Joint Risk Management Section: 4).

These policies cover a wide range of losses including costs for ransomware payments, forensic investigations, lost income, civil penalties, lost digital assets, reputational damage, theft of money and customer notification.

I think in the long-term it's unlikely that companies will adopt a stance where they stop investing in security and just rely on the insurance to recoup losses, because insurance companies will have a concrete economic interest to make sure that payouts happen as rarely as possible, and that means raising the premiums of companies that constantly get breached until they can't ignore their security problems. Historically, this economic interest is shifted to the customer because it's usually the customer that loses when their data gets breached and the company doesn't report it.

If anything, I believe that cybersecurity insurance will make companies more likely to do the right thing when they are breached and inform customers, because the costs of customer notification and reputational damage would be covered by the insurance. At the moment if a company does the right thing and informs their customers of a breach, the company suffers reputational damage, so there is little incentive to do the right thing. This will prevent incidents from occurring such as when Yahoo! failed to disclose a data breach affecting 500m customers for over two years (Williams-Alvarez 2017).

CK: I wonder if there is more of a spectrum here— from bug bounties to vulnerabilities equities processes (VEP) to cybersecurity insurance— all of them being a way to formalize the knowledge of when and where vulnerabilities exist, or when they are exploited. What are the pros and cons of these different approaches (I can imagine that a VEP is really overly bureaucratic and unenforceable, whereas insurance might produce its own incentives to exploit or over/under-report for financial gain). Any thoughts on this?

MAB: Bug bounties and cybersecurity insurance policies are controlled purely by the market and are an objective way to measure the economic value or impact of vulnerabilities, whereas VEP is a more subjective

process that is subject to political objectives.

In theory VEP should be a safeguard to be used situations where it is in the public interest to disclose vulnerabilities that may otherwise be more profitable to exploit, but this is not the case in practice. Take the recent WannaCry ransomware attack for example, which used an exploit developed by the National Security Agency, and affected hundreds of companies around the world and the UK's National Health Service (NHS). You have to ask if the economic and social impact of that exploit falling in the wrong hands was really worth all the intelligence activities that the NSA used it for. How many people died because the NHS couldn't treat patients when their systems were offline?

GC: Do you have a sense of what the US government (and others around the world) are doing to attract top hacker talent—for good and bad reasons? Should governments be doing more? Should it be an issue that we (in the public) know more about?

MAB: In the UK, the intelligence services like the Government Communications Head Quarters (GCHQ) run aggressive recruitments campaigns to recruit technologists. Even going so far as to graffiti 'hipster' adverts on the streets of a techy part of London (BBC NewsBeat 2015). They have to do this because they know that their pay is very low compared to London tech companies. In fact, Privacy International – a charity which fights GCHQ – will pay you more to campaign against GCHQ than GCHQ will pay you to work for them as a technologist.

So in order to try to recruit top tech talent, they have to try and lure people in by the promise that the work will be interesting and "patriotic", rather than it paying well. That is obviously becoming a harder line to toe though, because the intelligence agencies are less popular with technologists in the UK than ever, given the government's campaign against encryption. Their talent pool is extremely limited.

What I would actually like to see however, is key decision makers in government becoming more tech savvy themselves. Technology and politics are so intertwined these days that I think it's reasonable that at least a few Members of Parliament should have coding skills. Perhaps someone should run a coding workshop or class for interested Members of Parliament?

CK: I have trouble understanding how improved technical knowledge of MPs would lead to better political decisions if (given your answer to the first question) all the incentives are messed up. This is a very old problem of engineers vs. managers in any organization. The engineers can see all the problems and want to fix them; the managers think the problems are different or unimportant. Just to play devil's advocate, is it possible that hackers, engineers, or infosec researchers also need a better understanding of how firms and governments work? Is there a two-way street here?

MAB: I mean this in a more general sense: politicians make poor political decisions when they deal with technical information security problems they don't understand, for example with the recent encryption debate. In the UK, the Investigatory Powers Bill was recently passed, which allows the government to force communications platforms based in the UK to backdoor their products if they use end-to-end encryption.

Luckily most of these platforms aren't based in the UK, so it will have little impact. But this has a harmful effect on the UK technology sector, as no UK technology company can now guarantee that their customer's communications are fully secure, which means UK tech firms are less competitive.

A classic example of poor political decisions in dealing with such problems is the EU cookie law, which requires all websites to ask users before they place cookies on their computers (The Register 2017). In theory it sounds great but in practice most users always agree and click yes because the request dialogs are disruptive to their user experience. Even so, a saner way to implement such a policy would be to require the few mainstream browsers to only set website cookies after user approval, rather than ask millions of websites to change their code.

There are already plenty of hackers and engineers who are involved in politics, but there are very few politicians who are involved in technology. Even when engineers consult with the government on policies, their advice is often ignored, as we have seen with the Investigatory Powers Bill.

MUSTAFA AL-BASSAM (“tflow”) is a doctoral researcher at the Department of Computer Science at University College London. He was also one of 6 core members of the hacking collective LulzSec.

BIBLIOGRAPHY

- BBC News Beat. (2015). “Spy agency GCHQ facing fines for ‘hipster’ job adverts on London streets.” November 27th. <http://www.bbc.co.uk/newsbeat/article/34941261/spy-agency-gchq-facing-fines-for-hipster-job-adverts-on-london-streets>
- Joint Risk Management Section of the Society of Actuaries. (2017). “Cybersecurity: Impact on Insurance Business and Operations.” Report by Canadian Institute of Actuaries, Casualty Actuary Society, the Society of Actuaries. <https://www.soa.org/sections/joint-risk-mgmt/cyber-security-impact.pdf>
- The Register. (2017). “Planned ‘cookie law’ update will exacerbate problems of old law – expert.” March 1st. https://www.theregister.co.uk/2017/03/01/planned_cookie_law_update_expert/
- Williams-Alvarez, Jennifer. (2017). “Yahoo general counsel resigns amid data breach controversy.” *Legal Week*, March 2nd. <http://www.legalweek.com/sites/legalweek/2017/03/02/yahoo-general-counsel-resigns-amid-data-breach-controversy/>

Hacking/Journalism

Philip Di Salvo explores the trading zone between journalism and hacking.



JOURNALISM AND HACKING ARE GETTING closer in recent times. WikiLeaks, the Snowden case and the other published “megaleaks” have blurred the boundaries between newsrooms and hackers and inspired the rise of a hybrid form of reporting, where elements historically associated with hacking are now also visibly involved in journalism. This hybridization is the result of a process of boundary-crossing, whose most visible manifestation is in the adoption of new technologies. For instance, reporters increasingly rely on encryption tools to protect their sources and their work. Whistleblowing cases have been where this process has taken place in the most extensive way.

Whistleblowers have always supplied

investigative reporters with leaks, leads, and documents. The notable US instances from the 70s, like the Watergate and the Pentagon Papers cases, established whistleblowing-led journalism and made it mainstream and part of the popular record. The act of blowing the whistle hasn’t changed much since. A substantial game changer was WikiLeaks and the digital “megaleaks” it published starting from 2010. WikiLeaks’ Afghan and Iraqi War Logs, together with the Cablegate leaks, were an unprecedented novelty for journalism: they were composed of a hundred thousand documents in digital format that were leaked through encrypted channels to a hacker organization by Chelsea Manning, a US soldier

turned whistleblower with cultural ties to the hacking community. When it comes to journalistic and newsroom practices, the most disruptive change came when WikiLeaks began to partner with major news organizations to publish material; encryption played an enabling role in that whistleblowing. The WikiLeaks and journalists “consortium” represented a turning point in the relationship between journalism and hacking and it was able to put hackers and reporters at the same table, working jointly by sharing goals, skills, tools and practices. On that occasion, WikiLeaks contributed the source material and the technology, a resource that newspapers didn’t have at the time, while journalists brought their editorial skills and knowledge and, moreover, access to their audiences and influence.

In 2013 the Snowden case strengthened further the connection between hackers and journalists. Whistleblower Edward Snowden had strong affinities with the hacking community; the subjects of the leak – surveillance and cybersecurity – were core issues for hackers and, once again, encryption tools played a fundamental part in facilitating communication between the source and the journalists. Allegedly, Glenn Greenwald risked losing the story of the decade by not following Snowden’s request to communicate via safer channels. The debate about encryption that followed the Snowden case inspired more journalists and media outlets to adopt cybersecurity strategies and practices in order to better protect their work in times of pervasive digital surveillance. At the same time, other similar hacking-influenced instances of journalism based on digital leaks have also multiplied: Offshore Leaks (or the “Panama Papers”, “Swiss Leaks” and “Luxembourg Leaks”), published by the International Consortium of Investigative Journalists (ICIJ) and the “Drone Papers”, published by *The Intercept*. These cases helped set new standards for reporting on leaked material and showed the potential of a proactive attitude towards encryption.

As Baack argues (2016), digital leaks have now become normalized for



"Everybody Needs a Hacker"

PHOTO BY ALEXANDRE DULAUNOY / FLICKR CC / BY-SA 2.0

contemporary journalism and, because of the recurring presence of hackers and their technology, it is possible to look at some of these instances in order to describe how journalism is becoming more like hacking. The encryption tools used by Snowden and Greenwald to communicate with one another, for instance, exemplifies how journalists and reporters are now routinely embedding traditional hacking tools within their toolbox. Pretty Good Privacy (PGP) encryption software, the Off-the-record (OTR) encryption chatting protocol, and the mobile app Signal are now commonly included in the journalism toolbox; digital security literacy is now directly associated with the duty of protecting sources in the digital era. WikiLeaks pioneered a peculiar tactic to digital whistleblowing with its own online encrypted anonymizing submission

system, whose approach is now used, via the hacker-coded GlobalLeaks and SecureDrop open source software, also by several major news organizations such as *Associated Press*, *Washington Post*, *The Guardian* and *Vice*, among others. Encryption has now become a crucial strategy for reporters in need of a safe digital environment, or to apply "data disobedience" to shield their work (Brunton & Nissenbaum, 2015: 62).

The adoption of encryption in journalism has created a hybridization of practices between hackers and journalists that can be described as a "trading zone" (Galison, 1997; Lewis and Usher, 2014). "Trading zones" are symbolic spaces where actors hailing from different backgrounds work with shared purposes. For hackers, encryption has always held connotations of political resistance and the stress on privacy protection and anonymity safeguards is often part of the definition of the identity of hackers as well. For journalists encryption helps protect not only themselves and their work, but also their sources, giving them robust safeguards and protection from tracking and retaliation. In their tripartite analysis, Coleman and Golub (2008) have identified "cryptofreedom" to indicate how encryption is used by hackers as one "moral expression of hacking." In the "trading zone" between hackers and journalists what is being adopted by the latter is an approach to technology—and encryption tools in particular—that wasn't at all

routinized in journalism before WikiLeaks and Snowden. Charlie Beckett (2012: 32–33) defines "networked journalism" as the transformation of journalism from "a closed to an open system," where elements that were not once included in the journalism ecosystem are now being embedded in it. In recent times, "networked journalism" has been used to explain the context in which new formats of news making, new identities, and new professional boundaries have been set. Data journalism is a good example of this process, as it embodies elements – such as data analysis and data visualization – that are not defining elements of journalism per sé. Consequently, the "boundaries of journalism" have expanded (Carlson and Lewis, 2015) to the extent that tactics whose roots are not entirely in journalism – such as adopting encryption tools in our case – can now have a role in the media ecosystem and can contribute to the news-making process.

This said, the encounter of journalism with hacking can't be explained by changes in journalism alone. This hybrid "trading zone" has also been enabled by the growing process of politicization of hacking and the new political stances that emerged among hackers engaged in direct action or civil disobedience as tactics (Coleman, 2017). Politicization has become more visible especially in regards to leaks in the service of civic and public goals and with media exposure as an aim. Hackers and hacktivists have become

BIBLIOGRAPHY

- Baack, Stefan. (2016). "What big data leaks tell us about the future of journalism – and its past." *Internet Policy Review – Journal on Internet Regulation*, available at: link.
- Beckett, Charlie. (2012). *WikiLeaks. News in the Networked Era*. Cambridge: Polity Press.
- Brunton, Finn & Nissenbaum, Helen. (2015). *Obfuscation. A User's Guide for Privacy and Protest*. Cambridge, MA: The MIT Press.
- Carlson, Matt & Lewis, Seth. C. (eds.). (2015). *Boundaries of Journalism. Professionalism, Practices and Participation*. London: Routledge.
- Coleman, Gabriella & Golub, Alex. (2008). "Hacker practice: Moral genres and the cultural articulation of liberalism." *Anthropological Theory*, 8(3): 255–277.
- Coleman, Gabriella. (2017). "From Internet Farming to the Weapons of the Geek". *Current Anthropology*, vol. 58(15): 91–103.



Edward Snowden

PHOTO BY GAGE SKIDMORE / FLICKR CC / BY-SA 2.0

more involved in the communication field and more interested in “work traditionally ascribed to journalists, expanding what it means to be involved in the production of news and, in the process, gaining influence over how traditional news stories and genres are constructed and circulated” (Russell, 2016: 7). This process was also helped by the “fluidity” of the hacker identity which, despite a loose acceptance of a common ethos, has always been “pliable, performative and fluid” (Fish & Follis, 2016) and consequently open to the widening of the spectrum of their activities.

According to Adrienne Russell, this hybridization is also visible in the rise of what she calls a new “media vanguard” composed of “journalists, activists, communication-technology hackers” who “are exerting significant influence in

today’s media environment through innovation and media competence” (2016: 9–10). At the current stage, it is important to point out how this hacking-influenced form of reporting has received differential forms of acceptance within the journalism community. It would be wrong to claim this represents a globally accepted status quo. Some news outlets, especially in the US, have embraced working with hackers and technology more explicitly and have made it the defining element of their editorial strategy: Glenn Greenwald’s *The Intercept*, for instance, has put “adversarial journalism” in the field of surveillance and cyber-affairs at its core. Together with the wide adoption of encryption as a central component of its reporting, *The Intercept* has been extensively covering hacking cases, establishing a generally positive attitude towards hackers. *ProPublica* also frequently works with hackers and coders of different backgrounds, including digital security or data journalism, and has also published first-hand reporting on the Snowden documents.

Other outlets’ acceptance of hacking has been far more reserved: while still covering news or documents coming from hacking cases, for instance, the *New York Times*, has been notably critical of hackers and hacktivists such as Julian Assange; and they have been more aloof than other news outlets while covering Edward Snowden (Di Salvo & Negro, 2015). *The Washington Post*, despite having

reported on the Snowden files, having won a Pulitzer Prize for its own coverage of the NSA case, and being a SecureDrop adopter, called for President Obama not to pardon Snowden (Washington Post, 2016). Further research, and ethnographic research in particular, will help in grasping the new boundaries of journalism and how they are set, established and influenced by hacking. When it comes to digital security, encryption and source protection, for instance, the contribution of hackers is crucial for literacy, knowledge sharing and tools-crafting in the journalistic field. Moreover, hacking-influenced journalism has proven to be a catalyst for investigative reporting; some of the most interesting journalistic investigations of recent times has involved some form of hacking. For newsrooms, in times of pervasive digital surveillance, journalists are put under new threats and pressures. Being proactively ready to assist whistleblowers and sources with proper encryption tools will become increasingly urgent. ■

PHILIP DI SALVO is a researcher and a journalist. Currently, he is a doctoral student at Università della Svizzera Italiana (Lugano, Switzerland), doing research on digital whistleblowing and the relationship between hacking and journalism. As a journalist, he writes for *Wired* and *Motherboard*, among others. He is also The European Journalism Observatory Italian editor.

- Di Salvo, Philip & Negro, Gianluigi. (2015). “Framing Edward Snowden: A comparative analysis of four newspapers in China, United Kingdom and United States.” *Journalism*, 17(7): 805–822.
- Fish, Adam & Follis, Luca. (2016). “Gagged and Doxed: Hacktivism’s Self-Incrimination Complex”. *International Journal of Communication*, 10: 3281–3300.
- Galison, Peter. (1997). *Image & logic: A Material Culture of Microphysics*. Chicago: The University of Chicago Press.
- Lewis, Seth. C., & Usher, Nikki. (2014). “Code, collaboration, and the future of journalism: a case study of the Hacks/Hackers global network.” *Digital Journalism*, 2(3): 383–393.
- Russell, Adrienne. (2016). *Journalism as Activism. Recoding Media Power*. Cambridge: Polity.
- Washington Post. (2016). “No pardon for Edward Snowden.” *The Washington Post*, September 17. Available at: [link](#).

REFUSE

AND

Joan Donovan dives into the dumpster of the Internet, and comes up holding some tasty ideas about what “doxing” means today and yesterday.

RESIST



It doesn't take an anthropologist to tell you that your trash is one of the most telling artifacts of your life. For punks, union organizers, private eyes, cops, journalists, phreaks, and hackers willing to get dirty, the dumpster can be a Pandora's box of treasure, triumph, and tribulation. But what happens when the dumpster goes digital and there's no garbage man to pick up the trash? Doxing—the act of collecting and publishing information

online on a person, organization, or company—has become a controversial tactic to shame, extort, and intimidate targets. Here, I explore how dumpster diving developed as a technique for information retrieval used in court cases, lawsuits, and exposés long before doxing was even possible. What new potential does doxing hold for those seeking more than retaliation or retribution, but rather social justice?

THIS IS GOOD TRASH!

Throughout my early twenties, my crusty punk friends and I spent hours ripping open bags from grocery stores, retail outlets, and doughnut shops in anxious anticipation of what we might discover. Being piss poor meant dumpstering was the only form of hospitality we could show our visiting friends, who we enthusiastically greeted with bags of smushed crullers and jellies.

Over time it became a way of life for one Boston punk. Knowing how to find good trash earned him a job with the union. He would forage through hotel trash bins looking for information about payroll and employees. Tossing aside soiled linen, empty take-out containers, and tons of pornography, he searched for scraps of paper and small notes. In one find, a manager had thrown away his home phone bill in the business trash. The information was useful to the union, who now knew where he lived as well as who he called. The union staged protests outside the boss's front door and called every number on the bill to pressure him to negotiate a new contract. Ten years later, this punk turned professional is still scaling fences and doing deep dives for evidence of corporate wrongdoing and to obtain potential leads.

Dumpster diving is a tactic frequently used in other domains, where the found information can be used to compel, extort, or influence others. There is a long history of private eyes digging through trashcans, where investigations involve “wastebasket recovery” of evidence to be used in divorce proceedings and lawsuits. Trash is also valuable to journalists and paparazzi alike, who sort through celebrity rubbish and government bins for

evidence of cuddling and/or collusion.¹ While corporations once used dumpstering to gain an advantage over competitors, they have revived this practice to intimidate activists and progressive groups.² Throughout the 1980s and 1990s, identity thieves targeted department stores for discarded checks and credit card applications. In these cases, the recovered materials were refashioned as evidence in court cases, sources in newspapers, new commercial products, and to intimidate or impersonate others.

At the same time, phone phreaks and hackers routinely searched dumpsters as a trove of informational treasure. Phreaks were known to crawl through the trash of Bell Telephone and even break into service trucks to obtain lineman's equipment. While this form of “no-tech hacking” was most popular in the 1980s and 1990s, popular targets included the phone company, high-tech companies, Radio Shack, law firms, banks, and post offices.³ Crackers and phreaks call this “information diving,” where they seek out not only miscellaneous papers, old faxes, and bills, but also discarded hard drives and other computer waste. Infamous hacker Kevin Mitnick began his career by stealing bus transfers from dumpsters and gaming the transit system. In 2000, Oracle admitted to paying private investigators to go through the trash of Microsoft and their affiliates.⁴

If info-garbage is really this valuable, why is dumpster diving still legal?

The law here is clear: once an item is thrown away, it is considered abandoned to the public domain. There is one catch, though; if a trash receptacle is on private property, the dumpster diver is trespassing. This law is not in place to protect punks, unions, hackers, or journalists; rather, it serves the police.

In 1984, a Laguna Beach police officer was following leads on a suspect, Billy Greenwood. Failing to obtain a search warrant for his home, local police asked the garbage man to collect his trash and keep it aside for them. In the garbage, the police found drug paraphernalia, which was cause for obtaining a search warrant for Greenwood's

1 In the 1990s, Benjamin Pell, a British man, combed the bins of celebrities and law firms for information to sell to the media (Leonard 2002).

2 For more on corporate spooks, see Ruskin (2013).

3 See Jason Scott's archive of BBS boards for early accounts of dumpstering (<http://textfiles.com/phreak/TRASHING/>) and Brad Carter's website (<http://www.phonelossers.org/dumpsterdiving/>)

4 For more on the Oracle scandal, see Stone (2000).

home. Four years later, the California Supreme Court in *California v. Greenwood* (486 U.S. 35; 1988) ruled that trash is expected to be “readily accessible to animals, children, scavengers, snoops, and other members of the public” and is therefore not protected by the Fourth Amendment. Police departments rely on this precedent to justify sifting through garbage for evidence.

THE DUMPSTER GOES DIGITAL

Knowing where to find good trash is just as important as how to use it. With the Internet, the landfill has changed, and so have the stakes. As more of our lives move online, we now do much of our work and pay our bills on networked computers while also using these same terminals to post images, write screeds, find love, and consume media. If you are anything like me, your hard drive is a garbage can overflowing with discards from the last decade of your life, whereas your Internet history is a digital dumpster that holds untold possibilities for extortion, embarrassment, and the ‘lulz’. Though your physical garbage resides on the curb for a few hours a week, your digital garbage rots for decades strewn across networks, systems, and accounts. Save for the invisible labor of commercial content moderators, who scrub social media platforms of noxious materials, little is done to remove the mundane and everyday detritus of our everyday life online (Roberts 2016).

Doxing involves combing through the digital debris, collecting all pieces of information on that person or group, analyzing how one piece may lead to a new place to look, and then making sense of the information as a single record. Like dumpstering, the method of doxing is similar for the police, union organizers, and private eyes, who seek to build cases against organizations or individuals. For journalists, this kind of digital sleuthing is also a rather routine aspect of the job.⁵ Activists tend to take this tactic one step beyond compiling information, publishing the dossier online to shame, embarrass, or bully targets. Websites such as Pastebin or Doxbin are ready-made receptacles for unidentified circulation. Like dumpstering, doxing is a low-tech form of hacking in which information is valuable resource to be exploited.

Doxing is controversial because it has been used to humiliate, shame, and intimidate intended targets. Most notably, “social justice warriors” (i.e., women with opinions and platforms) were doxed by supporters of “ethics in journalism” in the Gamergate scandal.⁶ Today doxing is a preferred tactic of right-wing activists, who screenshot videos of leftist protests to identify organizers. Depending on the techniques used to gather information and the level of engagement with the target, doxing can warrant charges such as cyberstalking and harassment, especially

if it leads to “real-world” contact such as swatting.⁷ Often though, those who do this kind of information diving are not held accountable because the police decline to make arrests or “the doxer” uses methods to remain anonymous (Edwards 2017). Overall, doxing is regarded as a low-cost and low-tech way of intimidating and shaming targets.



FIG. 1: Luckily, I grew up when most people used anonymous screen names, but here is a picture of my cat from 2007 that I recently found when searching an old avatar. Ain't she cute?

But here's where the sludge thickens. While doxing can be used to expose, extort, or expel, it can also be a powerful leveler for those who seek social justice when they know criminal justice is far out of reach. Like the union's use of dumpster diving, doxing holds the potential to pressure institutions to enact sanctions that the courts will not. Doxing has been used by groups such as Anonymous

and Occupy protesters in an attempt to expose and reign in police, governments, and corporations.

Doxing of police officers gained mainstream media attention during the Occupy Movement of 2011–2012. Digital information diving was spreading to new groups of activists as a tactic that forced a response. Since 2011, #OpPigRoast continues to be an ongoing Anonymous



FIG. 2: This is what a dox looks like.

5 See Coleman (2014:418) for an account of doxing practices used by Anonymous and journalists.

6 Liz Losh (2016) recounts the history of Gamergate.

7 A side effect of doxing, trolls will call in fake emergencies that lead to a home invasion via swat team (Fagone 2015).

action in which information about police officers and police unions is collected, archived, and shared.

The doxing of Officer Anthony Bologna was one of the critical factors kickstarting the Occupy movement. A week into the occupation of Zuccotti Park, a NYPD officer pepper-sprayed a small group of protesting women who were already confined behind a police barricade.⁸ This video quickly spread through activist networks across the Internet. By looking at different pieces of footage from throughout the day, protesters were able to match the face of the officer with a photo clearly displaying the officer's face and badge from earlier in the march. The identity-revealing image was tweeted by a labor-activist, who posted the picture to shame the officer who was acting aggressively.

With name and badge number in hand, Anonymous tweeted a dox containing the officer's name (Anthony Bologna), last known addresses, family members, phone number, and legal troubles. Because Bologna was identified, the story became newsworthy and was subsequently picked up by major media outlets. Bologna's actions cost the city of New York \$382,501 to date and, short of losing his job, he was transferred to a different station.⁹

Lieutenant John Pike, now infamously known as the "pepper-spraying cop," is another example of doxing for social justice by Occupy protesters.¹⁰ A photo of Pike casually pepper-spraying sitting students at the University of California, Davis, became an overnight Internet sensation.¹¹ Activists at UC Davis sought to bring Pike to justice by shaming UC Chancellor Linda Katehi; Pike eventually was fired. He was subsequently awarded \$38,000 in worker's compensation for emotional distress after his phone number and email address were repeatedly published online; he reportedly received 17,000 emails, 10,000 texts, hundreds of voicemails, and lots of unwanted mail.¹² UC Davis paid \$1 million to victims of Pike's assault.

More curious though, Pike's online popularity ended up contributing to former Chancellor Katehi's resignation. In an attempt to manage UC Davis's online image, Katehi authorized \$175,000 in university funds to scrub the Internet of references to this event and to improve the school's reputation. Protesters continued to pressure Katehi long after the Pike incident, while journalists and administrators investigated her contracts, affiliations, and conflicts of interest. Allegations that she tried to polish her own online image using university funds led to her undoing.¹³

While reputation management firms sell products they claim can improve tarnished reputations, currently there is no way to tell shit from Shinola. More than just rebranding UC Davis, aides reported that Katehi simply wanted them to "get me off the Google."¹⁴ Reputation

management firms know all too well that there is no sure-fire way to remove information from the Internet. Instead, they fill the bin higher and deeper with more junk, hoping to cover over what's at the bottom, like a cat in a litterbox.

Importantly, the information obtained and published about these officers was already public; it was just a matter of knowing where to look for information, where to publish it, and ultimately how to use new and old media to unlock its potential. Poking around at the fetid leftovers online seems to be fine as long as you do not try to leverage that information politically. Whereas the police have found it advantageous to ensure they have access to curbside rubbish, these online scraps are legally ambiguous for civilian doxing.

THIS PLACE IS STARTING TO SMELL

What was once a specialized tactic of punks, journalists, unions, police, phreaks, hackers, and private detectives, dumpster diving has proliferated for all types of reasons. We used to rely on the telephone book to share public information; today, things like phone numbers and home addresses should be preciously protected information in an era of digital dumpsters. What's most concerning is that information abandoned online is more durable than the stuff we throw into those enormous steel bins. Because the Internet is designed to capture and distribute information to the widest audience, once information is posted, it is difficult to erase. The tools of search, hyperlinks, screenshots, and the ease of copy/paste supports the proliferation of content, not its disposal. Just like trashcans, the digital dumpster has overflows. For Katehi, this was an expensive lesson.

Activists know that doxing is an effective tactic when applied to pressure sanctions from civil institutions. Occupy protesters used the information networking capacity of the Internet to bring together stores of information into a single container and repackage it for popular consumption. So far, no one has been charged with publishing or sharing information about Bologna or Pike. For Occupy protesters, doxing was a demand for social, not criminal, justice. In doing so, we see that when the dumpster goes digital, movements can expand their political capacity by sorting the good trash from the bad, giving new meaning to the call to refuse and resist! ■

JOAN DONOVAN (*JoanDonovan.org*) is the Media Manipulation Project Lead at *Data & Society*.

8 See video of protesters being pepper-sprayed at <https://www.youtube.com/watch?v=TZO5rWx1pig>

9 For more on information on civil suits related to Bologna's actions, see Brown (2015).

10 Anonymous published a video of Pike's dox (Buzzfeed 2011).

11 For the lulz, see <http://peppersprayingcop.tumblr.com/>.

12 For more on the consequences of Pike's actions, see Garofoli (2016) and Huet (2013).

13 For more information on Katehi's resignation, see Stanton and Lambert (2016).

14 For more information on Katehi's troubles with online reputation management, see Lambert and Stanton (2016).

BIBLIOGRAPHY

- Brown, Stephen Rex. 2015. "Exclusive: NYPD Cop's Spraying of Occupy Wall Street Protesters Costs NYC Additional \$50K." *New York Daily News*, July 21. <http://www.nydailynews.com/new-york/nypd-spraying-ows-protesters-costs-nyc-50k-article-1.2298460>
- Buzzfeed. 2011. "Anonymous Fights Pepper Spray With Personal Information." *Buzzfeed*, November 21. Available at <https://www.buzzfeed.com/sly/anonymous-fights-pepper-spray-with-personal-inform>.
- California v. Greenwood*. 486 U.S. 35. 1988. <https://supreme.justia.com/cases/federal/us/486/35/case.html>
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, New York: Verso.
- Edwards, Jim. 2017. "FBI's 'Gamergate' File Says Prosecutors Declined to Charge Men Believed To Have Sent Death Threats—Even When They Confessed on Video." *Business Insider*, February 16. <http://www.businessinsider.com/gamergate-fbi-file-2017-2>
- Fagone, Jason. 2015. "The Serial Swatter." *New York Times Magazine*, November 24. https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0
- Garofoli, Joe. 2016. "UC Davis Pepper-Spray Officer Awarded \$38,000." *SFGate*, April 15. <http://www.sfgate.com/politics/joegarofoli/article/UC-Davis-pepper-spray-officer-awarded-38-000-4920773.php>
- Huet, Ellen. 2013. "Pepper-Spray Cop Seeks Worker's Comp." *San Francisco Chronicle*, July 26. <http://www.sfchronicle.com/bayarea/article/Pepper-spray-cop-seeks-workers-comp-4688820.php>
- Lambert, Diana, and Sam Stanton. 2016. "'Get Me Off the Google,' UC Davis Chancellor Katehi Urged Communications Staff." *Sacramento Bee*, August 9. <http://www.sacbee.com/news/local/education/article94733812.html>
- Leonard, Tom. 2002. "Benji the Binman cleans up." *The Telegraph*, March 22. <http://www.telegraph.co.uk/news/uknews/1388476/Benji-the-Binman-cleans-up.html>
- Losh, Elizabeth. 2016. "Hiding Inside the Magic Circle: Gamergate and the End of Safe Space." *boundary2 online*, August 15. <http://www.boundary2.org/2016/08/elizabeth-losh-hiding-inside-the-magic-circle-gamergate-and-the-end-of-safe-space/>
- Roberts, Sarah. 2016. "Digital Refuse: Canadian Garbage, Commercial Content Moderation and the Global Circulation of Social Media's Waste." *Wi: Journal of Mobile Media* 10(1) (Mobile Trash Issue). <http://wi.mobilities.ca/digitalrefuse/>
- Ruskin, Gary. 2013. "Spooky Business: Corporate Espionage Against Nonprofit Organizations." Washington, DC: Essential Information. <http://www.corporatepolicy.org/spookybusiness.pdf>
- Stanton, Stan, and Diana Lambert. 2016. "UC Davis Chancellor Katehi Steps Down Under Pressure." *Sacramento Bee*, August 9. <http://www.sacbee.com/news/local/education/article94627837.html>
- Stone, Brad. 2000. "Diving into Bill's Trash." *Newsweek*, July 9. <http://www.newsweek.com/diving-bills-trash-161599>



Half-lives of hackers

Re: Risotto

From: john.podesta@gmail.com

To: peter_huffman@yahoo.com

Date: 2015-09-19 02:50

Subject: Re: Risotto

Yes and no

Yes it with absorb the liquid, but no that's not what you want to do. The slower add process and stirring causes the rice to give up it's starch which gives the risotto it's creamy consistency. You won't get that if you dump all that liquid at once.

and the shelf life of hacks

What is the speed of hacking? Luca Follis and Adam Fish explore the temporality of hacking and leaking in the cases of Snowden, the DNC leaks and the Lauri Love case.

FAST

Hackers helped Donald Trump win the 2016 U.S. election. It wasn't so much the content the hackers released about Hillary Clinton to the public through WikiLeaks; instead, it was the air of suspicion they created that led to her undoing: the Secretary of State could be and was hacked. That became Clinton's problem, not what she and her colleagues wrote. Who had time to read the 19,252 emails from the Democratic National Committee (DNC) leak that WikiLeaks released four months before the election or the 20,000-plus emails from John Podesta—White House chief of staff and chairman of Clinton's US presidential campaign—published a month before the November 8 election? Muckrakers barely had time to conduct keyword searches in WikiLeaks's archives. The sheer size and breadth of the material made analysis difficult. Big data smothered interpretation. *Langue* trumped *parole*.

Whether a slow and insistent "leak" or a cataclysmic data "dump," the pace, frequency, and size of the hack matters. Blindingly fast and impenetrably large, the political impact of the hack is potentially larger than the content contained within. Here we plot the temporalities of three hacks ranging from the fast to the slow to the still: we describe the excesses in volume and speed in the Clinton case, the slow journalism of the Snowden/Greenwald collaboration, and the non-leaked hack of Lauri Love, an Occupy and Anonymous hacktivist scheduled for extradition to the United States for allegedly hacking military and banking institutions but not releasing any material.

Some of the material in the DNC and Podesta leaks

did receive attention, whether it was due or not. For example, Edgar Welch was inspired by blogged conspiracy interpretations concerning the reoccurrence of the worrisome term "pizza" in the emails and their obvious connection to a Clinton child sex slave dungeon located in a Washington, DC, pizzeria. So on December 4, 2016, carrying a shotgun, assault rifle, and .38 revolver, Welch went to the Comet Ping Pong restaurant to search, in his report to police, "for evidence of hidden rooms or tunnels, or child sex-trafficking of any kind" (Jarrett 2016). Finding none, he shot up the place with his AR-15 rifle and was arrested on federal charges for this mission on behalf of what came to be known as "fake news." Facebook CEO Mark Zuckerberg has emerged with a seven-point plan to tame "fake news" on his website including the typical crowd-sourced self-regulation and self-reporting or flagging (Jamieson and Solon 2016). We can't wait to get officially illicit along with our Facebook-verified news and hacks.

While thankfully no diner at Comet lost their life because of this poor hermeneutical reading of hacked leaks, somebody likely did lose the U.S. presidency because of it. "Spirit cooking" was a trending term days before the 2016 U.S. presidential election. In an email from performance artist Marina Abramović, Podesta was invited to dinner with the line, "I am so looking forward to the Spirit Cooking at my place" (Lee 2016; Podesta did not respond to this invitation). The alt-right seized upon this term as an oblique reference to satanic rituals involving human sacrifice, with



DIVER SIGNALS COURTESY OF WIKIMEDIA COMMONS

Clinton seated at head of the occultic new world order (Ohlheiser 2016). These are some of the few stories to come from the trove. Otherwise, much of it is boring, trivial, and gossipy, or requiring the skilled interpretive acrobatics of the best conspiracy theorists.

Some of the material revealed—Clinton’s staff emails colluding with the DNC to dispose of Democratic challenger Bernie Sanders, her Wall Street speeches, and the forms of “pay-to-play” access given by the Clinton Foundation to the global elite—does present damning evidence. Yet it wasn’t the content, we argue, but the impenetrable volume and the breakneck pace of the leaks that cursed Clinton and puzzled journalists. Whatever legitimate political harm was created by the disclosures was not a result of analysis, attribution, or even denial.

The present world of hacks and leaks is front-loaded. It is overwhelmingly determined by the volume and pacing of the disclosures, a fact that can substantially eclipse the revelatory (and factual) nature of the material itself. It is true that economic and demographic reasons are more likely contenders than an email scandal for why Clinton lost to an unprepared, platformless, tax-dodging, racist, bankruptcy-prone, misogynistic, fact-phobic, former reality television star. But it certainly didn’t help. Her quandary provides a window into a new politics of suspicion that forms at the intersection of volume, velocity, and disclosure, factors that eclipse revelation, attribution, and denial, which are the stickier subjects of scandal. Excess and speed, the sheer volume of the hacked materials paired with the velocity with which the content appeared on contraband websites—in user-friendly boolean searchable form, no less—are the quintessential marks of the hacktivist today.

Velocity and volume combine powerfully and call to mind Paul Virilio’s (1977) writings on the impact of technologically hastened politics. His term “dromology” refers to the inner logic of speed and the moving object’s tendency to dominate slower rivals. It is an apt way to think about the current state of leaks: fast volumes dominate the headlines and overtake slow journalism. The present moment in hacktivist history

is marked by an excess of information exploding centrifugally outward against both left and right political ideologies. Clinton was a victim of the excess dromology of this election cycle. But not all hacks need to follow this pace and fill public space in this manner. There remains a time and space for revelation.

SLOW

On June 6, 2013, Glenn Greenwald published a story in *The Guardian* based upon a top-secret court order requiring Verizon (a major U.S. telecom company) to provide the National Security Agency (NSA) with information on all telephone calls in its systems within the United States and between the United States and other countries. The following day, *The Washington Post* and *The Guardian* published the first stories detailing the NSA’s bulk domestic surveillance program PRISM along with four internal PowerPoint presentation slides from the whistleblower and former NSA employee Edward Snowden. Snowden’s disclosures were parsimonious and carefully chosen, accompanied by careful and contextual reporting, and their overall sequencing was staggered over the course of multiple years (Greenwald 2015).

Indeed, apart from the tremendous political impact of his revelations, what remains striking today is the fact that the published and publicly disclosed documents represent a very small proportion of the full Snowden trove. The archive that Snowden shared with news outlets contained about 50,000 documents, of which approximately 7,300 have been released since 2013. Further, although there is debate about the total number of sensitive documents he downloaded from the NSA, conservative estimates put the figure at 1.5 million (Kloc 2014).

Contrast this figure with the 20,000 Democratic National Committee emails, 891 documents, and 175 spreadsheets released by WikiLeaks on July 22, 2016, just days before the Democratic National Convention was held in Philadelphia (July 25–28). The data hacking is notable because of its timing, sheer volume, and indiscriminate character: John Podesta’s risotto tips absurdly sit alongside evidence of strong anti-Bernie



Sanders bias among staffers. And just days after the leaks, in the midst of the national convention, DNC Chairwoman Debbie Wasserman Schultz resigned. The following month DNC CEO Amy Dacey, CFO Brad Marshall, and communications director Luis Miranda all announced their intention to leave the DNC (Tau and Nicolas 2016).

Clearly the leaking of the Snowden and DNC documents was timed for maximum impact. Although the former sought to influence then-current events, the full impact of the disclosures is oriented towards the *longue durée* and the extensive digital archive of American global panopticism that will be preserved in posterity. The DNC leaks, on the other hand, were timed for immediate, disruptive, and destabilizing force: that is, their form (the fact they existed and their sheer size) had more impact than their actual content. Further, in contrast to the selective and parsimonious character of the Snowden disclosures (and some prior WikiLeaks releases), the DNC files were published all at once and with no apparent curation.

The difference between these two “leaks” or disclosures is also informative with respect to the shifting tactical uses of identity and attribution. Snowden’s character and motivation became integral components of the story, providing an anchor for the leaked material that also gave it salience and immanence, and vouched for its authenticity. In contrast, everything known about the DNC hacks seems designed to confound, frustrate, and work against the intuitive alignment between legitimate political activism, information transparency, and whistleblowing. Initially, the hack was attributed to two different Russian intelligence adversaries, Cozy Bear and Fancy Bear. And while six cybersecurity firms and two newspapers agreed that the level of sophistication—and a few self-incriminating mistakes—indicated a Russian state-level hack, other names and motives soon arose. The first pseudonym to step forward was Guccifer 2.0, a reference to the 1.0 Guccifer, a Romanian hacker extradited to the United States and recently sentenced to 52 months in federal prison. Guccifer 2.0 claimed to be a hacktivist colleague of the original Guccifer until questions concerning his

fluency in Romanian and his connection with Russia surfaced (Goodin 2016).

That WikiLeaks released the DNC emails certainly did not help clarify matters, and Julian Assange’s sloppy remarks on Dutch TV identifying the leaker as recently murdered DNC staffer Seth Rich only generated further ambiguity (Stahl 2016). Thus far, the DNC hacks have been linked to the Russian state, Romanian hackers, a dead DNC staffer, and—as one former NSA analyst and counterintelligence officer for the Navy claimed—the NSA itself (Schindler 2016). The DNC hacks provide a glimpse into one facet of the shifting tactical array employed by state-based forms of hacking in which the political tropes, themes, and expectations we have come to associate with hacktivist and whistleblowing disclosures (including the factual authenticity of the material itself) are hijacked for anti-political and disruptive effect.

INERT

Hacks may be small or large; they may contain influential evidence or not. Some hacks we don’t know about because they are never made public. We know of their existence through hearsay, rumor, or acts of partial transparency. We know of the form, but not the content; the deed but not its result. The case of Occupy activist and alleged Anonymous associate Lauri Love is a case in point. In July 2016, Westminster Magistrates Court ruled that the United Kingdom would extradite the Finnish-Welsh hacker to the United States to face computer fraud charges in three federal jurisdictions. Little is known about the accusations actually leveled against him. It’s not just that the rules of extradition prevent the examination of Love’s alleged criminal activities but also that the content Love is charged with exfiltrating from the United States was never publicly released. This is the leak that never happened, and Love faces 100 years in jail for it.

Love’s case is connected with the suicide of internet freedom activist Aaron Swartz on January 25, 2013, and the political action that followed his death. Two weeks later, Anonymous initiated Operation Last Resort, which included the hijacking of a Massachusetts

Institute of Technology (MIT) website to create a Swartz tribute as well as the usurping of the U.S. Sentencing Commission website (ussc.gov) and a website of the Department of Justice (Blue 2013). The only leak associated with Operation Last Resort is the release of the 4,000 banking executives' names on February 4, 2013, which contained no information of political significance (Robertson 2013). This hack was a spectacle without the substance.

Associated with the action, Anonymous claimed to have distributed encrypted government files pertaining to U.S. Supreme Court Justices and threatened to release the decryption keys if the government did not reform the draconian laws they believed led to the death of Swartz. In press releases and videos, Anonymous called these decryption files, each referencing a U.S. Supreme Court Justice, "warheads," for example "Scalia.warhead1." Why weren't the keys released, and what does their absence mean for the study of the political impact and consequences of hacking?

In contrast to Snowden and the DNC hacks, the temporality of Love's alleged hack does not follow the trajectory and pace of the 24-hour news cycle but is oriented to the slow temporalities of the criminal justice state. On October 23, 2013, the first of three U.S. court indictments against Love were filed. Two days later he was arrested and a search warrant was served on his parents' house. Nine months separated the initiation of Operation Last Resort and Love's arrest. On July 3, 2014, Love was released on bail, his passports were returned, and the Crown Prosecution Service declined to prosecute for lack of evidence. Almost one year later (July 15, 2015), Love was arrested again, this time by the Metropolitan Police's extradition unit for the outstanding U.S. indictments connected with Operation Last Resort, which include hacking into the Federal Reserve, the U.S. Army, NASA, and the Missile Defense Agency. From June to July 2016, Love appeared in court challenging the extradition request and was denied on September 16, 2016, when Judge Tempia ruled in favor of extradition. Love has an appeal, but it is likely that

he will eventually face his accusers in the United States and be sentenced to significant time in prison.

The case provides an important counterpoint to Snowden and the DNC hacks. This is the leak that never happened. Its temporality was interrupted and hijacked by a criminal justice process that has and will continue to control the tempo, volume, and content of material that will appear in the public record with respect to Operation Last Resort (Fish, forthcoming). It is likely that what will be revealed in Love's criminal trial(s) will be scrubbed of its impact and separated from the political events that gave it relevance by the slow time of courtrooms and the veil of prosecutorial abstraction. In this sense, the inertia that surrounds the case also crystallizes the stakes involved: Love's ability to frame the hack as an instance of political activism or in terms of public interest claims concerning the content of the material he exfiltrated is vitiated by the very real threat of self-incrimination (Fish and Follis 2016). In the absence of such an account, the courtroom becomes a space for the deployment of a very particular technology of truth. Who is Lauri Love? What are his motives? How grave are his actions? Is he an activist, a terrorist, or a foreign agent? These questions swirl around the case and assert themselves in the interpretive vacuum generated by his criminal defense.

Operation Last Resort, much like the Snowden disclosures and the DNC hacks, points to the emergence of a powerful "hermeneutics of suspicion" (Ricoeur 1970) where the deeper (and perhaps more authentic) meaning that sits behind text and event, between actor and act, oscillates unpredictably under the force of multiple, fractious interpretations delivered contemporaneously. The variegated publics that are its targets have grown increasingly insular, wary of expert claims, and skeptical of the facts that support them. In response, a new counter-critical common sense informs their reading of political and world events, a reading both determined by and filtered through a dromological news cycle saturated with leaks and data dumps.

BIBLIOGRAPHY

- Ashok, India. 2016. "Weebly Confirms Over 40 Million Users, Foursquare Accounts Are Also Exposed." *International Business Times*, October 21. Available at [link](#)
- Blue, Violet. 2013. "Anonymous hacks US Sentencing Commission, distributes files." *ZDnet*, January 26. Available at [link](#).
- Fish, Adam R. forthcoming. "Scalia.warhead1: Securitization Discourses in Hacktivist Video." In *Visual Security Studies: Sights and Spectacles of Insecurity and War*, edited by J. Vuori and R. Saugmann. Abingdon-on-Thames, UK: Routledge.
- Fish, Adam R., and L. Follis. 2016. "Gagged and Doxed: Hacktivism's Self-Incrimination Complex." *International Journal of Communication* 10:3281–3300.
- Goodin, Dan. 2016. "'Guccifer' leak of DNC Trump Research has a Russian's fingerprints on it." *Ars Technica*, June 16. Available at [link](#).
- Greenberg, Andy. 2016. "Hack Brief: Yahoo Breach Hits Half a Billion Users." *Wired*, September. Available at [link](#).
- Greenwald, Glenn. 2015. *No Place to Hide: Edward Snowden, the NSA and the US Surveillance State*. New York: Picador.
- Jamieson, Amber, and Olivia Solon. 2016. "Facebook to begin flagging fake news in response to mounting criticism." *The Guardian*, December 15. Available at [link](#).
- Jarrett, Laura. 2016. "'Pizzagate' shooting suspect facing new federal charges." *CNN*, December 13. Available at [link](#).
- Kloc, Joe. 2014. "How Much Did Snowden Really Take? Not Even the NSA Really Knows." *Newsweek*, June 9. Available at [link](#).

HACK HOROLOGY

On the top shelf of a dusty Oxbridge bookshelf, we can already see the 2017 *Oxford English Dictionary* making room in itself for a “fake news” sequel to its 2016 word of the year, “post-truth.” The volumetric and expedient hack contributes to this erosion of facts creating an aura of ambiguous “truthiness,” the Merriam-Webster 2006 word of the year. As speculation and conspiracy increase, the English dictionaries—like the hegemonic public sphere—are reflecting the erosion of consensual reality, and logical democratic consensus is a victim.

Political hacks today come in the context of pervasive data insecurity and systemic cyber vulnerability. Whether it’s news that many major companies (e.g., LinkedIn, Dropbox, Tumblr, Yahoo, Foursquare, Weebly) have recently suffered large-scale data breaches or the dramatic outages caused by the recent global distributed denial of service (DDoS; when a hacker makes a network unavailable to its users) attack on internet switchboard company Dyn, it seems as if everything and everyone in our media-saturated societies is now potentially vulnerable, including our sense of reality (Ashok 2016; Greenberg 2016).

The temporality and volume of leaks influences their public reception, meaning, and impact. The primacy of these two factors displaces and distorts some of the categorical, normative, and political inventory we traditionally use to make sense of the motives of hackers/leakers and the importance of their disclosures. In other words, speed and volume displace and distort the most analytically important category of all: revelation.

One conventional way of thinking about political hacks and leaks (as opposed to breaches) involves their *revelatory* intent. The strength and impact of a leak or data dump are usually tied to the extraordinary character of the material contained in the disclosure. An influential leak is factual; it provides information or documents that offer incontrovertible legal-grade proof of a whistleblower’s or leaker’s claims about the state of reality. Such leaks can usually weather official denials and evasions. Indeed, in cases of serious

criminal activity or malfeasance, leaks might prompt governmental action through investigations and/or prosecutions.

The situation we describe here is one in which the extraordinary has become commonplace and where radical information transparency is ubiquitously, indiscriminately, and summarily applied. One danger here is that the sheer volume, speed, and frequency of disclosures is greatly outpacing our capacity to separate politically salient or criminally significant acts and facts from the ambient digital noise they come bundled with. On the one hand, this clearly points to the need to better align tactics of revelation and disclosure with questions of timing and scale.

Yet in a deeper way, it also seems to threaten the capacity of digital technology and the web to serve the wider project of critique and dissent because the dromology of the data dump feeds into and strengthens already existent power asymmetries. We have already noted how the DNC hacks illustrate the increasingly common appropriation of hacktivist tropes and forms by state power, thereby coopting the tactics of the weak into stratagems of power. In a world where the effect or impact of a leak is divorced from the content it contains, it becomes possible (even inevitable) that faux leaks and fake news become yet another tool in the arsenal of states. ■

LUCA FOLLIS is a political sociologist and Lecturer in the Law Department at Lancaster University; his work focuses on the intersection of law, the state and resistance. **ADAM FISH** is an anthropologist and Senior Lecturer in the Sociology Department at Lancaster University where he researches digital industries and digital activism. He is the author of the book *Techoliberalism* (Palgrave Macmillan) and co-author of *After the Internet* (Polity).

- Lee, Benjamin. 2016. “Marina Abramović mention in Podesta emails sparks accusations of satanism.” *The Guardian*, November 4. Available at link.
- Ohlheiser, Abby. 2016. “No, John Podesta didn’t drink bodily fluids at a secret Satanist dinner.” *The Washington Post*, November 4. Available at link.
- Ricoeur, Paul. 1970. *Freud and Philosophy: An Essay on Interpretation*. New Haven, CT: Yale University Press.
- Robertson, Adi. 2013. “Anonymous Posts banking industrial data dump in ongoing Aaron Swartz protest.” *The Verge*, February 4. Available at link.
- Schindler, John. 2016. Did the NSA Try to Destroy Hillary Clinton, *Observer*, August 8. Available at link
- Stahl, Jeremy. 2016. “WikiLeaks is Fanning a Conspiracy Theory that Hillary Murdered a DNC staffer.” *Slate*, August 9. Available at link
- Tau, Bryan, and Peter Nicholas. 2016. “Three More Democratic Officials Resign in the Wake of Email Leak.” *Wall Street Journal*, August 2. Available at link
- Virilio, P. 1977. *Speed & Politics: An Essay on Dromology*. New York: Semiotext(e).



Se toco á su Original

el dia 2o de Mayo de 1749 a.

THE ILLICIT AURA OF INFORMATION

Does the unfiltered, illicit status of a leak change the nature of information? **Molly Sauter** offers a consideration of the half-life of stolen data.

IF A DATABASE, LIKE AN EMAIL DATABASE, IS STOLEN or hacked by outsiders (as opposed to being leaked by insiders or extracted via the Freedom of Information Act [FOIA] or other legal mechanisms) and dropped, unfiltered and uninterpreted, on the open web, does that change the way that information is received upon its release? Would its origins and manner of release change the way the information contained within the database could be used, or the types of narratives that might be spun out of it?

In this article I suggest that when personal, private, secret, or otherwise not-public email databases are hacked and released onto the public Internet without the initial mediation of an established journalistic entity, these databases become the ideal medium for the growth and dissemination of successful and tenacious conspiracy theories. This is due in part to what I've called, after Benjamin, the "illicit aura of stolen information," and the ways in which this aura cuts against norms of analysis, investigation, and interpretation, norms which professionalized journalists had until recently been in a powerful position to defend and enforce. The illicit aura shifts analytical authority from experts to amateurs, strips journalism of its role as legitimator of information and director of attention without reassigning that role, and overrides analytical distinctions between "privacy" and "secrecy." It creates feedback loops because any actions taken by individuals caught up in these data dumps to maintain their privacy are likely to be interpreted as attempts to conceal evidence of wrongdoing. Hacktivists who wish to publish the private communications of powerful individuals should bear in mind the ways in which the data-dump model of publication encourages conspiratorial modes of analysis and has the potential to damage journalistic norms like fact-checking, translation, and contextualization.

To illustrate this aura, I focus on two cases: the 2009 Climate Research Unit email hack, known as

"Climategate," and the 2016 hack of the internal emails of the Hillary Clinton presidential campaign and the #Pizzagate conspiracy theory.

These cases have a number of points in common. They both involve the exfiltration of large email databases. These databases may contain records that fall under American and British Freedom of Information Acts, but are fundamentally the mundane interpersonal communications of professionalized in-groups, and as such the language used in them is both specialized and casual. The content of the databases in both cases initially went unnoticed by mainstream professionalized journalistic news organizations. Non-expert, non-journalist writers working independently on social media or for smaller blogs had the first interpretive crack, while mainstream news sources either reported on the fact of the hack without interpreting the content of the databases or began their reporting only after the initial conspiratorial interpretations had been made and publicized, putting them in a position to report on both the hack and the conspiratorial interpretation simultaneously. The conspiratorial interpretations stemming from these databases proved particularly influential and tenacious, repeated by politicians and other influential figures or resulting in real-world violence.

CASE 1: CLIMATEGATE

In 2009, more than 160 megabytes of data were exfiltrated from a server used by the Climatic Research Unit (CRU) at the University of East Anglia in the United Kingdom. Included in this cache were nearly 1,000 emails and 3,000 other documents. The cache was uploaded to a Russian server, and from there, links were distributed directly to various "climate-skeptic" sites and organizations.

Climate-change deniers became fixated on a few email threads in the cache, wherein a handful of scientists discuss how to present certain data, the deletion



of data in the face of FOIA-type requests, the issue of peer review, and their general and specific disdain for climate-change deniers. One thread in particular, in which CRU director Phil Jones and Penn State Earth Systems Science Center director Michael Mann discussed using a statistical “trick” to “hide the decline” in climatic warming as indicated through tree ring data, was repeatedly cited as evidence of an international conspiracy by a cabal of scientists to suppress data that contradicted the anthropogenic theory of climate change.¹

Climate-denier blogs provided the initial reporting on the cache, the conspiracy, and hack itself, including Anthony Watt’s *Watts Up With That* blog, which named the event “Climategate.”² Less than a week later, *Telegraph* columnist James Delingpole picked up the story, writing a *Telegraph* blog entry titled, “Climategate: The Final Nail in the Coffin of ‘Anthropogenic Global Warming’?”³ This column set off a flood of attention, with other blogs repeating the conspiracy theory put forward by *Watts Up With That* and Delingpole, and mainstream news organizations subsequently reporting on the hack and commenting on the ensuing scandal.⁴ The cache was the subject of an annotated, color-coded report published by the Lavoisier Group, a “climate-skeptic” organization located in Australia. Various politicians, mostly established climate-change deniers, commented publicly

on the cache, including Sarah Palin and Jim Inhofe, concentrating almost exclusively on the particular lines regarding statistical “tricks” and “hid[ing] the decline.” Climate scientists at the Climatic Research Unit and other climate research centers also reported an uptick in threatening emails, phone calls, and other communications (Clynes 2012).

Multiple independent reviews, including those performed by FactCheck, the House of Commons Science and Technology Committee, Penn State University, the U.S. Environmental Protection Agency, the U.S. Chamber of Commerce, and the National Science Foundation, found no misconduct or inappropriate manipulation or mishandling of data had occurred, and the use of the words “trick” and “hide” were professionalized, in-group language referring to normal statistical manipulations. However, when interpreted out of context by non-experts and outsiders (particularly outsiders with a specific interpretive bias), these words were seized upon as evidence of intentional concealment and deception. This conspiratorial interpretation became more tenacious because it was repeated by those promoting it and by mainstream news organizations reporting on the “scandal.”

CASE 2: DNC/PODESTA HACK AND #PIZZAGATE

During the 2016 election, the personal Gmail account of John Podesta, a former White House chief of staff

- 1 The “tree-ring divergence problem,” or the conflict between instrumental temperature data and tree ring data, is a well-documented and thoroughly discussed issue in the study of historical climate data, and not generally considered to be a scientific counterargument to the anthropogenic theory of climate change.
- 2 The moniker first appears in the comment thread on the November 19, 2009, post “Breaking News Story: CRU Has Apparently Been Hacked—Hundreds of Files Released” (Watts 2019). A user called “Bulldust” comments, “Hmmm I wonder how long before this is dubbed ClimateGate?”
- 3 Originally published at <http://blogs.telegraph.co.uk/news/jamesdelingpole/100017393/climategate-the-final-nail-in-the-coffin-of-anthropogenic-global-warming/>, the article has since been removed. It is mirrored at various climate-denier blogs such as *Global Climate Scam* (Delingpole 2009).
- 4 Some examples of the mainstream press coverage: The *New York Times* picked up the story on November 20, not using the “ClimateGate” moniker, in an article titled “Hacked Email is New Fodder for Climate Dispute” (Revkin 2009a). The article notes the “trick” email, quotes climate scientists calling critics “idiots,” and quotes a Cato Institute-affiliated climate “skeptic” as saying, “This is not a smoking gun; this is a mushroom cloud.” The first article to use the “ClimateGate” name was published on November 27 (Revkin 2009b). Since 2009, the *Times* has published 84 articles citing ClimateGate. The *Washington Post* picked up the story on November 21, again quoting the “trick” email, and quoting climate-denier sources like the Competitive Enterprise Institute tit-for-tat as it quoted the scientists defending their private comments (Eilperin 2009a). The *Post* continued coverage on December 1, when Phil Jones, one of the participants in the “hide the decline” thread, announced he was stepping down from the Climate Research Unit. The *Washington Post* quoted Marc Marano, identified as the editor of a “climate skeptic blog,” as writing “One Down: ClimateGate Scientist Phil Jones to temporarily step down... pending investigation into allegations that he overstated case for man-made climate change” (Eilperin 2009b).



and the chairman of Hillary Clinton’s 2016 presidential campaign, was spear-phished, its contents exfiltrated and passed to Wikileaks. The hack took place in March 2016, and WikiLeaks published a selection of Podesta’s emails in a series of drops in October and November 2016.

From the Podesta emails emerged what would become the defining conspiracy theory of the 2016 campaign. The #Pizzagate conspiracy theory alleged that John Podesta, Hillary Clinton, and other prominent Democrats were involved in a pedophilic sex trafficking ring run out of the basement of a popular Washington, DC, restaurant and event venue, Comet Ping Pong. The theory was incubated on 4chan, 8chan, and two subreddits, r/The_Donald and r/pizzagate.⁵ #Pizzagate spread quickly through the rightwing/libertarian blogosphere, pro-Trump “fake news” sites,⁶ and Twitter. It made the jump to mainstream press coverage on December 4, 2016, when a 28-year-old man walked into Comet Pizza with an AR-15-style rifle and fired several shots in the restaurant. He later claimed that he was there to “self-investigate” the #Pizzagate theory and the claims that the restaurant was a front for child sex trafficking.

#Pizzagate sprang from a close reading of emails within the Podesta cache that mention performance art star Marina Abramovic, rock shows, pizza, Italian food, or handkerchiefs. The conspiracists allege that the Podesta emails contain a code wherein “cheese pizza” or other Italian food items are actually veiled references to child pornography or trafficked children or different sex acts. The theory extended beyond Comet Ping Pong to include allegations that various symbols on different storefronts on Comet Ping Pong’s block were also references to a secret pedophilia ring, that bands who had played at the venue were involved in the enterprise, or that the Instagram account of the restaurant’s owner (which was set to private after it began to attract abusive attention from Pizzagaters) contained incriminating images.

Most dramatically, #Pizzagate led to the arrival of

the “self-investigating” gunman at Comet Ping Pong in early December, but also inspired ongoing protests outside the restaurant; visits from (unarmed) individuals who sought to film, take pictures, or livestream from inside the restaurant; angry and harassing phone calls to Comet Ping Pong, other businesses implicated in the theory, and to individuals associated with these businesses; and acts of online harassment and doxxing. The theory is still evolving, having since grown to include the Crisis Actor conspiracy arc⁷ to explain the shooting incident on December 4.

BENJAMINIAN AURA AND STOLEN DATA

In discussing his concept of “aura” in “The Work of Art in the Age of Mechanical Reproduction,” Walter Benjamin (1969[1936]) notes the centrality of context, “[the object’s] presence in time and space” in the interpretation of a work of art, and the fundamental transformative effect of potential shifts in that context on the object’s reception and interpretation:

With the different methods of technical reproduction of a work of art, its fitness for exhibition increased to such an extent that the quantitative shift between its two poles turned into a qualitative transformation of its nature. This is comparable to the situation of the work of art in prehistoric times, when by the absolute emphasis on its cult value, it was, first and foremost, an instrument of magic. Only later did it come to be recognized as a work of art. In the same way today, by the absolute emphasis on its exhibition value the work of art becomes a creation with entirely new functions, among which the ones we are conscious of, the artistic function, later may be recognized as incidental (Benjamin 1969[1936]:225; emphasis added).

I posit that internal email databases, when exfiltrated by outsiders and dumped on the open web without the initial interpretive intervention of mainstream

-
- ⁵ The PizzaGate subreddit was eventually shut down by Reddit, inadvertently contributing to a central conspiratorial narrative of persecution by those in power with something to hide.
 - ⁶ The term “fake news” is used here to refer to purported news websites that sprung up during the 2016 election, often with the goal of producing salacious, compelling articles, predominantly pro-Trump, to attract clicks and social media shares.
 - ⁷ The Crisis Actor conspiracy arc is an overarching theory invoked to claim that any given tragedy (most notably the Sandy Hook massacre and 9/11) were actually dramatic performances, complete with actors playing the victims, victims’ families, and law enforcement, staged by the government to justify crackdowns on civil liberties and constitutional rights.

journalistic entities, experience an aura shift similar to the type Benjamin describes between private, secret cult objects and public, exhibition-oriented works of art. As the context of the data changes from an internal, local, in-group and personal context to a public, out-group context, different aspect of the data shift as well: its trustworthiness and reliability are affected, as well as its relationship to the people that produced it (its authors) and those people reading it (its audience).

A core aspect of the illicit aura is an assumption that the database in question was purposefully concealed from the public and required liberating. As something that was *stolen to be made public*, the database becomes something that was *kept hidden*. It wasn't simply *private*, it was *withheld*. The database itself and the information it contains experiences a contextual shift from mundane-communications-media-archive to illegally-obtained-evidence of *something*.

An illicit aura affects an object's very legibility, affecting how people and professional groups use and *don't* use such databases. Whereas an unconfirmed unverifiable data dump may be functionally invisible or at least unusable by the mainstream journalistic community in the initial period after its release, these same factors make these data dumps hypervisible and hypersalient for other communities. The manner of acquisition and release of the ClimateGate and Podesta email databases changed the way the databases could be thought *about* and thought *with*, foreclosing some avenues of interpretation, legitimization, and engagement and making others more attractive and likely to be pursued.

Three factors contribute to the development of this aura: manner of *acquisition*, manner of *release*, and manner of *reception*. The illicit aura can develop even in cases where journalistic attention is promptly paid to these dumps: the Podesta dump *did* attract attention from mainstream, professionalized journalistic commentators. Wherefore, then, #PizzaGate?

Whereas for ClimateGate, the inattention of mainstream journalists allowed the interpretive vacuum to develop, one that climate-change deniers rushed into, I here argue that the development of #PizzaGate had more to do with the dramatic manner of the release. WikiLeaks began dropping the Podesta emails an hour after the release of *Access Hollywood* hot mic video in which then-presidential candidate Donald Trump commented on, among other things, grabbing women's genitals without consent (Sharockman 2016). WikiLeaks's dumps of the emails, complete with Photoshopped header and Twitter card images,

occurred over multiple weeks, extending the drama of revelation and surprise. The ClimateGate dump was one event that became a central touchstone of discussion and worldbuilding for an established community; the Podesta emails were in essence many events chained together, each event a chance for journalists to lose interpretive authority. This multiple-event release model created more opportunities for conspiratorial interpretations to be repeated and gain traction among multiple audiences.

ASPECTS OF THE ILLICIT AURA

It is authoritative because it is raw: The illicit aura makes the untranslated nature of these databases a desirable virtue instead of a barrier to understanding. As collections of personal correspondence, in-group language abounds in these databases, along with imprecise, casual references, professional jargon and elisions, in-jokes, and other snippets of not-readily-accessible interpersonal ephemera.⁸ In theory, this type of data requires translations and contextualization for outsiders to understand. But when saddled with illicit aura, any attempts at expert-led contextualization become suspect, as anyone with access to the expert knowledge needed to provide such a translation is considered compromised before the fact. In the context of the illicit aura, the "raw" database is considered "honest," whereas any attempt at translation or contextualization would seem to open the door to interference by those who had tried to conceal the data in the first place.⁹

The modern virtue of corporate and governmental "transparency" is often interpreted as simply releasing data, lots of it, often in its rawest form. This is akin to a similar fetishization of source code as "ultimate performative utterance," as described by Wendy Chun (2008). "Raw data" are often viewed as those that correspond most to reality, containing the least bias or interpretive contamination.¹⁰ This view casts interpretive vacuums as somehow ideologically pure, and actively cuts against attempts at expert interpretation or curation, by casting it as unnecessary or intentionally misleading bias instead of a necessary step to aid understanding by the general public. This creates opportunities for dramatic, esoteric theories that often echo familiar narratives from popular culture to gain footholds.

Data dumps negate traditional sources of legitimization: Because the illicit aura contains an inherent skepticism of expertise as an interpretive asset, it also unseats the need for legitimization, particularly the role

8 In the Podesta cache, examples of these interpersonal ephemera include family recipes for walnut pizza, risotto, and Marina Abramovic's "Soul Cooking" fundraising dinner.

9 This predisposition is readily apparent in climate-denier treatments of the CRU emails and response of the scientific community to the theft. On November 28, the *Telegraph* published a column in which climate-denier Christopher Booker called the scientific community in consensus on anthropogenic climate change "Our hopelessly compromised scientific establishment" and calling the Royal Society "a shameless propagandist for the warmist cause" (Booker 2009).

10 For an example of this epistemic perspective, see Johnson (2015), who advises that 25% of your daily "information diet" be "raw information." For a rebuttal, see Gitelman (2013).

of the press as a legitimator and designator of information in the public interest.

A database that is dropped onto the open web and *not* picked up as an analytical source by news organizations can signal against its reliability as a primary source to other mainstream journalistic news organizations and *simultaneously* signal its attractiveness to conspiracy theorists by virtue of its being rejected by those organizations. While a newspaper that adheres to the professionalized ethics of journalism may ask “Is this source trustworthy?” or “Are the privacy violations inherent here justified by the value of the data?” or even banal considerations such as “Is there anything newsworthy here to begin with?” amateur analysts might see the refusals to take up the data as *evidence* of the database being suppressed, and go looking for what secrets it may contain.

At the point of release, decisions to filter or curate are themselves interpretive moves, as is the decision not to. Interpretive space is limited; each attempt to offer an interpretation claims ground that can then be considered “occupied territory” in the minds of a given audience. Intentionally holding that interpretive space open by declining to provide an interpretation upon the release of data that can be reasonably expected to be controversial is rhetorically similar to “just asking questions.” Those in the position to respond to such unfiltered data dumps the most quickly (with the most narratively complete story), and thus stake out the interpretive high ground, are those least bound by professionalized ethics and their attendant timelines.

The illicit aura cuts against the value of experts, but leave their role unfulfilled. It implicitly encourages each individual coming into contact with the information to “judge for themselves” its relevance and meaning. This is similar to Benjamin’s observations on the dissolution of barriers between the author, the audience, and the critic:

And today there is hardly a gainfully employed European who could not, in principle, find an opportunity to publish somewhere or other comments on his work, grievances, documentary reports, or that sort of thing. Thus, the distinction between author and public is about to lose its basic character.... At any moment the reader is ready to turn into a writer. As expert, which he had to become willy-nilly in an extremely specialized work process, even if only in some minor respect, the reader gains access to authorship.... Literary license is now founded on polytechnic rather than specialized training and thus becomes common property
(Benjamin 1969[1936]:232).

Excising the expert leaves a void which those who are already disinclined to believe experts and distrust established journalistic organizations, or who have pre-formed, usually negative opinions about the target of the data dump, rush into. But because the aura has rejected the ideas of experts, translation, and contex-

tualization, the type of judgment it encourages tends towards deeply personal, first principles-based styles of logical reasoning that both demand empirical experience and makes accessing the testimony of that experience (those of the in-group that produced the database) nearly impossible on an intellectual level.

I note here that recognizing the interpretive role of the press is not antithetical to the hacktivist ethos. Attacking social and civil norms is not a core function of hacktivism: there is nothing about data exfiltration that requires the delegitimization of expertise as an analytical resource. The Snowden/Greenwald relationship, joint projects between WikiLeaks and various established newspapers, and the collaboration between the Panama Papers leaker(s) and the International Consortium of Investigative Journalists are a few examples of hacktivist data exfiltrations or leaks that productively involved journalists to contextualize and translate reams of specialized, in-group data to the general public. Furthermore, performative hacktivist collectives such as Anonymous have implicitly acknowledged the role of the media as a legitimator for political activism, making space for that role in their actions, establishing #press channels on operation IRC servers or making their actions legible to the press through announcements and other releases.

Although hacktivists have at times endorsed the unfiltered data dumping practices critiqued here, it was not due solely to their identification as hacktivists or with hacktivist practices. Delegitimizing experts or the press within civil society is not a core aspect of hacktivist practice. When groups claiming the hacktivist mantle engage in tactics that undermine these roles or gesture at hacktivist politics to justify their use of these tactics, the audience would do well to question more closely why such tactics were chosen.

Secret things are always relevant: The illicit aura taints *private* with *secret*. The *personal* and the *incidental* are invested with importance because they are interpreted as *having been intentionally concealed*. Email correspondence is made of minutiae. The everyday communications of most people, even important people, are boring. They are cluttered with material relevant primarily to their existence as people, rather than to their power. However, the taint of *secrecy* renders the mundane extraordinary by interpreting everything through the lens of political power.

The illicit aura favors an interpretation that things are concealed only because they are incriminating. As #PizzaGate progressed, believers began to target people involved with the Comet Ping Pong, including bands that had performed there, which induced several of them to lock down their online presences or move offline entirely. “Going dark” may be viewed as a reasonable reaction to strangers suddenly accusing you of running a child sex ring. But #Pizzagaters interpreted privatizing of Instagram accounts, deleting Twitters, or altering of signs and websites to be evidence: evidence of guilt, evidence of concealment, evidence of *something* (Reply All 2016), anything other than the normal, emotional, self-preserving reaction of individuals

suddenly targeted by a mob.

In this interpretive mode nothing is accidental, but also nothing is merely *personal* or *social*. Similarly, the privatization of social media account is not a reestablishing of *privacy*, but is only an attempt to establish antidemocratic *secrecy* (Hofstadter 1964). There is a third concept at play in this eliding of the *personal* and the *secret*: *gossip*, particularly *gossip as informal social control and resistance*. James C. Scott discusses gossip as “a kind of democratic ‘voice’” (Scott 1985:282) through which social and political norms are both identified and defended:

Although it is by no means a respecter of persons, malicious gossip is a respecter of the larger normative order within which it operates. Behind every piece of gossip that is not merely news is an implicit statement of a rule or norm that has been broken. It is in fact only the violation of expected behavior that makes an event worth gossiping about. The rule or norm in question is often only formulated or brought

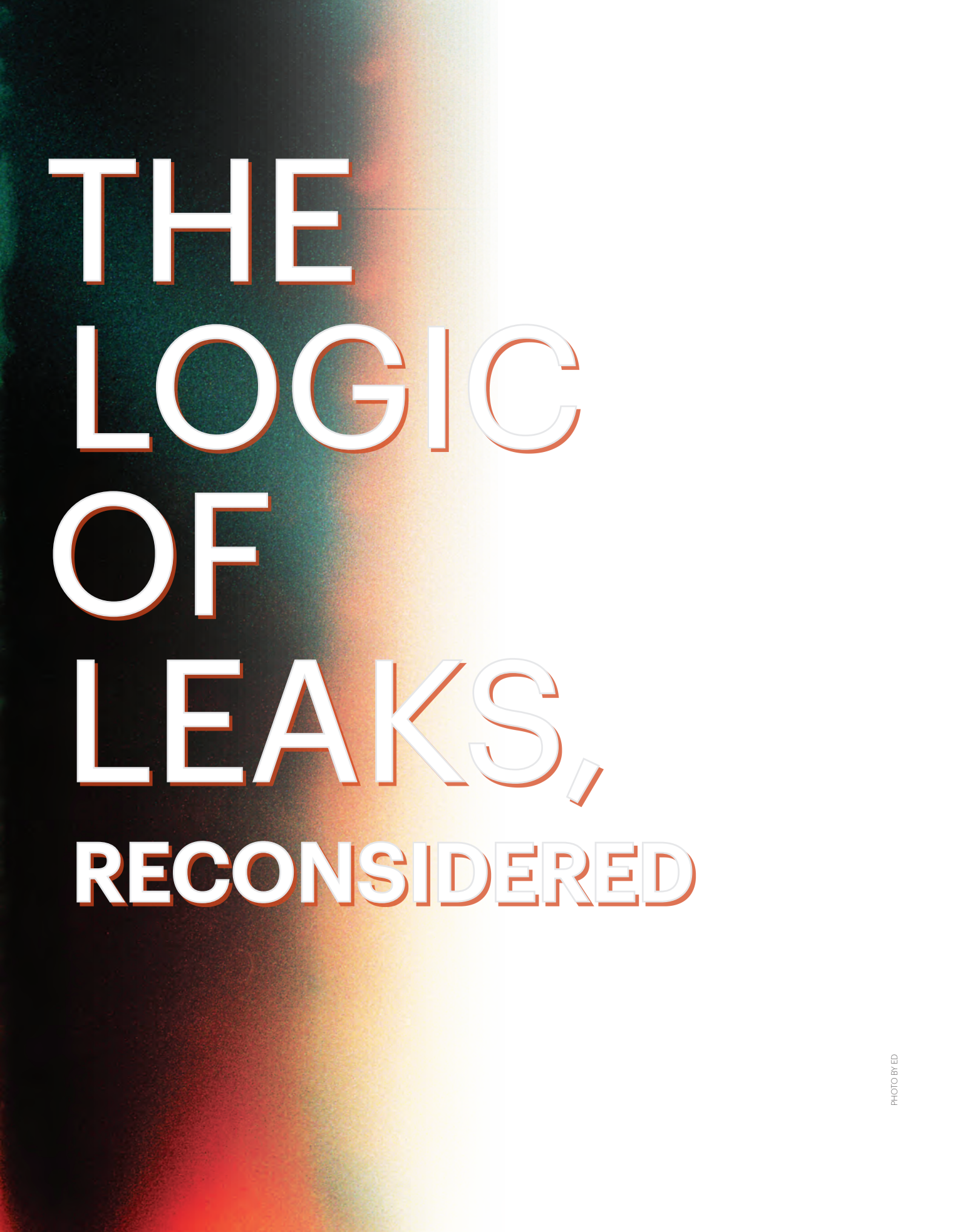
to consciousness by the violation itself
(Scott 1985:282; emphasis added).

The data dump provides the raw, irresistible material for gossip, and is cast as a resource to be mined for proof of the violations the illicit aura assumes are already there. The aura further implies a certain relationship between the audience, the stolen dataset, and its originators: *Hey you, Average Joe! Find out what the guys in power don't want you to know*. As Scott notes, only violations are worth gossiping about. The dataset is only worthy of attention if it contains transgressions, and as it is being presented as worthy of attention, it *must therefore contain transgressions*. The illicit aura creates an assumption of wrongdoing before any analysis takes place. ■

MOLLY SAUTER is a PhD candidate at McGill University in Art History and Communication Studies, and the author of *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*, published by Bloomsbury in 2014.

BIBLIOGRAPHY

- Benjamin, Walter. 1969 (1936). “The Work of Art in the Age of Mechanical Reproduction.” In *Illuminations*, edited by H. Arendt (pp. 217–253). New York: Schocken.
- Booker, Christopher. 2009. “Climate Change: This Is the Worst Scientific Scandal of Our Generation.” *The Telegraph*, November 28. <http://www.telegraph.co.uk/comment/columnists/christopherbooker/6679082/Climate-change-this-is-the-worst-scientific-scandal-of-our-generation.html>.
- Chun, Wendy Hui Kyong. 2008. “On ‘Sourcery’ or Code as Fetish.” *Configurations* 16(3):299–324.
- Clynes, Thomas. 2012. “The Battle Over Climate Science.” *Popular Science*, June 21. <http://www.popsci.com/science/article/2012-06/battle-over-climate-change?nopaging=1>
- Delingpole, James. 2009. “Climategate: The Final Nail in the Coffin of ‘Anthropogenic Global Warming?’” *Global Climate Scam*, November 21. <http://www.globalclimatescam.com/causeeffect/climategate-the-final-nail-in-the-coffin-of-anthropogenic-global-warming/>
- Eilperin, Juliet. 2009a. “Hackers Steal Electronic Data from Top Climate Research Center.” *Washington Post*, November 21. <http://www.washingtonpost.com/wp-dyn/content/article/2009/11/20/AR2009112004093.html>
- . 2009b. “Climate Scientist at Center of E-Mail Controversy to Step Down.” *Washington Post*, December 1. <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/01/AR2009120102737.html>
- Gitelman, Lisa. 2013. *Raw Data is an Oxymoron*. Cambridge, MA: MIT Press
- Hofstadter, Richard. 1964. “The Paranoid Style in American Politics.” *Harpers*, November.
- Johnson, Clay. 2012. *The Information Diet*. Sebastopol, CA: O’Reilly Media
- Reply All. 2016. “Episode 83: Voyage into PizzaGate.” Gimlet Media, December 8. <https://gimletmedia.com/episode/83-voyage-into-pizzagate/>
- Revkin, Andrew C. 2009a. “Hacked E-Mail Is New Fodder for Climate Dispute.” *New York Times*, November 20. <http://www.nytimes.com/2009/11/21/science/earth/21climate.html>
- . 2009b. “Hacked E-Mail Data Prompts Calls for Changes in Climate Research.” *New York Times*, November 28. <http://www.nytimes.com/2009/11/28/science/earth/28hack.html>
- Scott, James C. 1985. *Weapons of the Weak: Everyday Forms of Peasant Resistance*. New Haven, CT: Yale University Press.
- Sharockman, Aaron. 2016. “It’s True: Wikileaks Dumped Podesta Emails Hour After Trump Video Surfaced.” *Politifact*, December 18. <http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta-its-true-wikileaks-dumped-podesta-emails-hour-afte/>
- Watts, Anthony. 2009. “Breaking News Story: CRU Has Apparently Been Hacked—Hundreds of Files Released” *Watts Up With That?* November 19. <https://wattsupwiththat.com/2009/11/19/breaking-news-story-hadley-cru-has-apparently-been-hacked-hundreds-of-files-released/>



THE
LOGIC
OF
LEAKS,
RECONSIDERED

Are leaks fast and slow? Does their “illicit aura” matter? Naomi Colvin dives into the debate about leaking and the politics of journalism today.

WHAT IS IT ABOUT LEAKS THAT MAKES THEM DIFFERENT FROM other news events? If the statements of governments and media organizations are anything to go by, it’s file size that counts.¹ The UK Law Commission’s recent consultation document on the Protection of Official Data suggests that maximum sentences for unauthorized disclosure under the Official Secrets Act ought to be increased because “[i]n the digital age, the volume of information that can be disclosed without authorization is much greater” (United Kingdom Law Commission 2017).

Media organizations, too, have adopted this metric. When reporting on the Panama Papers began in 2016, the primary claim made by the news organizations involved was that it was big, very big. *Sddeutsche Zeitung*, the original recipient of the data from the Mossack Fonseca law firm, claimed that the 119 million documents were “more than the combined total of the WikiLeaks Cablegate, Offshore Leaks, Lux Leaks, and Swiss Leaks” (Obermeier et al. 2016) and produced an infographic comparing those respective disclosures on the basis of their gigabyte count. *The Guardian* confidently stated that the Panama Papers were “history’s biggest leak,” again suggesting that file size should be directly correlated with significance (Harding 2016).

In fact, file size as a metric tells you next to nothing about the volume of the information actually disclosed to journalists, never mind the popular resonance or political valency of particular revelations.² It also places a great deal of emphasis on the role of traditional gatekeepers of information. Or, to put it another way, as a way of understanding leaks, it misses almost everything that is important.

What primarily distinguishes leaks from the other unofficial disclosures of information that are the journalist’s stock in trade is not the amount of information disclosed to journalists, but the amount of original source material made accessible to the public. This public input changes the dynamics of how news is produced and how narratives are formed, bringing a multiplicity of voices into areas of decision-making that were formerly reserved

for insiders. In the absence of a clear understanding of how leaks land in particular instances and what factors inform their reception, some have been tempted to see the dispersion of interpretative power as a problem: this, too, is mistaken.

Adam Fish and Luca Follis’s essay on the “temporality” of leaks (p. 44) points toward a promising way of thinking about large-scale document disclosures. It is clearly the case

that the major disclosures of the past seven years have had a long political half-life. This persistent—“slow”—quality, the ability to inform political debate long after most news stories have been forgotten, is a key defining quality of leaks and one of the major reasons why they have become a significant political phenomenon.

The consequences of Chelsea Manning’s whistleblowing are pre-eminent and inescapable in any serious treatment of this topic. The U.S. State Department cables that WikiLeaks began to publish in November 2010 remain a standard reference point for anyone writing about international affairs nearly seven years later, while the Afghanistan and Iraq War logs continue to be the subject of academic analysis in fields as diverse as epidemiology, statistics, geography, and war studies.³

Manning’s disclosures remain unsurpassed in their global impact, but less comprehensive document collections have also had a longer shelf life than might be expected. In early 2010, hacktivists liberated a cache of emails from U.S. security consultancy HB Gary. This brought to the surface at least one news story of major significance—that Bank of America had commissioned a group of private companies to disrupt WikiLeaks and its support base—but also formed the basis of Project PM, a crowdsourced investigation into the organizational ecology of security contractors in the United States that was only disrupted by the arrest of its founder and moving spirit in 2012.

What these examples have in common is that original source documents were made available to the general public in the form of a searchable database and that this was an integral part of the publication strategy, not an afterthought. Particular groups of documents lend themselves more easily to being organized in a database than others (the State Department cables, prepared in a consistent format with unique identifiers and metadata tags designed to be machine readable, are again a key example), but searchable archives are an important reason why some document caches are able to persist beyond short-term news values.

1 For clarity, in this essay I’m using “leak” as a shorthand for “major unauthorized disclosure of digital information.”

2 Uncompressed pdfs comprising scans of thousands of pages might well take up more hard disk space than a million pages of plaintext plus metadata. It does not follow that they contain a greater volume of useful information.

3 In May 2016, for instance, at least five separate New York Times articles referred to the State Department Cables (Timm 2016).

Fish and Follis recognize that publication strategy influences how leaks are received, but no disclosure happens in a vacuum. They attempt to draw distinctions between “fast” and “slow” leaks on the basis of purposeful editorial decision-making—how much information is being released? Is it tied in to a particular news event?—but their analysis fails to take sufficient account of the context in which publication decisions make a difference. As a result, they fall into the trap of comparing information environments—like election campaigns and court cases—rather than the role leaks play within them. A separate problem is that their characterization of publication strategies doesn’t quite fit what actually happened. This, for example, is what they say about Edward Snowden’s “slow” disclosures, which they contrast with the Democratic National Committee (DNC) and Podesta emails:

Although the[y] sought to influence then-current events, the full impact of the [Snowden] disclosures is oriented toward the *longue durée* and the extensive digital archive of American global panopticism that will be preserved in posterity. (Follis and Fish, 2017)

In fact, a major omission in the Snowden publication strategy was precisely that there was no provision made for producing a searchable archive to ensure that once documents were put into the public domain, they remained accessible after individual news stories had been and gone. Compounding the problem was that extracts from the Snowden archive were not published in a consistent way that allowed readers to easily connect insights to individual documents, a situation exacerbated by a degree of inconsistency and repetition within the archive itself.⁴

In other words, news values dominated entirely over the interests of researchers, or even those with a professional interest in, say, mitigating the impact of National Security Agency (NSA) operations against the Tor network or commercial infrastructure. Individual stories were timed for maximum political—and sometimes disruptive—impact. To take two examples from June 2013, the publication of Presidential Policy Directive 20 made public America’s offensive cyber warfare ambitions on the eve of a summit with China (Greenwald and MacAskill 2013). The revelation of NSA operations against universities and other institutions in Hong Kong bolstered Edward Snowden’s personal position at a time when his extradition from the territory was still a possibility, bringing out protesters in his defense (Lam 2013). Despite this, no provision was made for collating stories in one place, still less producing an archive of source documents. The two full-text search engines that do exist were created by third parties independent of the publication process on the basis of open-source research.

If the Snowden revelations have had a longstanding impact, it was due to the momentous and specialized nature of their content, rather than a publication strategy intended to maximize the ability for nonspecialists to generate insights into the documents after the news cycle had moved on.

Although the presentation of documents has improved markedly since the first Snowden revelations were published in mid-2013, the experience shows a continuing need for agreed publication standards for contentious document sets.⁵

In contrast to the Snowden revelations, the DNC and Podesta emails, which were published in stages from July 22 to October 7, 2016, respectively, were published in searchable form from the outset. Fish and Follis characterize these as “fast” releases that defied comprehension; what this misses is that the context into which they were released is key.

The Podesta emails in particular were published in the middle of a particularly acrimonious and negative election campaign. Elections form a very particular kind of information environment: fast-moving and elaborately choreographed with a disproportionate emphasis on gaining short-term advantage. One of the few points of concurrence in the voluminous political science literature on election campaigns that the impact of “shocks” and individual campaign events tends to decay quickly (Jacobsen 2015).

It is precisely this short-termism that makes what election consultant Lynton Crosby is reported to have called the “dead cat on the table” strategy viable: campaign timetables move so quickly that it is rarely necessary to “win” an argument on a factual basis to seize attention from your opponent. In fact, putting together a coherent argument is an inefficient strategy when a calculatedly lurid non sequitur will serve just as well.⁶

Assessment of the ultimate impact of the DNC and Podesta emails on the U.S. presidential election will have to be left to subsequent researchers, but the episodic nature of their release, their capacity to be searched for new insights, and their resonance with already latent concerns about the Clinton candidacy meant they were not “fast” in the context of the election campaign, as Fish and Follis would have it. In contrast with the various leaked stories that were published by the *New York Times* and *Washington Post*, the DNC and Podesta leaks were, in fact, subversively slow.

In fact, compared with stories appearing in a similar context, leaks are generally “slow,” and the greater the opportunities for public engagement, the slower they are likely to be. Precisely because they have a long half-life and can be interrogated by nonspecialists, leaks

4 The two projects are Courage’s Snowden Doc Search (<https://search.edwardssnowden.com/>) and Canadian Journalists for Free Expression’s Snowden Archive (<https://snowdenarchive.cjfe.org/greenstone/cgi-bin/library.cgi>). I am involved in the former project.

5 Redaction is a related area where agreed standards would be useful. One interesting issue that emerged in relation to the Snowden documents is the potential for confusion in cases where there might be privacy as well as security reasons for redacting particular details. See, for example, the representation of the author of an NSA instructional PowerPoint presentation as an “agent” (Cesca 2014).

6 The utility of the dead cat strategy is such that it proved strikingly effective in the UK General Election of 2015 even though the public had long been primed to look out for it (see Delaney 2016).



"INTERNATIONAL ALPHABET FLAGS" BY J. LANDECKER

accompanied by publicly accessible archives also deprecate the role of traditional gatekeepers. For Fish and Follis, the importance of deeming the DNC and Podesta releases “fast” is to convey the sense that information entered the public domain with such rapidity that it effectively defied rational analysis, leading to the proliferation of conspiracy theories.

Molly Sauter, in another essay in this issue (p. 51), makes a related argument using the same case study, specifically that leaks of emails by outside parties are liable to become fruitful ground for conspiracy “without the initial interpretive intervention of mainstream journalistic entities.”

Sauter argues that although mainstream journalists did not ignore the Podesta emails, their episodic release “extended the drama of revelation and surprise” wherein “journalists lost their interpretative authority.” This is deemed problematic because individuals without journalistic expertise and those with existing ideological standpoints are liable to mistake the “illicit aura” of exposed intragroup communications for the public interest. In distinguishing between leaks that emerge from within organizations and others, Sauter implies that this misapprehension about what constitutes the public interest applies as much to the sources of stories as it does to their readers.

There are a number of objections to make to these lines of argument. First and foremost, pizza-themed conspiracy theories were clearly neither the dominant nor the most politically relevant narratives to emerge from either set of emails, which were covered extensively by major media organizations. The initial publication of the DNC emails came on July 22, 2016, and the Podesta emails on October 7. Within 24 hours, mainstream outlets identified the DNC’s conduct during the primary campaign and

Hillary Clinton’s paid speeches as the most significant content of each release. (Chozik et al. 2016; Shear and Rosenberg 2016). Controversies about the publication of the document sets ran alongside these reports, but it is simply wrong to assert that the substantive content of the releases was ignored.

Neither is it the case that the 2016 email releases failed to inform substantive analyses beyond the immediate context of the election itself (Sifry 2017). Observers have noted that the *New York Times*, if offered the DNC material, would likely also have chosen to publish the material in some form (Goldsmith 2017). Controversies about the ultimate sourcing of the material and partisan concerns aside, the assertion that there was no public interest justification for the releases seems misplaced.

So far, so typically leaky. The second, more interesting line of argument is that readers are dependent on journalists to properly interpret the content of disclosures. While the information in some archives—the Snowden documents, for instance, or some of the financial disclosures coordinated by the International Consortium of Investigative Journalists—may present technical obstacles for nonspecialist readers, the gist of the Fish and Follis and Sauter articles is that readers are liable to misinterpret documents produced in ordinary professional contexts, either through an inability to parse large quantities of information or a misapprehension about what is newsworthy.

What these arguments miss is that most of the major contemporary leaks have seen the professional and nonprofessional spheres working in tandem. The accessibility of source material to the public, combined with the common presence of interested parties (journalists, subject experts, readers) on social media, has produced a powerful dynamic of parallel scrutiny wherein the two

K 
KILO
**"I WISH TO
 COMMUNICATE
 WITH YOU"**

U 
UNIFORM
**"YOU ARE
 RUNNING
 INTO DANGER"**

spheres inform, criticize, and check the excesses of each other. This is a change of real significance: the formation of mainstream narratives is no longer the closed process it used to be when readers' main route for response was the newspaper Letters to the Editor pages.

To return to Chelsea Manning's disclosures for a moment, it is easy to forget how reporting on the State Department cables proceeded. The initial wave of mediated reporting via WikiLeaks's major media partners *El Pais*, *Le Monde*, *Der Spiegel*, *The Guardian*, and the *New York Times* began on November 28, 2010. Among substantial stories such as Saudi lobbying of the United States to take a hard line toward Iran and the United States pressuring other countries not to pursue extraordinary rendition cases through their domestic courts, Cablegate's first 24 hours included a host of stories about U.S. diplomats' less-than-flattering descriptions of world leaders (Chen 2010).

Based on that initial wave of reporting, opinion pieces were written predicting that the political impact of the cables' release would be limited, aside from inadvertently reinforcing the status quo. It was only a week after that this was comprehensively refuted when cables about Tunisia, distributed by Lebanese paper *Al Akhbar* and the Tunileaks website set up by nawaat.org, became a rallying point for local activists, helping to spark off the Arab Spring and the global wave of democratic revolts that followed.⁷

This almost unprecedented popular energy was reflected back in crowdsourced activity around the searchable cable archive, which both collated and criticized the output of major media on blogs like WLPress and WikiLeaks Central, and sought to locate, discuss, and publicize unreported stories under the hashtag #wlfnd. One of the major stories to come out of the archive

was actually located this way by independent journalist Kevin Gosztola. The discovery of a previously secret report on U.S. war crimes in Iraq written by the United Nation Special Rapporteur on Extrajudicial, Summary or Arbitrary Execution, was duly picked up by others and led directly to the Maliki government refusing to renew U.S. troops' immunity from prosecution.⁸

The checking function works in the other direction too. In August 2012, crowdsourcing on another WikiLeaks release, the Global Intelligence (GI) Files, a collection of emails drawn from the hack of private intelligence firm Stratfor, identified a surveillance system purchased by a selection of U.S. public authorities called Trapwire. A great deal of momentum built up online about Trapwire, which had not featured in any of the professional reporting on the GI Files. Speculation about Trapwire's capabilities was combined by a growing frustration that mainstream journalists were not picking up the story. Intense lobbying of reporters on social media went on for several days.

This interaction paid dividends, although perhaps not quite in the way the crowd tweeting about #trapwire envisaged. The checking function provided by those who had seen a few overblown Homeland Security sales pitches before resulted in a story about petty corruption and cronyism in the security industry rather than advanced secret surveillance capabilities (*that* story was to emerge 10 months later; Shachtman 2012).

The Trapwire episode offers a direct response to Molly Sauter's concerns about "unmediated" leaks: interpretation is a two-way street. The initial crowdsourced reaction to the raw information in the GI Files may have been mistaken but, without the pressure of the crowd, what turned out to be a rather revealing story about how the industry works would have been missed entirely. Had the professional reporting community not acknowledged the



TUNILEAKS
 A project
 run by
 Nawaat.

7 See Anne Applebaum's article in the Washington Post (2010), a hot take that has not stood the test of time.

8 Kevin Gosztola's article (2011) originally appeared in the Dissenter column at firedoglake. For the impact of the story, see MacAskill (2011) and Karon (2011).

newsworthiness of issues identified by their nonprofessional counterparts—despite initial resistance—the two communities could well have become profoundly alienated from each other. There are probably lessons to be learned here.

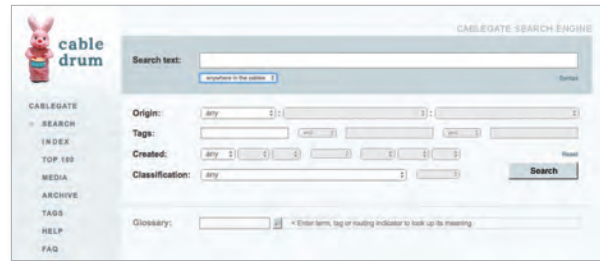
At a rather fundamental level, both the Fish and Follis and Sauter accounts of the Podesta emails are skewed by a profound unease about the results of the 2016 U.S. presidential election and speculation that Russian state actors may have had a hand in their sourcing. Should we be having second thoughts about the wisdom of anonymous leaks? Has there been a fundamental change that makes it naive to be drawing parallels with the halcyon days of 2010–2012, when leaks felt like a more straightforward emancipatory proposition?

Moments of high drama have a way of drawing concerns and reservations from those who are otherwise sympathetic to the case for disclosure. Long-term critic of government secrecy Steven Aftergood explained his reservations about WikiLeaks just as the Manning disclosures were beginning back in 2010. Three years later, NSA whistleblower Bill Binney’s initial reaction to Edward Snowden’s revelations was also qualified, if generally supportive.⁹

The DNC and Podesta email disclosures are not outlier events that bear no relation to the leaks that came before them, and it’s important not to lose sight of those continuities. Parallel scrutiny, too, has not disappeared: as I write this article, lively debate is ongoing about the content and presentation of WikiLeaks’s #Vault7 release of CIA malware. Nevertheless, I do share some concerns about the environment for leaks in 2017.

A limitation of parallel scrutiny is that it requires some kind of common forum to operate properly. In that regard, the development of self-contained “distinctive and insular” media ecosystems that limit the opportunity for encountering a broad range of dissenting views is potentially problematic (Benkler et al. 2017). In addition, researchers have found respondents with high degrees of political knowledge and low levels of trust in established institutions to be especially prone to the kinds of motivated reasoning that are often labeled as conspiracy theories. The concerns that preoccupy Fish and Follis and Sauter are closely related to these dynamics (Miller et al. 2016; Nyhan 2017; Swift 2016).

Neither an appeal to authority—as Sauter suggests—nor Fish and Follis’s recommendation of publication strategies that align “time and scale” will be sufficient to resolve this situation. A central difficulty is that although some conspiracy theories might appear irrational, it does not follow that a diminished degree of trust in established institutions is also irrational. The emergence of insular and alienated information communities reflects a endemic political problem that is not restricted to the public sphere.



Leaks have become politically important because, at a time when trust in institutions is collapsing across the board, they represent a rare instance of elite power being dissipated in a way that has genuinely broadened participation and brought with it surprisingly large social benefits. Without the parallel scrutiny of journalists, experts, readers, and researchers, Cablegate would not have been the phenomenon it was: journalists alone would not have been able to generate anything like the same world-changing, emancipatory impact. The practice of journalism has changed as a result for the better (Benkler 2013).

It seems strange to have to assert that increasing access to knowledge is more likely to present benefits to society than not, but that appears to be the state of the debate in 2017. The shock of the Trump vote, and the Brexit vote, has produced an understandable hunger for explanation, accompanied by a crisis of intellectual confidence.

Journalistic practice is undergoing a period of radical upheaval in the digital age and leaks are a major part of the process whereby the formation of narratives has been opened up to wider scrutiny. Aspects of 2016’s agenda will inevitably give pause to those who closely followed the contours of Cablegate, but scholars of these trends must take care not to confuse cause and effect. The development of isolated information communities has not been caused by leaks, but it has made clearer some of the social and political problems that have been coming to a head since 2008. Not least of these is a widespread sense of institutional failure and corresponding alienation from conventional political narratives.

Leaks, particularly when accompanied by public access to source material, have provided some of the few instances where that divide has been successfully negotiated. Those who misidentify leaks as the problem therefore run the risk of embracing deeply anti-democratic norms. Without a reality check, this could become self-perpetuating. ■

NAOMI COLVIN is Beneficiary Case Director at the Courage Foundation, which supports whistleblowers, hacktivists and other truth-tellers who have made import contributions to the historical record.

⁹ For Steven Aftergood’s reservations, see Aftergood (2010; the comments section captures the heady atmosphere of 2010 as well as anything else you’ll find); Bill Binney’s initial concerns about Edward Snowden’s disclosures may be found at Eisler and Page (2013).

BIBLIOGRAPHY

- Aftergood, Steven. 2010. "Wikileaks Fails "Due Diligence" Review." *Secrecy News*, June 28. <https://archive.is/qhl12#selection-251.0-251.38>
- Applebaum, Anne. 2010. "Why the WikiLeaks Cables Aren't as Threatening as Advertised." *Washington Post*, December 7. <http://www.washingtonpost.com/wp-dyn/content/article/2010/12/06/AR2010120605409.html>
- Benkler, Yochai. 2013. *WikiLeaks and the Networked Fourth Estate*. London, UK: Palgrave.
- Benkler, Yochai, Robert Faris, Hal Roberts, and Ethan Zuckerman. 2017. "Study: Breitbart-Led Right-Wing Media Ecosystem Altered Broader Media Agenda." *Columbia Journalism Review*, March 3. <http://www.cjr.org/analysis/breitbart-media-trump-harvard-study.php>
- Cesca, Bob. 2014. "NSA Worker's Identity Exposed in Poorly-Redacted Snowden Document." *The Daily Banter*, February 1. <http://thedailybanter.com/2014/02/the-name-of-an-nsa-agent-exposed-in-poorly-redacted-snowden-document/>
- Chen, Adrian. 2010. "All the Hottest Diplomatic Gossip from the latest Wikileaks." *Gawker*, November 28. <http://gawker.com/5700705/all-the-hottest-diplomatic-gossip-from-the-latest-wikileaks>
- Chozik, Amy, Nicholas Confessore, and Michael Barbaro. 2016. "Leaked Speech Excerpts Show a Hillary Clinton at Ease with Wall Street." *New York Times*, October 7. <https://www.nytimes.com/2016/10/08/us/politics/hillary-clinton-speeches-wikileaks.html>
- Delaney, Sam. 2016. "How Lynton Crosby (and a Dead Cat) Won the Election: 'Labour Were Intellectually Lazy.'" *The Guardian*, January 20. <https://www.theguardian.com/politics/2016/jan/20/lynton-crosby-and-dead-cat-won-election-conservatives-labour-intellectually-lazy>
- Eisler, Peter, and Susan Page. 2013. "3 NSA Veterans Speak Out on Whistle-Blower: We Told You So." *USA Today*, June 16. <http://www.usatoday.com/story/news/politics/2013/06/16/snowden-whistleblower-nsa-officials-roundtable/2428809/>
- Follis, Luca, and Adam Fish. 2017. Half-Lives of Hackers and the Shelf Life of Hacks. *Limn*. <http://limn.it/half-lives-of-hackers-and-the-shelf-life-of-hacks/>
- Goldsmith, Jack. 2017. "Journalism in the Doxing Era: Is Wikileaks Different from the New York Times?" *Lawfare*, January 16. <https://www.lawfareblog.com/journalism-doxing-era-wikileaks-different-new-york-times>
- Gosztola, Kevin. 2011. "Attention Called to Major War Crime Coverup by Wikileaks Cable." *Shadowproof*, September 1. <https://shadowproof.com/2011/09/01/major-war-crime-coverup-called-attention-to-by-wikileaks-cable/>
- Greenwald, Glenn, and Ewen MacAskill. 2013. "Obama Orders US to Draw up Overseas Target List for Cyber-Attacks." *The Guardian*, June 7. <https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas>
- Harding, Luke. 2016. "What Are the Panama Papers?" *The Guardian*, April 3. <https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers>
- Jacobsen, Gary C. 2015. "How Do Campaigns Matter?" *Annual Review of Political Science* 18:31-47.
- Karon, Tony. 2011. "Iraq's Government, Not Obama, Called Time on the U.S. Troop Presence." *Time*, October 21. <http://world.time.com/2011/10/21/iraq-not-obama-called-time-on-the-u-s-troop-presence/>
- Lam, Lana. 2013. "Edward Snowden: US Has Been Hacking Hong Kong and China for Years." *South China Morning Post*, June 13. <http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china>
- MacAskill, Ewen. 2011. "WikiLeaks Disclosure Reopens Iraqi Inquiry into Massacre of Family." *The Guardian*, September 2. <https://www.theguardian.com/world/2011/sep/02/wikileaks-iraq-massacre-inquiry>
- Miller, J. M., K. L. Saunders, and C. E. Farhart. 2016. "Conspiracy Endorsement as Motivated Reasoning: The Moderating Roles of Political Knowledge and Trust." *American Journal of Political Science* 60:824-844.
- Nyhan, Brendan. 2017. "Why More Democrats Are Now Embracing Conspiracy Theories." *New York Times*, February 15. <https://mobile.nytimes.com/2017/02/15/upshot/why-more-democrats-are-now-embracing-conspiracy-theories.html>
- Obermeier, Frederik, Bastian Obermayer, Vanessa Wormer, and Wolfgang Jaschensky. 2016. "About the Panama Papers." *Sueddeutsche Zeitung*. <http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/>
- Shachtman, Noah. 2012. "Trapwire: It's Not the Surveillance, It's the Sleaze." *Wired*, August. <https://www.wired.com/2012/08/trapwire-strafor-biz/>
- Shear, Michael D., and Matthew Rosenberg. 2016. "Released Emails Suggest the DNC Derided the Sanders Campaign." *New York Times*, July 22. <https://www.nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html>
- Sifry, Micah. 2017. "Obama's Lost Army." *New Republic*, February 9. <https://newrepublic.com/article/140245/obamas-lost-army-inside-fall-grassroots-machine>
- Swift, Art. 2016. "Americans' Trust in Mass Media Sinks to New Low." *Gallup*, September 14. <http://www.gallup.com/poll/195542/americans-trust-mass-media-sinks-new-low.aspx>
- Timm, Trevor. 2016. "President Obama, Pardon Edward Snowden and Chelsea Manning." *The Guardian*, June 1. <https://www.theguardian.com/commentisfree/2016/jun/01/edward-snowden-chelsea-manning-barack-obama-pardon>
- United Kingdom Law Commission. 2017. *The Protection of Official Data*. <http://www.lawcom.gov.uk/project/protection-of-official-data/>



Interview: Lorenzo Franceschi-Bicchierai

Journalist **Lorenzo Franceschi-Bicchierai** talks with *Limn* about the details of the DNC hacks, making sense of leaks, and being a journalist working on hackers today.

Gabriella Coleman: As you know well, the DNC [Democratic National Committee] hack and leak were quite controversial, with a batch of commentators and journalists debating whether the contents of the email were newsworthy, and another batch of commentators assessing their geopolitical significance. Our *Limn* issue features pieces that in fact assess the importance of the DNC hack in quite distinct ways: one author taking the position [that] the emails lacked consequential news, while another author forwards a public interest defense of their release. As someone who has covered these sorts of hacks and leaks, how important was the DNC-Podesta hack? And in what way? Does it represent a new political or technical threshold?

Lorenzo Franceschi-Bicchierai: They were definitely relevant from a geopolitical standpoint, if you will. All signs point to Russia. So, this was a nation-state hacking a legitimate target from the point of view of their interests, and from the intelligence point of view, these were legitimate targets. So, that's not too crazy, and this is something that would get a lot of people on Twitter saying, "Well, spies are gonna spy." But I think it was interesting because, of course, it did cross a threshold or line, if you will. Because this wasn't just hacking and spying on them, it was putting everything in the open. They published the stolen data through WikiLeaks, they published through their own leaking platforms, they had this website called DC Leaks, and they had the famous Guccifer 2.0. They had all kinds of channels and they were actually very good at using multiple channels just to get as much attention as possible, even if the content wasn't actually that compelling.

GC: What you're suggesting is that the trade craft of state spying has always worked on these discretionary channels, that is, back channels that only the intelligence world has access to. And all of a sudden here's this moment where they decide to move everything from the back stage to the front stage.

LFB: Yes that's definitely a good way to put it. Spies, by definition, work in the shadows. We know about intelligence operations when they leak or when someone talks, and sometimes it's years later. At that point it's not even that newsworthy. But in this case, it all unfolded in real time, which was very interesting. The big question in the DNC-Podesta hack that we'll probably never know the answer to—if the DNC and CrowdStrike didn't come out with the attribution, if they didn't come out saying this is Russian intelligence—is: would the hackers and the Russian government have responded in the way that they have? By systematically leaking documents and slowly dripping information? I don't know. Maybe they would, maybe they wouldn't....

GC: Ah, that's a good point. Did CrowdStrike call out Russia before the material was leaked?

LFB: Yes, CrowdStrike attributed the attack to Russia on June 14, and Guccifer 2.0 came out on June 15. But it's important to note that there was another website, also linked to Russia, that started leaking stuff before that. The site was called DCLeaks and it started publishing stolen documents just a few days before CrowdStrike went public, but it's almost like no one noticed it right away. DCLeaks published hacked emails from Hillary's [Clinton] staff on

June 8, according to the Internet Archive. This means that perhaps Russia was already going to leak documents, and CrowdStrike's accusation only accelerated the plan. Perhaps they were planning to release the more interesting stuff closer to the election, but they felt like they somehow had to respond to the public accusation. Who knows!

GC: Your point is an important one because it suggests that perhaps the execution of this hack and leak was experimental and it also seemed quite sloppy as well.

LFB: Maybe it was the plan all along. Even if it wasn't, it definitely didn't look very well planned at times. I think the best example is this Guccifer 2.0 persona. He—let's say "he," just because they claim to be male—he showed up a day after the CrowdStrike and Washington Post reports and it definitely seemed like the character was a little bit thrown together. He claimed to be a hacktivist trying to take the credit he deserved, which would have made sense if he really wasn't a Russian spy or someone working for Russian spies. But then he chooses the name of another famous hacker as his own, simply adding the 2 in front of it and—you know this better than me—some hackers can have a big ego; why not just come up with a different name?

GC: True, they want recognition for their work.

LFB: Just like writers. You know, it's like, "I wanna have people know that I did something that I think [is] awesome and worthy of recognition" thing. We all have our egos. And using the same name as another famous hacker from years ago just sounds very strange. I don't think I've ever seen that before.

GC: It's funny to imagine the meeting where this happened in some nondescript Russian intelligence office where someone's like, "All right, we are looking for a volunteer to play the role of the hacker...." And whoever got nominated or volunteered didn't do a very good job. Which is a little bit weird because Russia does seem to obviously have a lot of talent in this area.

LFB: Yeah, they seem to be very good with these information campaigns and deception campaigns, and stuff like that. It's always possible that they contracted this out to someone. **Maybe they thought this would be an easy job, but somehow it snowballed.**

GC: Let's turn to the next question, which is related to the first one. Many of these recent leaks, from Cablegate to the DNC leaks, are massive, and the journalistic field mandates quick turnaround so that you have to report on this material very quickly, right? What interpretive or other challenges have you faced when reporting on these hacks and leaks?

LFB: Yes, there's many. You definitely nailed one of the biggest ones: the quickness and fast-paced environment. And I think that sources are catching up to it, or sources of leaks and publishers of leaks, I guess. There are still large data dumps that just drop out of the blue. And everyone scrambles to search through them. But, for example, WikiLeaks have become very good at staging leaks in

phases. They slowly put out stuff because they know very well that they're going to extend the time that they cover [an issue], that they will get attention. With the Podesta leaks, it was almost every day that there was something new.

GC: Right, that was very well imed and orchestrated.

LFB: And it wouldn't have worked if they had just dumped everything the first day. Because we're humans too and we get overwhelmed. And everyone gets—readers get overwhelmed too. And if you dump 3,000 emails, you're just going to get a certain level of attention. If you do it in segments, and in phases, then you get more attention. I think sources are catching up to that.

But the other challenge is that sometimes you get things wrong, or you just assume that the documents are correct, and you publish the story based on the documents, saying, "Oh, this happened." And maybe you haven't had time to verify. There's also competition. You always want to be the first. The ideal scenario is always getting something exclusively so you have the time to go through it. The advantage, though, of having stuff in the public is the crowdsourcing aspect. So, for example, when The Shadow Brokers data came out, pretty much everyone in the infosec world spent the entire day, all their free time, looking through what had come out. And they published their thoughts and their findings in real time on Twitter.

For example, one of these people was Mustafa Al-Bassam. So that's something that maybe you can't get if you have information exclusively. And then getting something exclusively obviously has its advantages, but that's one of the drawbacks. You don't get the instant feedback from a large community.

GC: And that seems to have happened with the recent CIA-WikiLeaks leak as well.

LFB: And it happened with the Hacking Team leak. It was very useful for me and others to keep an eye on Twitter and see what people found because there was just so much data... That's also exactly what happened when the Shadow Brokers dumped hacking tools stolen from the NSA [National Security Agency]. These weren't just emails or documents that a lot of people could look at and understand or try to verify. These were sophisticated pieces of code that needed people with a lot of technical skills to understand and figure out what they were used for and whether they worked. Luckily there's a lot of very good infosec people on Twitter and just following their analysis on the social network was really useful for us journalists.

GC: Based on what you've seen and reported, do you think that we—not just lay people, but experts on the subject—are thinking clearly on vulnerability? Is there a focus in the right place on threat awareness, technical fixes, bug bounties, vulnerability disclosure, or do you think people are missing something or are misrepresenting the problem?

LFB: In the infosec world there's sort of a fetish for technical achievements. And it's understandable, it's not the only field. But sometimes this fetish for the latest, amazing zero-day, or the new proof-of-concept way to put ransomware on a thermostat—which, you know, is tough, I wrote a story about

it—but sometimes it makes us forget that these are still kind of esoteric threats, maybe, and also unrealistic threats. In the real world, what happens usually is phishing, or your angry partner or ex-partner still knows your password to your email and after you break up they get into your email... stuff like that. Some cybersecurity expert might scoff at this and say, “That’s not hacking,” but that’s what hurts the most, though.

And I think that, for example, Citizen Lab has done a great job of highlighting some real-world cases of abuse, of hacking tools used against regular people, but also dissidents and human rights defenders. And in many of those cases, there was no fancy exploit, there was no amazing feat of coding or anything involved. It was just maybe a phishing email or phishing SMS [text message]. So I think that we could all—both journalists and the industry—do a better job of explaining the real risks to an average person and telling them what to do, because just scaring them is not going to help.

GC: Yeah, this is a great point and reminds me of considering public health-type campaigns: in this case, a concerted security hygiene program to teach everyday people the basics of security. The history of biomedical public health campaigns are instructive here. When the germ theory of illness was gaining ground, it took enormous effort and labor to convince people to change their habits, like to wash their hands, to cover their mouths when they were sneezing. It took a few decades of public health campaigns both to convince people that there was something called bacteria that could make you sick, and that you had to change your behavior. So why wouldn’t we need something similar for computer security? But that’s obviously something that info security companies—rightfully so—are probably not going to invest in.

LFB: Yeah, there’s not a lot of money in that. But I think that we could demand more and expect more from companies that are only maybe tangentially in the infosec industry—like Google, Facebook, these big giants—that everyone yuses, more or less. So they can really make a big difference. If Google made two-step verification mandatory, or if they just made it an option to choose when you create your account, that could make a huge difference in the adoption of these measures.

GC: That’s an excellent point.

Let’s turn to another final question: Can you tell us a little bit about challenges you face writing on hackers and security?

LFB: One of the challenges is cutting through the noise. Infosec and cybersecurity have become so popular now that there’s so much noise. And it’s very easy to get lost in the daily noise. And as an online journalist, the risk is double because that’s kind of like my job: I have to be on everyday and see what happens everyday. Let me give you an example: yesterday there was some revelation about a vulnerability in the web versions of Telegram and WhatsApp. It made a lot of noise. It wasn’t that big of a deal in the sense that we don’t know many people are affected. Probably quite a few. But we don’t know how many people use the web versions of these apps.

Another challenge here is that so many people are trying to position themselves as experts in this field. As a journalist, it’s sometimes very hard to select your sources wisely

because there are a lot of people that want to say something. They want to have their opinion broadcasted, they just want to join the fray and talk about the latest infosec news.

GC: How do you go about resolving that noise? Are there some experts that you rely on more than others? Do you talk with colleagues?

LFB: Yes, I think it’s a combination of everything you said. Talking to colleagues helps. I work with a really great journalist, Joseph Cox, who you know as well. It helps sometimes to share.... We ask each other: who shall I talk to? That helps. It’s also just a matter of time. When I started out, it was really hard to tell [who to talk to]. You would go on Twitter or just...everyone seemed like an expert. It’s very easy to say “cybersecurity expert” or whatever, and make claims that sound more or less informed.

The PR and marketing machine behind the infosec world is also very strong. Every time there’s a breaking story, we get dozens of emails trying to sell random people saying stuff that is not even that interesting. But there’s a lot of money involved, and so marketing is very powerful in the present world. I think after a while you just become very cynical—in a good way. If you smell the marketing campaign, then you’re like, okay, I should probably ignore this because it’s just marketing.

GC: Right. Is there sometimes a situation where it is a marketing campaign, but it is also a really cool important technology that has the potential to change things, or already has?

LFB: Yeah, sometimes attention is warranted. I’m trying to think of an example. I mean, for example, [the cybersecurity company] Kaspersky has a really big marketing side, and they do push their research very strongly through their marketing and PR people. Most of the time, their research is actually very interesting, so it’s not necessarily—like if you use marketing, it’s not necessarily bad. There’s just too much of it now. The problem with marketing is mostly when the sources or companies try to make their research look too good or make unfounded claims. Obviously I understand that they’re trying to get attention. But I think that actually—they don’t realize it—that that sometimes can backfire.

GC: Right, that’s a good point. And you know, I’m always thinking of potential PhD topics for my students; it would be really interesting to study the domain of infosec company research and the processes of knowledge vetting. How is it similar or different to academic peer review? And as you say, there’s a lot of very respected researchers and the material coming out of there is often very strong and important. But from my understanding...they will limit what they release too. Right?

LFB: As a company, yeah.

GC: Right, because you don’t want people being able to take things from you. So there’s this fine line between researching, getting the data out there, but maybe not always being able to reveal everything.

LFB: And that’s why, for example, an average Citizen Lab report is more interesting than an average infosec

company X and Y report, because—and this is the point that Ron Deibert, the director of Citizen Lab, made when I spoke to him recently—you know, we don't have to hide anything. And they want to encourage other people to look at the data and look at it themselves.

Another big challenge is the anonymity and pseudonymity of sources. It's almost like a default...I don't have the numbers...but I think a big part of my sources and my colleague's sources are often anonymous or pseudonymous. They have a nickname, they have an alias. And the challenge sometimes is: Is this the same person I spoke to the other night? And the challenge there is not just verifying who they are, which is sometimes impossible, the challenge is sometimes keeping your head straight, and your sanity. Because the person sounds a little bit different. And "sounds" is probably the wrong word... because the tone is different...and you start thinking, is this a group? A friend of the guy or the lady that I spoke to the other day? But I think that when this happens, you have to focus on the content of the conversation, what they're talking about, what documents they might be providing. The story might be there, although...it's sometimes easy to forget, but what readers care the most about is people. So, the hacker, the hacktivist, is very often one of the most interesting parts of every story.

GC: Right, often there's a lot of mystique around them or hacker groups. And...I know this well from my research about how difficult it can be to always be dealing with pseudonymous people. I thought Jeremy Hammond was an agent provocateur by the way he acted. And I was completely wrong, you know. It can be very hard to suss out these things.

LFB: Definitely. I think that's one of the biggest challenges, for sure. But it's also interesting in a way. I don't fault them for trying to protect their identity. And that's just how it is. And that's not going to change anytime soon. Sometimes it is frustrating. Sometimes you wish you could have that certainty. In real life, you see a face, and that's the person. But in these cases, there's not really much to go on.

LORENZO FRANCESCHI - *Bicchierai* is a staff writer at Motherboard, where he covers hacking, information security, and digital rights.

Interview conducted March 2017.

ORGANIZATION CHART of THE TABULATING MACHINE CO.

BOARD OF DIRECTORS - C-T-R- CO.

Alfred DeBuys	Clarence P. King
George W. Fairchild	Stacy C. Richmond
Charles R. Flint	Joseph E. Rogers
A. Ward Ford	Christopher D. Smithers
Oscar L. Gubelman	Thomas J. Watson
Samuel M. Hastings	George I. Wilber
John W. Herbert	Rollin S. Woodruff
	Joel S. Coffin

COMPUTING-TABULATING-RECORDING CO.
Offices - 50 Broad St. - New York City

THE TABULATING MACHINE CO.

General Offices - 50 Broad St.
New York City

FACTORIES - WASHINGTON, D. C.
- ENDICOTT, N. Y.
- DAYTON, O.

THOMAS J. WATSON *President*
R. L. Houston *General Manager*

DIRECTORS

George M. Bond	James S. Ogsbury
George W. Fairchild	Gershom Smith
Thomas J. Watson	

MANUFACTURING
O. E. Braitmayer
Swift Boykin - Chief Clerk

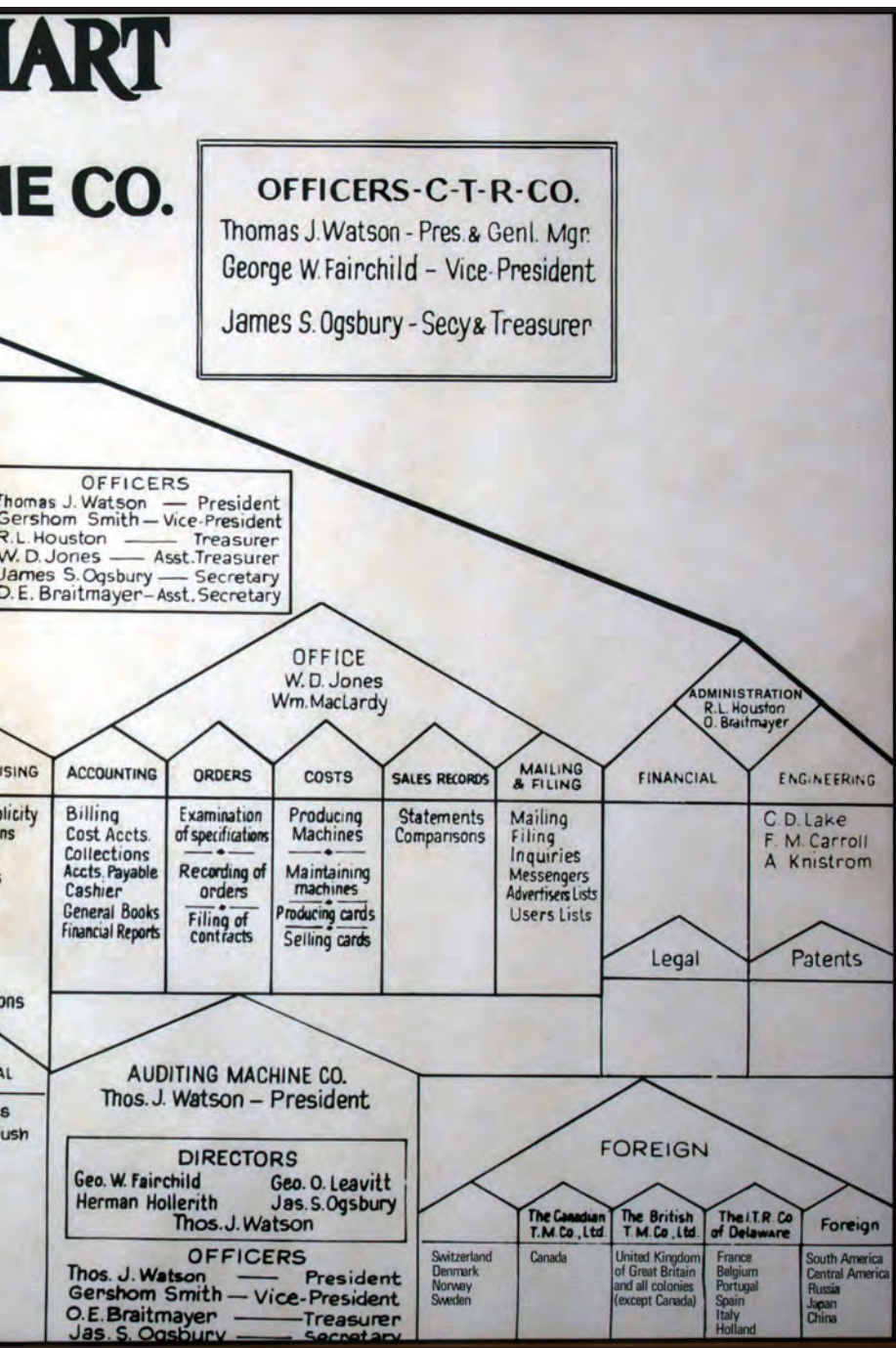
SYSTEMS
Gershom Smith
Pierre Bontecou

SALES
G. W. Spahr

Production Operating Machines	Production Cards	Maintenance Machines	Plant Maintenance	Purchasing	INVESTIGATION and RESEARCH	SCHOOLS	GENERAL EDUCATION	BOSTON DISTRICT	NEW YORK DISTRICT	PHILADELPHIA DISTRICT	CLEVELAND DISTRICT	ADVERTISING
J. J. O'Brien Elmer Oldroyd	J. E. Braitmayer	Taylor Garnett	J. E. Braitmayer	O. E. Braitmayer	Survey and study of industries not using machines at present. Study of present uses of machines. Distribution of information to field force.	Training of new men in classes		Boston Office Springfield Office Worcester Office Providence Office	J. L. Hyde New York Office Syracuse Office Buffalo Office Hartford Office Bridgeport Office Rochester Office	J. T. Wilson Philadelphia Office Scranton Office Altoona Office	P. D. Merrill Cleveland Office Detroit Office Cincinnati Office Pittsburg Office Pittsburgh Office	General Publications House Organ Booklets Pamphlets Circulars Catalogs Layouts Copy Cuts Illustrations
								CHICAGO DISTRICT	WASHINGTON DISTRICT	ST. LOUIS DISTRICT	SAN FRANCISCO DISTRICT	SPECIAL ADVERTISING
								C. L. Hayes Chicago Office Des Moines Office Indianapolis Office Milwaukee Office Minneapolis Office	M. W. Sheldon Washington Office Baltimore Office Atlanta Office	E. C. Richter St. Louis Office Houston Office Kansas City Office Dallas Office	C. W. Stoddard San Francisco Office Los Angeles Office Seattle Office	H. D. Coate C. I. Quackenbush

December, 1917

CAN YOU SECURE



LEFT: A 1917 exemplar of bureaucracy—the Tabulating Machines Company (later IBM).

Are bureaucracies defensible? **Nils Gilman**, **Jesse Goldhammer**, and **Steven Weber** explore the Office of Personnel Management hack, and what it tells us about the inherent vulnerabilities of bureaucratic organizations in a digital age.

AN IRON CAGE?



OVER THE COURSE OF 2014 AND 2015, The U.S. Office of Personnel Management (OPM) slowly discovered—and even more slowly disclosed—that it had been the victim of one of the biggest and most significant to national security hacks of personally identifiable information in U.S. history. Eventually OPM would admit that more than 21 million individuals’ records had been compromised, including the real identities and fingerprints of more than 5 million people both inside and outside the federal government: virtually everyone who at some point in the last 30 years had either sought or been required to obtain a security clearance.

OPM is a classic example of a bureaucracy, one of the defining inventions of the modern age: rational, rule based, and results oriented. When it works well, bureaucracy is a remarkable form of human organization that has enabled modern governments and corporations to provide previously unimaginable benefits to humans around the world. Before “scale” ever became a Silicon Valley slogan, it described a distinct post-18th-century organizational capacity to deliver goods and services to millions in a consistent, orderly, and equitable manner¹

But as we know from Max Weber, bureaucracy has a dark side: many “customers” and “citizens” experience bureaucracy as inexplicable confusion, frustration, and alienation. It was the bureaucratic insiders whom Weber saw as most painfully struggling with dehumanizing “systems,” processes, and rules. Weber worried about the impact of bureaucratic structure on individual freedom, an anxiety that gave rise to what is arguably his most famous metaphor: the “iron cage” (*stahlhartes Gehäuse*).

Weber’s metaphor paid homage to the dominant form of production at the time: industrial machines. Weber imagined bureaucracies as the organizational analog to an efficient machine: “The fully developed bureaucratic apparatus,” he observed in *Economy and Society*, “compares with other organizations exactly as does the machine with non-mechanical modes of production” (Weber 1978:973). But has modern bureaucracy finally met its match in the internet era? Put another way: In a networked digital age, does bureaucracy remain an efficient and effective apparatus for managing human affairs?

Important insights about this simultaneously theoretical and empirical question emerge from the now-infamous theft of data belonging to the federal government’s OPM in 2014 and 2015. The OPM breach turns out to be a powerful illustration of how a Weberian bureaucracy struggles and fails to meet one of the most profound challenges facing organizations that operate internet-connected digital networks in the 21st century: the hack. How OPM lost this battle foreshadows a deeply troubled future for bureaucracies in the increasingly digital decades to come.

THE OPM HACK: A SLOW REVEAL

Established in 1979 as part of the Civil Service Reform Act, OPM is essentially a human resources agency charged with overseeing the civil service of the U.S. federal government. In addition to “recruiting, retaining and honoring a world-class force to serve the American people,”² it is also responsible for the management of security clearances, not only for federal employees but also for the millions of contractors who serve in security-sensitive capacities.

Until 1996, OPM itself conducted background investigations for security clearances. That year, as part of then-Vice President Al Gore’s “Reinventing Government” initiative that aimed to shrink the size of the federal civil service, OPM outsourced its investigative branch to private sector consulting firms, many of which were run by former high-level OPM employees. Two of these companies, the United States Investigations Services (USIS) and KeyPoint Government Solutions, would come to dominate the federal market for investigation services, conducting millions of background investigations over the next two decades on behalf of their federal clients. With the exception of the Nuclear Regulatory Commission, which manages security related to the U.S. nuclear industry, the formerly separate security clearance programs of each executive department were gradually merged into a single, government-wide clearance system charged with investigating both federal workers and contractors seeking Secret and Top Secret clearances.

Had OPM and its investigative surrogates continued to operate with paper files—even millions of them—OPM’s outsourcing almost certainly would not have posed the same risk as the pooling of digital files. But this combination of centralization of systems and outsourcing of functions established a risk-filled playing field through which the OPM hack would unfold over the course of 2014 and 2015 (Castelluccio 2015:79).

The public dimension of the OPM hack officially began on June 17, 2014, when USIS sent a memo notifying 15 federal agencies that it had uncovered a data breach that had taken place three months earlier, in March, with “all the markings of state-sponsored attack.” The breach had resulted, USIS said, in the disclosure of about 25,000 federal employees’ records.

One can only imagine the difficult conversations that must have ensued among OPM leaders when they

¹ For two radically divergent recent histories of bureaucracy, see Fukuyama (2014) and Graeber (2015)

² <https://www.opm.gov/about-us/our-mission-role-history/>

received this letter. As it turned out, OPM had itself also been the subject of an direct cyber attack by Chinese hackers back in March, one OPM had informed the White House about but had never disclosed publicly, because at the time OPM managers believed it had successfully thwarted the attack using an Intrusion Detection System, a computer network-monitoring appliance designed to spot malicious activity or policy violations (Smith 2015).

OPM's official response to the June 2014 USIS letter was straight from the bureaucratic playbook: sever its contracts with USIS and admonish its employees to be more vigilant with respect to cybersecurity threats (*Washington Post* 2015). In fact, as yet unbeknownst to OPM, the attackers were already inside their systems, having succeeded in dropping a RAT (remote access trojan) on one of OPM's key Microsoft SQL servers. By June 23, 2014, the hackers had moved laterally through OPM's computer network and found their way into one of OPM's mainframe computers. A legacy system incapable of supporting modern encryption technologies, this mainframe was where OPM kept its hypersensitive data on background investigations.

By July, the FBI had launched a wide-ranging investigation. In September, this investigation detected a data breach affecting KeyPoint Government Solutions, the other major provider of investigations services for the U.S. government, primarily serving the Department of Homeland Security (DHS). This breach is believed to have compromised as many as 400,000 current and former DHS employees, contracts, and job applicants (Associated Press 2015). In December, yet another, separate breach was discovered at KeyPoint, leading OPM to notify more than 48,000 federal employees that their security credentials as well as other personally identifiable information had been compromised.

Though the U.S. government didn't realize it at the time, the aim of the hackers was not just to gain access to the data stored at USIS or KeyPoint, but even more to acquire virtual private network (VPN) credentials from these contractors that would enable the hackers to access data inside OPM itself. In April 2015, when OPM upgraded its internal security tools, it discovered that since the previous December it had been the victim of a months-long data breach.

Called to testify before Congress on the matter on April 22, 2015, OPM's Chief Information Officer Donna Seymour admitted not only that USIS and OPM had both been hacked near simultaneously back in March 2014, but also that the KeyPoint and OPM attacks were coincident in December 2014 (Sternstein 2015). It was now becoming clear that the contractors were serving as vectors for entering the U.S. government systems themselves.

It was only in June 2015, nearly a year after the original OPM breach, that the government began to realize (or admit) the breathtaking scope of the hack. The

breach, including massive amounts of data from OPM's e-QIP System, which a year earlier the *Washington Post* had described as "including applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers" (Nakashima and Rein 2014). In addition to this data, the hackers would also have acquired information from "adjudication," or the supplemental information that investigators would have considered before granting a security clearance, including:

...information on "sexual behavior" that "reflects lack of discretion or judgment" to evidence of "foreign influence," including a broad definition of "risk of foreign exploitation" associated with mere "contact with a foreign family member." For instance, the information collected to adjudicate a simple Top Secret single-scope background investigation includes a "Personal Subject Interview" and "interviews with neighbors, employers, educators, references and spouses/cohabitants." It also includes "record checks with local law enforcement where the individual lived, worked, or went to school in the past 10 years" (Adams 2016).

Finally, while it has been widely reported that the OPM hackers were able to obtain fingerprint data from 5.6 million individuals, it may also be the case that they obtained polygraph results from individuals who sought high-level security clearances, as this information would have been included in any typical adjudication process.

THE INHERENT CYBER VULNERABILITY OF WEBERIAN BUREAUCRACIES

The hackers who stole a treasure trove of data about U.S. citizens did not simply demonstrate the vulnerability of a particular government agency. Rather, they systematically exploited weaknesses that are endemic in bureaucracies and did so in a way that calls into question their *modus operandi*, which Max Weber articulated succinctly: the definition of bureaucratic administration is domination through knowledge and process (Weber 1978:225).

OPM's information networks mirrored the structure of the organization itself. When OPM outsourced functions like investigations to improve its efficiency, it necessarily created new network nodes, managed by private contractors, which increased complexity, vulnerability, and risk.

That changing network architecture configuration ultimately put OPM in a terrible bind. It was not enough just for OPM to build information technology (IT) systems that support its core mission, namely the management of human resource records; it would also need to develop a new and highly costly expertise that was far afield from the types of knowledge that OPM had managed since its inception. And, that

new knowledge—cybersecurity—would reside in and govern not only OPM itself, but also its symbiotically intertwined contractors. This put OPM in the position of requiring a wide range of technical standards, from authentication to encryption to threat mitigation, that OPM was itself unable to meet.

OPM's centralizing and outsourcing of its investigative services reflected what seemed at the time a rational choice for a federal human resources bureaucracy charged with the mandate to operate more cost-effectively. What Daniel Yergin once termed the Reagan bureaucratic "revolution" (Yergin and Stanislaw 1998) was in fact less of a revolution than an evolutionary move to redirect bureaucratic functions from the public to the private sector (Gualmini 2008). The goal of this move was to drive efficiency. Whereas public sector bureaucracies are typically governed by process norms (are they operating according to the appropriate laws, regulations, rules, and norms?), private sector bureaucracies in for-profit businesses are supposed to be governed more powerfully by efficiency objectives: How much does it cost to get the job done? The private incentives are to maximize productivity and minimize wasteful processes.

But private sector bureaucracies are still bureaucracies: hierarchical, rule-driven, complex, and when they operate at scale, anti-entrepreneurial. The ideology behind outsourcing was rooted not in a critique of bureaucracy per se, but in a belief in the disciplining force of the profit motive and a concomitant anti-statist disposition against *government* bureaucracies (Considine and Lewis 1999).

The efficiency argument turned out to have less weight than its proponents had hoped. This is because, as Paul Dimaggio and Walter Powell observed in their classic 1983 paper "The Iron Cage Revisited," organizations that interact intensely and largely exclusively start to converge in structure and processes so that their interactions can themselves become efficient. In other words, the larger and more intimately connected to the public sector a "private" bureaucracy is, the more it looks and operates like (becomes isomorphic with) the public sector agencies it serves. Because the contractors serving OPM had to interact intensively with government agencies, they inevitably began to mirror OPM's operational habits and organizational structures. Going private didn't offer an escape from the iron cage of bureaucratic inefficiency; it just shifted the bars on the windows (Dimaggio and Powell 1983).

This convergence might have been merely a disappointment to efficiency mavens. But 1996 was also the year that the World Wide Web came into widespread use, signaling a new era in organizations' dependence on digital networks. The U.S. government bureaucracy and its stable of contractors found itself unprepared for a set of threats that were unforeseen at the time: cyber

attacks from networked adversaries. The greater complexity of the outsourcing system may have increased its vulnerability to adversaries who were aware of that complexity and prepared to exploit it ruthlessly for criminal gain.

Bureaucracies have been historically successful when they are able to master knowledge complexity through the development of expertise, role differentiation, and process innovation. Contemporary information networks profoundly challenge this supremacy. The digital world operates with infinitely greater speed than the old paper-based models that bureaucracies were invented to manage. Digital networks encompass stores of information that far exceed the carrying capacity of a traditional bureaucracy. Digital machines execute actions on the basis of highly complex data analyses that exceed human cognitive abilities. The problem is simple: bureaucracies are designed to seek control through mastery of detail and predictable processes. Large-scale information networks have too many details—that is, they are too complex—to master in this way. Indeed, they are hackable precisely because specialization and division of labor do not actually facilitate the understanding, let alone management, of hardware and software vulnerabilities, especially given the fact that increasing technological sophistication also inadvertently multiplies complexity and vulnerability.

Bureaucracies have to operate according to codified rules and procedures. This can be effective for parrying *known* risks and threats, but can be worse than useless when defenders don't know the nature or source of the dangers in question. This dynamic is multiplied in the software environment. Frederick Brooks's classic study of software engineering is titled "The Mythical Man Month" (1975) for a reason: in the tar-pit that is software code, bureaucratic processes (like adding more workers to a project that has fallen behind schedule) often have perverse and literally counterproductive effects. "Brooks's Law" puts it this way: adding manpower to a late software project makes it even more late. Software engineers have developed alternative approaches to organizing that seek to compensate for Brooks's Law (such as Agile Programming), but such approaches to fostering innovation are at odds with bureaucratic demands for things like documentation and metrics of productivity and performance.³ Outsourcing work to private sector bureaucracies that serve the government bureaucracy changes nothing in this regard.

The offense-defense balance around bureaucracy is almost precisely reversed in the digital era from what it was during the industrial era. Now, bureaucracies are easier to attack than they are to defend, easier to undermine than they are to stabilize. And this calls the sustainability of the bureaucratic form into real

3 This point was recognized half a century ago in Thompson (1965).

question.⁴

We can bemoan the fact that OPM did not upgrade its information technologies and did not implement common-sense cybersecurity protocols, such as data encryption, in an effort to protect highly sensitive data about millions of Americans. But that lamentation rests on the assumption that bureaucracies can build and sustain information networks able to serve their core missions without dramatically increasing risks that can also be managed through a mastery of cybersecurity expertise.

We would have to believe that organizations like OPM can either administer their own robust cybersecurity protocols or outsource them to other parts of the government and/or the private sector without at the same time increasing the risk that such complexity will actually make OPM more vulnerable, not less. Indeed, even if OPM had done everything right—whatever that might mean—we would also still need to believe that a determined and sophisticated nation-state actor intent on stealing OPM’s data possibly could have been thwarted. In short, OPM was a sitting duck.

“A LINKEDIN FOR SPIES”

In July 2015, the news got even worse for Washington. United Airlines revealed that it too had been hacked, using the same exploits and techniques that had been used to penetrate USIS, Keypoint, and OPM. The data stolen from United consisted primarily of flight manifests, including information on flights’ passengers, origins, and destinations (Riley and Robertson 2015). And, as it turned out, the same signatures, according to various experts, marked the hack of the enormous American health care insurer Anthem, which had revealed in February 2015 that it had had 79 million records stolen from across its various brands, including Blue Cross and Blue Shield, Amerigroup, Caremore, and Unicare (Menn 2015).

The specter that this hacking triple-play raised for the U.S. government was a fundamental compromising of the U.S. intelligence community, perhaps for a generation. As *Ars Technica* put it, “When pulled together into an analytical database, the information could essentially become a LinkedIn for spies, providing a foreign intelligence organization with a way to find individuals with the right job titles, the right connections, and traits that might make them more susceptible to recruitment or compromise” (Gallagher 2015).

Ars Technica’s catchy “LinkedIn for spies” metaphor is just one installment among the dozens of imaginative and speculative thought pieces about how an adversary might take advantage of all of these data. Unfortunately, what we think we know about the consequences of the OPM, United, and Anthem hacks is belied by a stubborn reality. Did these hacks provide China with a geostrategic advantage?⁵ We don’t know.

Did they compromise our intelligence professionals? We don’t know. Did they harm anyone concretely or cause a human toll of any sort? So far, the answer appears to be a tentative “no,” but this might be an artifact of government secrecy. Did these hacks usher in radical transparency with visible consequences? Answer: probably not, or at least not yet.

The thing bureaucracies hate more than anything else is uncertainty. And yet the only certain impact of the OPM and associated hacks was to embarrass the U.S. government. Even former CIA Director Michael Hayden described the Chinese hacking of government records as “honorable espionage work” of a “legitimate intelligence target.” “This is a tremendously big deal,” he said. “My deepest emotion is embarrassment” (*American Interest* 2015).

In response to this embarrassment, OPM did what bureaucracies know how to do: it promised to adopt new policies, processes, and procedures. Despite its lack of native cybersecurity competence, OPM pledged to implement two-factor authentication, continuous diagnostics, and data encryption, though OPM noted, plaintively, that some of its systems are so old that they cannot be encrypted (Medici 2015). OPM also explained that it would hire a cybersecurity expert from “outside government” who would report directly to the OPM director. Finally, OPM asked Congress for additional resources to modernize its IT systems and ensure appropriate oversight of its agency and contractors.

POST-WEBERIAN POSSIBILITIES

It wasn’t so long ago that OPM managed investigations using paper, making it all but impossible to steal 21 million records. Now OPM and bureaucratic organizations like it are actively digitizing their core missions in the name of efficiency, and in so doing piling risks and vulnerabilities on top of each other as they venture beyond what humans and human processes are able to manage. While perfectly rational and appropriate in the Weberian model, these remedies are ineffective for addressing the fundamental weakness of traditional bureaucratic organizations that use modern information networks to prosecute their missions. In their current forms, such organizations simply cannot master the knowledge that is stored, transported, and analyzed on their networks. Instead, they will engage in flailing, piecemeal technical reforms to mitigate known risks, such as closing the ports from which their data have usually already escaped.

Worse, by extending the logic of Weberian bureaucracy, organizations like OPM are creating new classes of risks that they are also ill equipped to manage. For instance, they will embrace algorithmic policy decisions and enforcement, a digitization of their core functions, which may increase the efficiency with which they operate, but will also bury them in millions of lines of code

4 The idea that the cyber domain is an “offense dominant” one (in Robert Jervis’s terminology) is explored in Sergei A. Medvedev (2015).

5 China is widely believed to be the nation-state behind these hacks, even if no conclusive evidence has been proffered publicly.

and exacerbate the impact of mistakes. In response to current threats, IT and cybersecurity functions will expand into every corner of these organizations, but the irony is that this expansion will merely create a wealth of new opportunities for hackers. Finally, to meet oversight requirements, these bureaucracies will come under increasing pressure to develop highly sophisticated compliance software that tracks every bit of data: where it's stored, who accessed it and when, why they accessed it, how it was combined with other types of data and, finally, when and how it was deleted. These highly complex compliance systems will provide a panoramic view into complex information networks, but they too will be vulnerable and hackable.

As we watch the struggles of the U.S. federal bureaucracy to adapt in the face of these novel threats, we

are left with a fundamental question about the future of an organizational form. Is the digital revolution also the death throes of the traditional bureaucracy, presaging a future of declining governmental effectiveness punctuated by occasional catastrophe? What seems certain is that government bureaucracies face a radical reset of stakeholder performance and risk expectations, that is, with the citizens they are supposed to serve. ■

NILS GILMAN *Nils Gilman is an historian and the Vice President of Programs at the Berggruen Institute.* **JESSE GOLDHAMMER** *is a political scientist and the Associate Dean at the UC Berkeley School of Information.* **STEVEN WEBER** *is Professor at the School of Information and Department of Political Science, UC Berkeley.*



BIBLIOGRAPHY

- Adams, Michael. 2016. "Why the OPM Hack Is Far Worse Than You Imagine." *Lawfare*, March 11. Available at link.
- American Interest. 2015. "Former CIA Head: OPM Hack was 'Honorable Espionage Work.'" *The American Interest*, June 16. Available at link
- Associated Press. 2015. "Hack May Have Exposed Info on 390,000 People Tied to Homeland Security." June 15. Available at link.
- Brooks, Frederick P. 1975. *The Mythical Man Month: Essays on Software Engineering*. Boston, MA: Addison Wesley Professional.
- Castelluccio, Michael. 2015. "The Biggest Government Hack Yet." *Strategic Finance* 97(2):79.
- Considine, Mark, and Jenny M. Lewis. 1999. "Governance at Ground Level: The Frontline Bureaucrat in the Age of Markets and Networks." *Public Administration Review* 59(6):467-480.
- Dimaggio, Paul J., and Walter W. Powell. 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American Sociological Review* 48(2):147-160.
- Fukuyama, Francis. 2014. *Political Order and Political Decay: From the Industrial Revolution to the Globalization of Democracy*. New York: Macmillan.
- Gallagher, Sean. 2015. "'EPIC' fail—how OPM hackers tapped the mother lode of espionage data." *Ars Technica*, June 21. Available at link.
- Graeber, David. 2015. *The Utopia of Rules: On Technology, Stupidity, and the Secret Joys of Bureaucracy*. New York: Melville House.
- Gualmini, Elisabetta. 2008. "Restructuring Weberian Bureaucracy: Comparing Managerial Reforms in Europe and the United States." *Public Administration* 86(1):75-94.
- Medici, Andy. 2015. "OPM fires back at hack criticism, vows further reform." *Federal Times*, June 24. Available at link.
- Medvedev, Sergei A. 2015. *Offense-defense theory analysis of Russian cyber capability* [dissertation]. Naval Postgraduate School. Monterey, CA.
- Menn, Joseph. 2015. "U.S. employee data breach tied to Chinese intelligence." *Reuters*, June 19. Available at link.
- Nakashima, Ellen, and Lisa Rein. 2014. "Chinese Hackers Go after U.S. Workers' Personal Data." *The Washington Post*, July 10. Available at link.
- Riley, Michael, and Jordan Robertson. 2015. "China-Tied Hackers That Hit U.S. Said to Breach United Airlines." *Bloomberg.com*, July 29. Available at link.
- Smith, Ian. 2015. "OPM Data Breach: What You Need to Know." June 8. Available at link.
- Sternstein, Aliya. 2015. "Here's What OPM Told Congress the Last Time Hackers Breached Its Networks." *NextGov.com*, June 15. Available at link.
- Thompson, V. A. 1965. "Bureaucracy and Innovation." *Administrative Science Quarterly* 10:1-20.
- Washington Post*. 2014. "E-mail to OPM staff on security breach." July 10. Available at link.
- Weber, Max. 1978. *Economy and Society*. Berkeley: University of California Press.
- Yergin, Daniel, and Joseph Stanislaw. 1998. "The Real Revolution." *Forbes*, May 4, 85-91.

power down



OMG! Hackers take down energy grid!
David Murakami Wood and **Michael Carter**
calmly explain the how and why (or why
not) of infrastructure hacking today.

INTRODUCTION

The video game franchise, *Watch_Dogs* (Ubisoft 2014), offers a vision of infrastructure hacking as a smooth and seamless tool of hooded urban outsiders who, at the push of a button, can take out the traffic lights, hijack the closed-circuit television (CCTV) networks, or close down the power plants of major cities. Traffic and streets lights have not only become iconic in games, but also feature regularly in security threat scenarios for “smart city” projects. In early 2017, just days before the inauguration of President Trump, Washington, DC’s downtown surveillance camera network was hacked and infected with ransomware that, city officials admitted two weeks later, prevented the city from digitally recording images from 80% of the cameras for three days (Williams 2017). The system was only brought back online two days before the inauguration.

That hackers can gain control of the systems that regulate physical infrastructures shows why government officials have pointed to hacking of control systems as an ever-growing and more ubiquitous threat. As technological infrastructures themselves have become something more expansive and pervasive, and as human societies and humans as individuals are being asked to depend more habitually on digitally connected systems, this threat has also acquired more serious consequences. The unauthorized destruction of or control over Supervisory Control And Data Acquisition (SCADA) systems, systems that manage other machines from factory robots to the aforementioned traffic light and surveillance camera networks, has become a particular concern, as the “move to open standards such as Ethernet, Transmission Control Protocol/Internet Protocol and Web technology is allowing hackers to take advantage of the control industry’s unawareness” (Turk 2005: 5).

HISTORIES OF INFRASTRUCTURE HACKING

The standard history of SCADA hacking, and “infrastructure hacking” more broadly, is murky and mythologized. Interest is often dated back to the supposed Urengoy-Surgut-Chelyabinsk pipeline incident in the 1980s in which an 8-bit computer control system allegedly was infected remotely, triggering an explosion in a Soviet oil pipeline in Siberia. Yet as Thomas Rid (2013) and others have shown, there is no convincing evidence that this explosion ever happened, let alone that it was due to a hack. Indeed, Rid insists it was virtually impossible to “hide” any kind of Trojan on such a primitive control system.

In fact, it remains difficult to find any actually confirmed incidents of significant infrastructure hacking. The Ukraine grid attacks of late 2015 were widely presented as “the first publicly acknowledged incidents to result in power outages” (Lee et al. 2016: 6), but

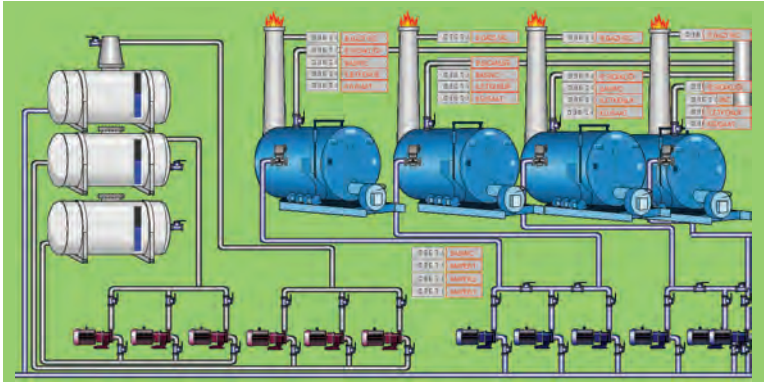


ABOVE: Hacking a pro-life lobbyist, tobacco exec in *Watchdogs*, 2014, Ubisoft.

is also mired in the propaganda war between Russia and Ukraine and its western allies. Much of the more immediate concern dates back to the 2003 electrical blackout across the northeastern United States and eastern Canada. However, this was not itself the result of a hack, but a combination of factors including old and buggy software, long-term policy and management failures, and a slow and inadequate response to the challenges of many simultaneous incidents of power lines being brought down by trees in a severe storm (U.S./Canada Power Outage Task Force 2004). It served to draw attention to the vulnerability of aging American electrical infrastructure and the relative complacency of power companies and governments in the face of multiple risks. The policy climate was already changing: “critical infrastructure protection” and “resilience” had become key concepts beyond simply emergency preparedness (Coaffee et al. 2009), and 9/11 not only accelerated those trends but reaffirmed and strengthened the place of security in the heart of state activity. This also hybridized with a longstanding obsession with “the enemy within,” which has always formed one of the bases for policing, and which has surged visibly at particular historical junctures. The most recent surges took place first at the end of the Cold War as intelligence agencies sought to retain and even expand budgets in the face of a declining overt threat and looked to political activists as a new group of threats, and then again after 9/11, an event that persuaded politicians that certain groups of citizens might be potential saboteurs.

Gabriella Coleman (2014) shows that this continues to be a major concern in her book on *Anonymous*, in which she recounts being quizzed by CSIS (the Canadian equivalent of the CIA) on whether the hacking collective could take down the electricity grid, despite the fact that they had given no indication of interest in doing such a thing. In other words, the argument was, if this can happen by accident, how much worse could it be if a determined effort was made to

¹ Security experts have questioned the conditions of the experiment in many ways, and raised doubts as to whether it demonstrated anything that would be practically possible.



ABOVE: One of many SCADA control system diagrams; this one for controlling boilers.

deliberately disrupt electrical grids by internal or external adversaries?

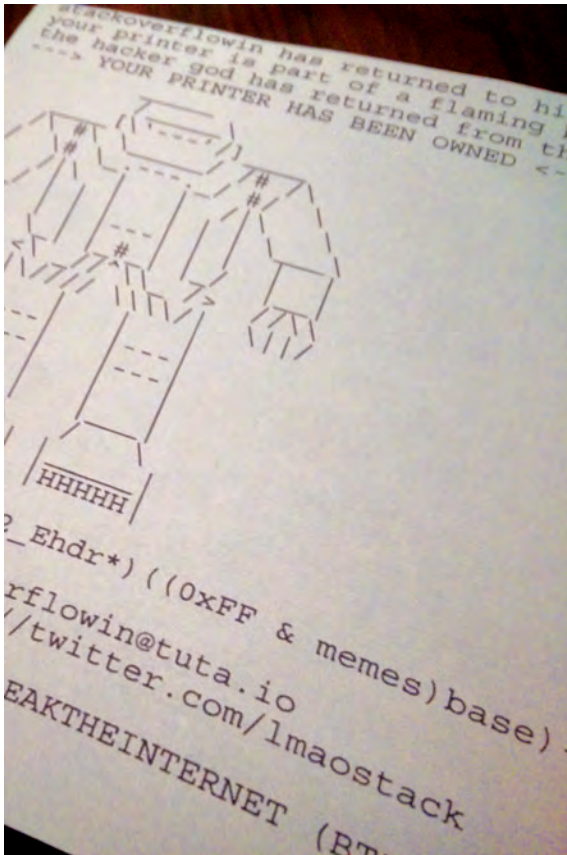
The pressure was therefore increased to develop “self-healing grids” (Amin 2004) based on the model of the original ARPAnet that became the Internet, intended as a military computer communications system that would be distributed and contain multiple redundancies to route around damage to any part. The U.S. government established a “Smart Grid Committee” in 2007 to facilitate movement toward such smart grids. But “smartness” itself was leading to new fears of vulnerabilities, as was shown by the Aurora grid hacking demonstration in that same year. This experiment, conducted in Idaho, demonstrated that in the experimental set-up, at least, a targeted systems intrusion could cause mechanical generators to operate slightly out of synchronization with the rest of the grid, creating a malfunction leading to explosion and fire.¹

The concern with infrastructural vulnerability has also grown because the very organizations tasked to prevent such attacks by western nation-states, largely intelligence agencies, know of the real possibilities of SCADA system hacking largely through their own use of such tactics against other states. The intelligence services’ concerns about Anonymous, for example, are derived not just from Aurora but also from their own use of worms as a form of cyberattack, in particular Stuxnet, which marked a new phase in state involvement in hacking occupying a blurred space between espionage “black ops”, and overt warfare (Zetter 2015). Stuxnet is almost certainly a weapon devised through U.S.-Israeli cooperation specifically to attack Microsoft Windows-based Siemens SCADA systems. In the original release, the worm was aimed at the control systems for centrifuges in Iranian factories suspected of producing nuclear materials; however, it did so with unprecedented precision and complexity, exploiting not just one or two vulnerabilities, but four “zero-day” (previously unidentified) vulnerabilities in different points in the system.

Because Iran knew hacking attacks were targeting such secret nuclear work, Iranian managers made sure that the control systems themselves were not on-line or connected to any outside network, a practice known as “air-gapping.” The Stuxnet program was therefore much more than just conventional hacking; it also involved old-fashioned subversion and the recruitment or insertion of human intelligence assets, or moles, inside the factory who could transport and insert the worm into the SCADA systems with a USB stick. Stuxnet was by all accounts “successful,” and yet this highly dangerous weapon has also been discovered in numerous networked systems in countries as far afield as India and Indonesia (Falliere et al. 2011), so it must have been used on more than just those air-gapped factory machines. Stuxnet was programmed to self-destruct after around two years, but this was not, as one industry speaker at the Computers, Privacy and Data Protection 2017 conference asserted, an example of “ethics” in cybersecurity. Rather, it was a form of prevention to keep the worm from turning and becoming a danger to factory SCADA systems in “friendly” countries, and also to prevent it from being repurposed by unfriendly ones.

Stuxnet took years to plan, millions of dollars in development, and careful cultivation of human plants inside targeted organizations who had to breach “air gaps” and carefully separated systems. This seems a long way from Anonymous’s “for the lulz” mode of ad-hoc and freewheeling political activism. However, both the fact of the leakage of Stuxnet “into the wild” and the increase in connected “things” of all kinds provides the rationale for the concern over the possibility of Anons taking down the electrical grid. The new wave of infrastructure hacking relies less on discovering and taking down the single “control” behind a particular system, and more on exploiting generalized connection of systems and objects, most obviously in the Internet of Things (IoT). Driven by the search for new profits within a saturated, globalized economy, entrepreneurial technological capitalism has discovered these potential profits in the surplus value of intimate and previously inaccessible intimate data generated by bodies and in the home, and the marketing of mass-customized services built on such data. The profit imperative demands that these sources of data must be connected, and connected quickly with minimal interest in the security of devices, networks, and people.

While the vulnerability of IoT devices is now well known, it is not just cheap consumer equipment that lacks sensible protocols or whose existing security capabilities remain undeployed by—or inaccessible to—their users. In one 2009 incident very important in thinking about such IoT-enabled hacking, Shi’ite



LEFT: Hacker “stackoverflowin” owned 150,000 thermal printers in February 2017.

make and sell. Whereas people would like technology to work (and that includes being secure), the tech world seems to believe that users should do the work themselves to make technology secure. This has resulted in several new threats both in practice and experiment. In the first category, alarm has increased about the hijacking of insecure IoT devices from toasters to smart home alarm systems and their integration into remotely controlled botnets used in distributed denial of service (DDoS) attacks. The attempted takedown of the Krebs on Security site created what was then the largest ever such botnet (Krebs 2016a) by the so-called “Mirai” malware, which looked for IoT devices still using insecure factory defaults (Krebs 2016b). In 2017, a similar hack took place that mobilized 150,000 printers, this time specifically to demonstrate the threat posed by unsecure connected devices (Moyer 2017). In this case, the printers were made to print out ASCII pictures of robots and were not actually part of a botnet, but the point was made: they could so easily have been.

In the second category are attacks that allow hackers to take over networked control systems. Many of these are ransomware attacks, in which relatively easy ways into systems are used to lock their legitimate users out of them. The users are then asked to pay to have their access restored, usually in bitcoin or some other hard-to-trace blockchain-based electronic currency. Security researcher Cesar Cerrudo found in 2014 that many smart urban traffic control systems had vulnerabilities, and that these would “allow anyone to take complete control of the devices and send fake data to traffic control systems. Basically, anyone could cause a traffic mess by launching an attack with a simple exploit programmed on cheap hardware” (Cerrudo 2014). Cerrudo’s findings are also relevant to the kinds of political decisions that might be made in response to such threats. He argues, “if a vulnerable device is compromised, it’s really, really difficult and really, really costly to detect it” (Cerrudo 2014). This means that there could “already be compromised devices out there that no one knows about or could know about” (Cerrudo 2014). A serious implication here is whether the pressure to find cheap, “smart” urban fixes in an age of austerity will actually make hacking attacks more prevalent, even normal, and this might put urban authorities lacking both financial and technical security resources at a permanent disadvantage, having to choose between smart and secure rather than having both.

REGAINING CONTROL?

Several of these examples make *Watch_Dogs* seem less simplistic in its portrayal of the ease of infrastructure hacking. Cerrudo’s insights are meant to provoke or force national governments to get more involved in assessing technologies. There is a more general issue here than simply hacking: in many jurisdictions, there is often barely any scrutiny of procurement by local government and other subnational agencies and

insurgent forces in Iraq hacked U.S. military surveillance drones, allowing them to watch the watchers, track what the U.S. surveillance military system was seeing, and adjust their positions and movements accordingly (Shachtman 2009). This was as far from the operational scale or investment involved in Stuxnet as one could imagine. Deploying a tactic not far removed from urban WiFi sniffing, the insurgents used a \$26 off-the-shelf Russian Skygrabber software more commonly used to download satellite television programs. There are crucial differences between this attack and Stuxnet. The Skygrabber hack is a cheap, flexible attack that exploits both the technological sophistication and the distribution and generalized nature of the system being hacked, whereas the Stuxnet attack was a major state-backed investment that engineered vulnerability in a highly secure system probably less technologically sophisticated than the attack itself. The key point here is that despite the turn to resilience and security, “infrastructure,” whether military or civil, is increasingly generalized, connected, and distributed, and less likely to be air gapped and secured in the manner of Iranian nuclear component factories.

This new shifting, flexible, and contingent form of operation can be seen in the exploitation of the fact that manufacturers and suppliers appear broadly unconcerned with the vulnerability of the systems they

authorities for any reason, let alone a detailed technical or security assessment. This is compounded by the fact that states and large corporations have ported their response to hacking infrastructure directly from the predominant official vision of hacking as cybercrime or, increasingly, cyberwar, concentrating on attacks on “critical infrastructure” and nationally significant computing systems rather than considering the security of people, groups, and smaller, local governments as priorities or even as a matter for government at all.

The focus on this top-level aspect, the view from a rather traditional, “realist” national threat model, makes cybersecurity sound exceptional. But there is nothing truly exceptional about cybersecurity that makes it an extraordinary threat. Infrastructure hacking attacks are technical in their means, but their solutions are frequently human and behavioral. The first biggest threat to security of control systems are degradation, failure, and accident; second, human users; and finally—and least likely and damaging of all—intrusion or “attack.” And many attacks are really exploiting human beings as much as the technical systems themselves; this is true even in the case of sophisticated worms such as Stuxnet, and all SCADA systems that are air gapped for security.

The question of air gapping should tell us something else: that the simplest form of security for infrastructure systems is disconnection. This is an important point to bear in mind when there is a mania for connecting everything, not just what one would formerly called computers or information systems, via the Internet of Things. Connection always means more openness and vulnerability, and every security action taken after connection is inevitably a (more expensive) mitigation of risk that also involves more intensive surveillance and compromises to privacy and other freedoms. We shouldn’t forget that if it serves no necessary purpose to connect, it shouldn’t be done. This lesson, however, goes against the powerful commercial imperatives that are driving the move towards the IoT, not only in terms of the sales of devices but the indirect exploitation of human users for yet more data, the direct sources having already been exhausted.

In the case of users, and that includes even relatively “expert” users such as police or security personnel, it is also ineffective and even counterproductive to blame individuals and demand that people conform to the systems or norms of highly expert producers within the developer community, especially because the commercial drivers assume and encourage such weakened privacy and security. Control also has an analogical meaning here in terms of measures, whether voluntarily by producers or mandated by stronger consumer protection laws that enable people and institutions that use connected devices to more easily control the security functions of devices and systems and understand the consequences. Again, this goes against certain technological trajectories, most notably the “infrastructureurization” of certain systems, or the vanishing of such systems from the sight of users who depend upon

them (Murakami Wood 2015). Although infrastructure is precisely designed to work unobtrusively and support other activities, and SCADA systems are the most invisible of all, this very invisibility can lead to inaccessibility to productive and useful alteration, as is already the case with many open source software design or mapping projects (Dodge and Kitchin 2013), but going further with crowdsourcing design or maintenance of civil infrastructure to provide greater real-world resilience and ownership, for example in helping to provide clean water in marginalized communities (von Heland et al. 2015). Far from all infrastructure hacking is offensive and destructive: as the growth of smart city hackathons, participatory programming, and the use of open data and open source is showing, many urban infrastructures can be more open and adjustable yet still be secure.

It might well be that although allowing generalized access to the “guts” of systems might not in practice provide for outcomes that are in the general good, providing greater access to the outputs might allow for both new uses and useful feedback. As in the case of the Iraqi insurgent hacking of U.S. drones, it is clear that this undermines military advantage; there is no such rationale in the case of urban CCTV. There is no fundamental reason why all citizens should not have access to public video surveillance feeds rather than their being purely an instrument of state authority. And what both cases share is that “control” over the system itself does not have to be compromised to allow the products of a technical system to be more widely available.

Although the security of control systems that allow infrastructures to function need defensive measures, perhaps a greater emphasis on designing the wider systems to be open to hacking would be both more cost-effective and more democratic, and lead to less paranoia and unnecessary closure. However, there are some very important cautions to overenthusiasm about participatory hacking. As Keller Easterling (2014) has argued, infrastructures are instruments of what she calls “extrastatecraft,” and in an age in which we are offered the false choice of neoliberalism and fascism, these can serve ends both exploitative and authoritarian. Despite the ongoing work of open source movements and the rise of Anonymous and the Pirate Party and other hackers with ethico-political motivations, both infrastructures and the tools of infiltration and control of those infrastructures remain predominantly in the hands of massively resourced state cybersecurity and cyberwar agencies or in the corporate campuses of Silicon Valley. There is no coherent current or foreseeable politics of hacking able to articulate a widely shared vision that is independent of either state or private sector. ■

DAVID MURAKAMI WOOD is Canada Research Chair (Tier II) in Surveillance Studies at Queen’s University, Ontario. **MICHAEL CARTER** is a doctoral research student in the Department of Geography, also at Queen’s University.

REFERENCES

- Amin, Massoud. 2004. "Balancing Market Priorities with Security Issues." *IEEE Power and Energy Magazine* 2(4):30–38.
- Cerrudo, Cesar. 2014. "Hacking US (and UK, Australia, France, etc.) Traffic Control Systems." *Ioactive*, April 30. <https://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html>
- Coaffee, Jon, David Murakami Wood, and Peter Rogers. 2009. *The Everyday Resilience of the City*. Basingstoke, UK: PalgraveMacmillan.
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso.
- Dodge, Martin, and Rob Kitchin. 2013. "Crowdsourced Cartography: Mapping Experience and Knowledge." *Environment and Planning A* 45(1):19–36.
- Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. New York: Verso.
- Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. W32.Stuxnet Dossier Version 1.4 (February). Cupertino CA: Symantec Corporation.
- Krebs, Brian. 2016a. "KrebsOnSecurity Hit With Record DDoS." *KrebsOnSecurity*, September 16. <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>
- . 2016b. "Source Code for IoT Botnet 'Mirai' Released." *KrebsOnSecurity*, October 16. <https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/>
- Lee, Robert M., Michael J. Assante, and Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, DC: SANS Industrial Control Systems/NERC.
- Moyer, Christopher. 2017. "This Teen Hacked 150,000 Printers to Show How the Internet of Things Is Shit." *Vice Motherboard*, February 8. https://motherboard.vice.com/en_us/article/this-teen-hacked-150000-printers-to-show-how-the-internet-of-things-is-shit
- Murakami Wood, David. 2011. "Vanishing Surveillance: Why Seeing What Is Watching Us Matters." Insights on Privacy discussion paper. Ottawa, Canada: Office of the Privacy Commissioner (OPC). https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/wood_201107/
- Rid, Thomas. 2013. *Cyberwar Will Not Take Place*. Oxford, UK: Oxford University Press.
- Shachtman, Noah. 2009. "Insurgents Intercept Drone Video in King-Size Security Breach." *Wired*, December 17. <https://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/>
- Turk, Robert J. 2005. *Cyber Incidents Involving Control Systems*. Idaho Falls: Idaho National Engineering and Environmental Laboratory.
- U.S./Canada Power System Outage Task Force. 2004. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Washington DC: Office of Electricity Delivery & Energy Reliability.
- von Heland, P. F., M. Nyberg, A. Bondesson, and P. Westerberg. 2015 "The Citizen Field Engineer: Crowdsourced Maintenance of Connected Water Infrastructure." Paper presented at the *Third International Conference on ICT for Sustainability (ICT4S 2015)*, Atlantis Press.
- Williams, Clarence. 2017. "Hackers Hit D.C. Police Closed-Circuit Camera Network, City Officials Disclose." *Washington Post*, January 26. https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html
- Zetter, Kim. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Broadway Books.



When GhostSec goes hunting

GhostSec engaged in vigilante counter-terrorism against ISIS.

Robert Tynes explores whether this makes them part of the state, part of civil society, or part of empire.

Hackers create the possibility of new things entering the world. Not always great things, or even good things, but new things.

McKenzie Wark, *A Hacker Manifesto*, 2004:4

WHAT WAS GHOSTSEC?

On Wednesday, January 7, 2015, two masked brothers carrying assault rifles burst into the offices of the Parisian satirical newspaper *Charlie Hebdo* and killed 12 people. Many others were injured. The brothers, who were members of al-Qaeda, fled the offices, fleeing across Paris for the next several days. During that time a police-woman was shot and killed in what seemed to be an unrelated incident in another part of the city. However, there was a connection: an associate of the brothers conducting the attacks was responsible for killing the police officer and taking hostages at a kosher supermarket. The associate had pledged his allegiance to the Islamic State of Iraq in the Levant (ISIL). Eventually police killed all three of the attackers (BBC 2015).

There were numerous public demonstrations and denouncements against the attacks across the globe. “Je suis Charlie” became a unifying slogan, expressing global civil society’s solidarity against terrorist organizations. Online, Anonymous created a campaign, “Operation Charlie Hebdo” or #OpCharlieHebdo, to take down terrorist organizations related to the attack:

We will track you everywhere on the planet, nowhere will you be safe. We are Anonymous. We are legion. We do not forget. We do not forgive. Be afraid of us, Islamic State and Al Qaeda—you will get our vengeance (International Business Times 2015).

Anonymous members declared war on politically violent Islamic extremists. Some Anons said it was their democratic duty to engage in the international political battle against groups. “[We will] track down all jihadist activities online and bring down Twitter and Facebook accounts of jihadists as well as close down any of their YouTube channels,” they said (*International Business Times* 2015).



FIGURE 1.
GhostSec Security
Logo.

The Anonymous declaration spawned multiple efforts to eradicate the online presence of terrorists. GhostSec was one such group that began targeting the Islamic State (ISIS) shortly after the call to cyber arms.¹ GhostSec’s main focus was ISIS, but it also went after other organizations such as Boko Haram, Al Shabaab, and Hamas. GhostSec members were both “horrified by ISIS’s atrocities” and concerned by the inability of governments to counter ISIS online:

The FBI has repeatedly admitted that. So, we got involved in #OpISIS in order to significantly slow ISIS down—recruitment and propaganda. We also wanted to be able to thwart attacks by collecting intel and turning that over to law enforcement (personal communication with GhostSec member Ransacker; March 2016).

In January 2015, GhostSec became an online citizen’s response to international political violence, working independently of the state but also willing to contribute to its goals. The core members of GhostSec were AnonCyberGost, WauchulaGhost, DigitaShadow, Comedianon, TorReaper, ISHunter, and GhostSecPI. The focus was to take down “daesh” in all its online manifestations.

GhostSec included women and men in its ranks, many ex-members of the U.S. military, and information technology (IT) and media professionals. There was a loose division of labor, with some members working the intelligence-gathering angle while other ghosts concentrated on the technical side of ISIS “hunting.” One ghost handled media requests and published a GhostSec Update website (<https://medium.com/@GhostSec>). The GhostSec project was coordinated through encrypted messaging applications, encrypted email, and, more publicly, on Twitter.

At first GhostSec was a “classic” instance of an Anonymous formation: they were indeed anonymous,

Anonymous members declared war on politically violent Islamic extremists.

¹ Note that GhostSec was one of many efforts to take down ISIS on the internet. There were hundreds of independent Anonymous hunters with aliases such as IS Hunting Club, TouchMyTweets, and The Doctor (Gladstone 2015). Other group-like Anonymous efforts include BinarySec and CtrlSec. Sometimes these groups worked separately, but in other instances there was overlap in members and efforts.



FIGURE 2. WachulaGhost defaces an ISIS Twitter Account in the name of Gay Pride.

and their information about ISIS was available to all. The ghosts were a mystery, but the point was to make ISIS as transparent as possible so that the extremist group's online presence could be frustrated and erased. And the efforts of GhostSec were valuable to everyone including the U.S. government. In the beginning, GhostSec never worked directly with the U.S. government, but some of its core members built a bridge to U.S. officials.

A few GhostSec members communicated with terrorist analyst Michael Smith II of the defense consulting firm Kronos Advisory. Smith, a prominent consultant to Congress about ISIS, became a liaison between GhostSec activities and the government (Segall 2015). This relationship with Smith became emblematic of differences within GhostSec. Some members wanted to retain their autonomy and anonymity, while three members—DigitaShadow, ISHunter and GhostSecPI—opted to work more directly for the American state cause. The three left GhostSec in November 2015, shed their Anonymous affiliation, and founded the Ghost Security Group (GSG) (<https://ghostsecuritygroup.com/>). The remaining GhostSec members remained Anonymous. The split, says GhostSec, was not about sharing or not sharing information with U.S. authorities; rather, it was more about having a formal arrangement with the federal government. There was also disagreement about getting paid to hunt down ISIS. Those who remained felt that going after ISIS was more of a cause than a job. “We do this for free,” said one GhostSec hunter. Or, as TorReaper put it: “The intel... became a commodity that had to be protected and so stopped getting shared with the group’s followers” (Raincoaster 2015). After the split, GhostSec continued on, remaining within the Anonymous fold. Meanwhile, the market consumed GSG via the state.

GhostSec’s initial focus was on websites. The first step was to report the website to the host. If nothing was done, then GhostSec moved on and attacked “... first by attempting to breach the site, then by ddos

[distributed denial of service] as a last resort. Breach attacks will include SQL injection, XSS attacks and brute force attacks” (Raincoaster 2015). Eventually ISIS’s flow of social media activity became so huge in 2016 that GhostSec shifted away from bringing down websites and moved toward looking for direct “...threats, propaganda, etc. Any actionable intel...” that could then be sent to U.S. law enforcement agencies (Rajan 2016). To do this, GhostSec focused almost exclusively on Twitter accounts. The hacking group claimed to have removed more than 50,000 Twitter accounts by 2015 (Stone 2015). GhostSec worked with any individuals or groups who wanted to contribute by calling out suspected Twitter accounts and/or websites.² The process involved a swarm of participants whose findings were processed by GhostSec members. Suspicious accounts were then reported to Twitter through its website (<https://support.twitter.com/forms/abusiveuser>.)

For GhostSec, the fight against Twitter remained online. The battle was waged in cyberspace, but there were also offline results: a decrease in ISIS’s ability to spread its propaganda and garner more recruits. It wasn’t entirely one-sided. ISIS sympathizers did retaliate against GhostSec members, mainly via verbal cyber rantings. Nevertheless, GhostSec was not significantly counter-hacked.

In late summer of 2016, GhostSec’s success caused another shift in the group, pulling them into a merger with BlackOps Cyber, a private group affiliated with the international corporation BlackOps Partners (<http://www.blackops cyber.com/home.html>). With the merger, GhostSec dropped its Anonymous mask/affiliation to become part of a CyberHUMINT counter-terrorism team. The transformation meant deeper connections to international policing: Interpol, MI5, and others. Hardt and Negri (2004) might say the move solidified them as a part of Empire, “enlisted in the global armies at the service of capital, subjugated in the global strategies of servile inclusion and violent marginalization” (2014:159).

Meanwhile, WauchulaGhost kept his Anonymous stance to fight alone as #GhostofNoNation. GhostSec was done, but hacking free of feds and capitalism continued. In the spirit of a Multitude stance (Hardt and Negri 2004), WauchulaGhost proclaimed to me, he fights for others: “Everything I do is for the People... this is a free service.” Some of WauchulaGhost’s accomplishments included defacing ISIS followers’ Twitter accounts and websites with lulz images of goats and pro-LGBTQ imagery.³

STATE, EMPIRE, OR MULTITUDE MINIONS?

GhostSec was a group of hacktivists, originally aligned with Anonymous, attacking politically violent Islamic groups, including Al-Shabaab, Boko Haram, and the

² On GhostSec’s update website the group put out a call for translators and anyone else who might have expertise useful to their cause: “Help might include naming and shaming site owners on social media, gathering intel about the sites and site owners and sending it to GhostSec members, or reporting sites to their hosts if they contain illegal content so that their host bans them.”

GhostSec

Anonymous non-state political actor

Ghost Security Group

Eaten by the State



WauchulaGhost/#GhostofNoNation

Expression of *Multitude*

GhostSec

Enveloped by *Empire*

FIGURE 3.
The Evolution of
GhostSec.

Islamic State (IS). GhostSec wanted to expose extremist Twitter accounts and take down their online presence. And it did. The goal was to prevent the “bad guys” from using cybertools to support their violence in Somalia, Nigeria, Libya, and Syria. As such, GhostSec was a humanitarian cause that prevented the territorialization of cyberspace by terrorists. It was a noble cause, a cyber battle, almost mythic. Was it so simple, though: good versus bad? And what was the desired outcome?

On one level, it would appear that GhostSec was doing its part to curb potential violence. GhostSec was severing an extremist group’s networking tool, effectively “neutering...[their] ability to use Twitter to broadcast its message outside of its core audience...reducing the organization’s ability to manipulate public opinion and attract new recruits (Berger and Morgan 2015:56).

But did these actions address the deeper problem of why Al-Shabaab and others exist? These Islamic fighter

groups were against the Western post-Westphalia liberal state. So was it possible that GhostSec’s actions were merely reproducing the same state structures (Althusser 2014) that ISIS and others so adamantly opposed? Or had GhostSec found a new way, a political action that shed state thinking (Bourdieu 2014)? It could be that GhostSec was effectively de-territorializing communication that had been territorialized for violence. If so, GhostSec was a piracy movement, carving out openings or temporary autonomous zones (Bey 1987) in the name of human rights. Or perhaps GhostSec was merely a privateer, “a private warrior” that generated profit from the global war on terror (de Zeeuw 2015:3).

The story above is about the role of GhostSec in international politics, specifically examining whether the hacktivist group was state-aiding, Empire-building, or Multitude-fulfilling (Hardt and Negri 2000). GhostSec was borne from the larger, amorphous movement

But did these actions address the deeper problem of why Al-Shabaab and others exist?

3 Multitude is a term drawn from Hardt and Negri (2004). Drawing from Spinoza, they define the multitude as “an open and expansive network in which all differences can be expressed freely and equally, a network that provides the means of encounter so that we can live in common... is composed of innumerable internal differences that can never be reduced to a unity or a single identity—different cultures, races, ethnicities, genders, and sexual orientations; different forms of labor; different ways of living; different views of the world; different desires. The multitude is a multiplicity of all these singular differences” (Hardt and Negri 2004:xiii-xiv).

BIBLIOGRAPHY

- Althusser, Louis. 2014. *On the Reproduction of Capitalism: Ideology and Ideological State Apparatuses*. Trans. and ed. G. M. Goshgarian. London, UK: Verso.
- Auerbach, David. 2015. “The Hacktivist War on ISIS?” *Slate*, December 10. Available at link.
- Berger, J. M., and Jonathon Morgan. 2015. “The ISIS Twitter Census: Defining and Describing the Population of ISIS supporters On Twitter.” *The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper*, No. 20, March. Available at link.
- Bey, Hakim. 1987. *T.A.Z.: The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism*. Brooklyn, NY: Autonomedia.
- Bourdieu, Pierre. 2014. *On the State*. Cambridge, UK: Polity Press.
- British Broadcasting Service (BBC). 2015. “Charlie Hebdo Attack: Three Days of Terror.” *BBC News Online*, January 14. Available at link.
- Coleman, Gabriella. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, UK: Verso.
- de Zeeuw, Daniel. 2015. “Pirates and Privateers: An Introduction in Three Acts.” *Krisis: Journal for Contemporary Philosophy*, Issue 1: 2–9.

known as Anonymous that had already executed a wide range of actions on the internet, from Operation Avenge Assange to Project Chanology to #OpTunisia to Operation AntiSec. As anthropologist Gabriella Coleman (2014) details in *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, Anonymous has used multiple tactics as well as multiple ideological stances. While the overriding premise of the movement seems to be “Anonymous is not unanimous” and information should flow freely (Coleman 2014:106), it has “no consistent philosophy or political program” (Coleman 2014:3). Nevertheless, it is vulnerable to grander sociopolitical forces, such as states, that attempt to capture the movement for its/their own needs.

With GhostSec we see a new, complex manifestation of Anonymous. It’s a triadic struggle between the exogenous forces of the State, Empire, and the Multitude (Hardt and Negri 2000, 2004). The weapons of GhostSec are XSS and DDOS attacks, webpage defacements, and straight-out lulz-screwing with Islamic extremist Twitter accounts. The complexity began when the Anonymous group split in fall 2015 (Auerbach 2015). The apparent success of GhostSec in its efforts to deter ISIS and others prompted the United States government to ask the Anonymous cell for intel help, which tore the group open via competing sociopolitical forces: the State, Empire, and the Multitude. It was the Weberian, hierarchical, bureaucratic apparatus versus “the decentered and deterritorializing apparatus of rule that progressively incorporates the entire global realm” (Hardt and Negri 2000:xii) versus the autonomous force that “has the capacity to create society on its own” (Hardt and Negri 2004:225). The tug of war resulted in the creation of the splinter faction, the GSC. The now nonprofit organization was then pulled into the fold of the State. As for the original GhostSec, it morphed into a transcendental arm of Empire, a force that considers violence and war legitimate when “in the service of right and peace”

(Hardt and Negri 2000:15).

But the morphing of GhostSec did not end there (See Figure 3). This version had its own internal schisms. It broke asunder, and core member WauchulaGhost became a solo Anonymous warrior. The rest of GhostSec merged with BlackOps Cyber, which was part of a private, international intel agency. In the end, it seemed that only WauchulaGhost moved into the realm of the Multitude, a nomad, “plural and multiple,” a new democratic form a la Hardt and Negri (2004:99).

The fact that GhostSec took advantage of the erosion of state-based authority appears to be part of something different, possibly new, in international politics. GhostSec may be an expression of the Empire force as envisioned by Hardt and Negri (2000). GhostSec did not align with one single state, but rather contributed to the global formation of a distributed and nonstate-centric sovereign sociopolitical force. In effect, GhostSec would become a part of the production of Empire’s war factory, or could be a part of the Multitude dynamic that could transform “through historical action and create a new world,” a new democratic order (Hardt and Negri 2000:159). So even though the trickster lulz Anonymous may jump out and raspberry the world while it “takes down” a terrorist group’s web presence, it still must consider who benefits from its antics. Are they feeding the State? Boosting Empire? Or could they be entering the Multitude: “the only social subject capable of realizing democracy, that is, the rule of everyone by everyone” (Hardt and Negri 2004:100)? ■

ROBERT TYNES is a political scientist and a member of the Bard Prison Initiative at Bard College.

ACKNOWLEDGMENTS

I thank the editors, Gabriella Coleman and Chris Kelty, for their invaluable comments and suggestions. Some of research and writing for this article was first presented at the 17th Annual Conference of the Association of Internet Researchers (AoIR) in Berlin, Germany, 5–8 October 2016. Bard College contributed partial funding for the research.

Gladstone, Rick. (2015). “Behind the Veil of Anonymity, Online Vigilantes Battle the Islamic State.” *The New York Times*, March 24. Available at link.

Hardt, Michael, and Antonio Negri. 2000. *Empire*. Cambridge, MA: Harvard University Press.

———. 2004. *Multitude: War and Democracy in the Age of Empire*. New York, NY: Penguin Books.

International Business Times. 2015. “‘Operation Charlie Hebdo’: Anonymous Threatens to Kill Terrorists, Hack Websites in Response to Paris Attack.” *International Business Times*, January 10. Available at link.

Raincoaster. 2015. “Putting #ISIS on Ice: An Interview with GhostSec of #Anonymous and Ghost Security Group.” *The Cryptosphere*, November 16. Available at link.

Rajan, Nitya. 2016. “This Is What It’s Like To Be An ‘Anonymous’ Female Hacker.” *HuffPost Tech*, March 24. Available at link.

Segall, Laurie. 2015. “The Secret Hackers Trying to Bring Down ISIS.” *CNNMoney*, November 20. Available at link.

Stone, Jeff. 2015. “Ghost Security Hackers, Offshoot of ‘Anonymous,’ Claim They Disrupted ISIS Attack by Intercepting Twitter Messages.” *International Business Times*, September 1. Available at link.

Wark, McKenzie. 2004. *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Rebecca Slayton looks at efforts to blend, certify and market the subversive skills of hacking with the ethos of professionalism.

the PARADOXICAL
AUTHORITY
of
the CERTIFIED
ETHICAL
HACKER

IN JULY 2013, the front page of *The New York Times* reported that Edward Snowden was a Certified Ethical Hacker (CEH). The *Times* noted that the certification process would have “given him some of the skills he needed to rummage undetected through N.S.A. (National Security Agency) computer systems and gather the highly classified surveillance documents that he leaked last month” (Drew and Shane 2013).

The founders of the CEH credential quickly distanced themselves from Snowden’s actions, noting that CEHs were required to follow a code of ethics, and that only one had previously lost a certification for disclosing confidential information (Drew and Shane 2013). By contrast, Indian papers were proud of the revelation that Snowden had received training in Delhi. The *Times of India* reported, “The hacker who shook the US intelligence machinery and had world leaders railing against the United States for spying on them picked up crucial skills in India” (Phadnis 2013:1). To undermine the U.S. intelligence machinery, it implied, was also to demonstrate technical mastery.

These responses illustrate a tension within the CEH credential: it sought to appropriate the technical savvy associated with hackers and the U.S. military and intelligence agencies while distancing itself from the untrustworthy and morally suspect image of hacking. In this essay I show how these tensions animated the early development and popular reception of the CEH credential. I argue that the certification did not represent the professionalization of ethical hacking—a field that had already existed for decades—so much as it did an effort to certify and market a blend of hacker skills and professional ethics.

I first describe how anxieties about hackers and the ethics of skilled information technology workers fostered the rise of information security certifications in the 1990s. I next discuss the establishment and early popularization of the CEH, showing how the credential sought to appropriate the technical authority and



mystique of hackers and the U.S. military without the stigma of the popular association of hackers with criminal activity. I then discuss how the authority and credibility of the certification was ultimately limited by the tension between the goals of professionalism—to standardize and authorize knowledge practices—and the creative and subversive spirit of hacking.

THE RISE OF INFORMATION SECURITY CERTIFICATIONS

Early efforts to establish information security certifications grew out of the audit community, and were modeled on the Certified Public Accountant. William Murray, a leader in the Electronic Data Processing (EDP) Auditors society, recalls first suggesting the idea in the mid-1980s, as hackers began making news headlines: “We were experiencing the same problems that have confronted every emerging profession including how to separate the professionals from the amateurs. It was particularly important for us because of the amateur, i.e., ‘hacker,’ culture that surrounded so much of what we do” (Murray 2003:76).

In 1989, the EDP Auditors society joined with other professional computing organizations to create the International Information Systems Security Certification Consortium, or (ISC)², a new organization dedicated solely to establishing a certification in information security. Over the next several years, (ISC)² developed the Certified Information Systems Security Professional (CISSP) exam, which was finally launched in 1994.

CISSP provided a broad, business-oriented perspective on security; it was based on 17 different “specialty areas,” which included access control methods, regulatory and legal issues, cryptography, policy development, and “information ethics” (Tipton 1993). Importantly, certification also required that members swear to uphold the (ISC)² code of ethics.

For many employers, the CISSP served not only to educate workers, but also to “civilize” highly skilled technical people by assuring their ethical intentions and suitability for business. For example, Steve Akridge spent 20 years in the Navy and retired in 1995 as a chief cryptologist, but industry employers wanted him “to prove he could address bottom-line problems and direct large operations security outside the military” (Dugan 2001:36). Organizations interested in “ethical hacking” services also expressed

a preference for CISSP-credentialed contractors because “CISSPs must take a vow to adhere to a high code of ethics that includes reporting unlawful activities” (Messner 1999:25).

While CISSP focused on deep technical skills, the System Administration, Networking and Security (SANS) Institute began developing a set of Global Information Assurance Certifications (GIAC) around 2000. By the early 2000s, CISSP was the best-known certification, followed by GIAC, but additional certifications were proliferating. As of late October 2003, *Certification Magazine* reported 56 vendor-neutral and 20 vendor-related security certifications. As the magazine reported, “IT [information technology] professionals seeking information security certifications have an embarrassment of riches to choose from” (Tittel 2004: 28).

ESTABLISHING THE CERTIFIED ETHICAL HACKER

The CEH credential grew out of this burgeoning economy of information security certifications. Ethical hacking had been a professional pursuit since at least the mid-1960s, when the U.S. military and other organizations began using “red teams” or “penetration testers” to attempt computer security breaches, and thereby help in identifying and mitigating vulnerabilities. However, the CEH credential was not directed primarily toward penetration testers, but rather toward any professionals who could benefit from learning to think like a hacker. It distinguished itself from other certifications by the promise of a proactive rather than a reactive approach to security, wherein organizations could anticipate and prevent breaches instead of constantly recovering from and planning around their most recent breach.

The first organization to offer CEH training was Intense School, a company established in 1997 by two brothers and IT consultants, David and Barry Kaufmann, and their cousin, Ron Rubens. As the name suggests, Intense School offered “boot camps” in information technology, and in the late 1990s, it began offering training for CISSP. However, it found the (ISC)² certifying body difficult to work with, so with the help of some hackers with military experience, it developed an ethical hacker certification (Ron Rubens, personal communication, October 23, 2016). After attending a federal information technology trade show in 2003, the

new certification began attracting publicity. As *Washington Technology* reported: “When hackers go bad, they bust into your Web site and wreak havoc. But when they go good... they may very well come from Intense School” (Socha 2003).

The founders of Intense School were not the only ones to see the appeal of the CEH. In response to the terrorist attacks of September 11, 2001, Jay Bavisi, a legal professional trained in Britain, led the establishment of the International Council of E-Commerce Consultants, or EC-Council, to help certify professionals who could protect against attacks on electronic commerce. By 2003 it was offering the “Certified Ethical Hacker” certification (<https://www.eccouncil.org/about/>). Rather than establishing entirely new schools, the EC-Council became a certifier of training courses and exams, mobilizing entrepreneurs in the information security training business. Rubens recalled that Intense School wanted to focus on training rather than building up the credibility associated with a certification (Ron Rubens, personal communication, October 23, 2016). By 2009, Intense School was recognized by EC-Council as the “#1 Authorized Training Center in North America” (<http://www.intenseschool.com/about/>). EC-Council’s strategy allowed the Ethical Hacker certification to expand rapidly, and by 2007 CEH courses were offered in more than 60 countries.

Paradoxically, the international spread of the credential resulted from the intensely local nature of training. Although some companies did begin offering online training—for example a “midnight hacking” course provided a “quick overview”—geographically specific boot camps provided the more in-depth training (Paulson 2006:3). In June 2003, *Forbes* signed up one of its tech reporters for the ethical hacker boot camp, and in the fall, she reported on her experience in a course held at a Comfort Inn in the Washington, DC, suburbs. She described the instructor as a “20-year veteran of the Canadian military” who was a “jovial version of a drill sergeant” (Schoenberger 2003: 119). Her class consisted of 18 men and 2 women from both private and government organizations, including the Army, Air Force, Department of Commerce, Microsoft, and other private sector firms (many of which were government contractors).

Military patrons were a crucial source of authority for the CEH credential.

Hire a CEH. He can Protect and Defend your network from attacks.

My name is HackMaster.
I bring down networks and steal Data.
I dare you to stop me from taking your network down.

CEH Sign Up for CEH Class Today. **EC-Council**

Don't Worry. I'm a CEH. I will handle it.

CEH Sign Up for CEH Class Today. **EC-Council**

Hire a CEH. He can Protect and Defend your network from attacks.

CEH Sign Up for CEH Class Today. **EC-Council**

Advertisements for CEH certification programs.

Announcing its certification in 2003, Intense School noted that it had been training defense department and National Security Agency workers for 18 months (Swartz 2003). It also hired former military professionals as instructors. While its “boot camp” style of training was not unique—other IT training programs were similarly structured around “all-inclusive” packages that covered lodging, food, and training—the boot camp also simulated elements of hacker sociality, such as marathon hacking sessions that

kept students up all night, fueled by piles of junk food.

CERTIFICATION VERSUS “REAL WORLD” EXPERIENCE

While the ethical hacker certification sought to appropriate the authority of hackers and the military, many hackers gave it little credence. For example, Pieter “Mudge” Zatko, a hacker who also worked on security for a Department of Defense contractor, suggested that ethical hacker certifications could be used to “weed out job candidates,” but that they didn’t teach real-life experience: “Certification courses teach you about buffer overflows and Microsoft hacking tools—stuff that’s already well known and rudimentary and then you get a hacker title. It doesn’t mean you have a strong grasp of security” (Leung 2005: 47).

The real skills of hacking were portrayed as resistant and even opposed to institutionalization. Marc Maiffret, a hacker who co-founded eEye Digital Security in 1998, stated: “Typically hackers are people who didn’t finish college because they were so into finishing [their hacking] project. I didn’t finish high school and there are people here who have PhDs in computer science who learned hacking on the side” (Leung 2005: 47). One professional who held the CEH label among other certifications acknowledged this point: “Real world experience and knowledge are what will carry the day. The best hackers are not the certified ones, but are the ones that are doing it for real and normally do not poke their heads up too often. Be practical, not certified” (Bort, 2008). Asked about the ethical hacker

certification in 2003, one “black-hat” hacker wrote: “Some ‘IT pros’ may find a few techniques to secure against well-known attacks, but the underground is always 10 steps ahead” (Swartz 2003).

Proponents of certification also acknowledged the derivative nature of such training in their responses to the question often posed to ethical hacking schools: Couldn’t the training be turned to nefarious purposes? Aaron Cohen, founder of the “Hacker Academy” in Chicago, said, “Hackers don’t need our help” (Paulson 2006:3). Furthermore, Cohen and his lead instructor, Ralph Echemendia, argued that it was important to learn from “black-hat” hackers. Echemendia, who had learned hacking as a teenager and went on to teach for Intense School, argued against the view that “if you associate with hackers you can’t be a certified professional.” He ran an underground hacker meeting where participants remained relatively anonymous, explaining that he got “real-world” information from them and occasionally tried turning them to legal hacking (Paulson 2006:3).

At the same time, training centers also felt pressure to distance themselves from the underground world of illegal hacking. When Intense School engaged the notorious hacker and social engineer Kevin Mitnick to help with one of its courses, certain companies threatened to cut their ties with the training program. Partly to satisfy their customers, and partly out of an uneasy sense that Mitnick might be an untrustworthy partner, they did not continue working with him (Ron Rubens, personal communication, October 23, 2016).



Industry Week February 7, 1994, p. 43.

CONCLUSION

Professional institutions and standards have historically been offered as a substitute for the interpersonal trust that becomes infeasible in a large and geographically dispersed field (Porter 1996; Shapin 1995). Something similar was at work with ethical hacker certifications in the early new millennium. As governments and corporations moved their operations online, demand for “ethical hackers” rose sharply, as did demand for means of demonstrating their trustworthiness.

But contrary to what theories of professionalization might suggest (Abbott, 1988), the ethical hacker certification did not come from penetration testers seeking to control entry to their field of work. In fact, the certification was not aimed primarily at people interested in becoming full-time penetration testers, but rather at any professional who could benefit from learning to “think like a hacker.” Rather than representing the professionalization of ethical hacking, the certification emerged as a means by which entrepreneurs could capture a particular market niche in the rapidly growing business of information security certifications. The certification promised to meld a professional ethos with the technical prowess of hackers.

While this melding was persuasive to many, the tension between the subversive skills of hacking and the standardizing aims of professional certification ultimately limited the authority of the credential. Hackers were quick to recommend being “practical, not certified.” And while U.S. military agencies implicitly endorsed the certification by sending some of its personnel to be trained, neither the Department of Defense nor civilian agencies ever granted the certification the monopoly powers enjoyed by organizations such as the American Medical Association. Certification became a valuable currency for jobseekers, but it continued to derive its credibility from the darker and more mysterious worlds of the military and hacking. ■

REBECCA SLAYTON is Associate Professor jointly in the Science & Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies.

BIBLIOGRAPHY

- Abbott, Andrew. 1988. *The System of Professions: An Essay on the Division of Expert Labor*. Chicago: The University of Chicago Press.
- Bort, Julie. 2008. “Security Certs, Vampires and Dumpster Diving.” *Network World*, April 10. link.
- Drew, Christopher, and Scott Shane. 2013. “Résumé Shows Snowden Honed Hacking Skills.” *The New York Times*, July 4. Available at link.
- Dugan, Sean. 2001. “Certifiably Secured.” *InfoWorld*, July 9, p. 36.
- Leung, Linda. 2005. “Hackers for Hire.” *Network World*, June 20, p. 47.
- Messmer, Ellen. 1999. “Could You Pass This Tough Security Test?” *Network World*, March 15, p. 25.
- Murray, William H. 2013. Oral history interview with William H. Murray. Charles Babbage Institute. Retrieved from the University of Minnesota Digital Conservancy. Available at link. P 76.
- Paulson, Amanda. 2006. “New Academy Teaches ‘Ethical Hacking.’” *Christian Science Monitor*, December 13, p. 3.
- Phadnis, Shilpa. 2013. “Snowden Honed Hacking Skills in Delhi.” *Times of India*, December 4, p. 1.
- Porter, Theodore. 1996. *Trust in Numbers*. Princeton, NJ: Princeton University Press.
- Schoenberger, Chana. 2003. “A Week at Hacker Camp.” *Forbes*, September 15, 119–120.
- Shapin, Steven. 1995. “Trust, Honesty and the Authority of Science.” In *Society’s Choices: Social and Ethical Decision Making in Biomedicine*, edited by Ruth Ellen Bulger, Elizabeth Meyer Bobby, and Harvey V. Fineberg (pp. 388–408). Washington, DC: National Academies Press.
- Socha, Evamarie C. 2003. “Survival Guide: Ron Rubens, CFO and COO, Intense School.” *WashingtonTechnology.com*, April 17. Available at link.
- Swartz, Jon. 2003. “Tech Pros Get to Know Their Enemy.” *USAToday.com*, September 23. Available at link.
- Tipton, Hal. 1993. “Certification of Security Practitioners.” *Information Systems Security* 1(4): 75–84.
- Tittel, Ed. 2004. “Building a Career in Information Security.” *Certification Magazine*, April, pp. 28–31, 48.

On reusable pasts

What makes a biohacker a hacker?
Sara Tocchetti explores the life (and lives) of hackers who care about living things.

#HACK EVERYTHING, TO CHANGE WHAT?

In the last 10 years, one of the most significant transformations in the subculture of computer hacking is that it has become mainstream. For instance, it is quite common to read in tech magazines such as *Make* that curtain rings used to hang bananas are a “banana hook hack” (Torrone 2006), that taking macro pictures by mating lenses together is a “macro lens hack” (Cunningham 2008), and that amateur tax evasion is a “tax hack” (Torrone 2010). As computer hacking hits the mainstream, discussions arise on the use of the “original” terms (Branwyn 2015), new modes of distinctions emerge. The semiotic-material productions of the subculture, with their capacity to produce meaning and agency, are borrowed and adopted as much as reused, co-opted, or recuperated. Some even propose that “hacking is being hacked” (Söderberg and Delfanti 2015).

In this piece I take the example of biohacking to argue that this borrowing of semiotic-material productions actually might have precluded biohackers and DIYbio members from elaborating situated, nuanced articulations of their personal and collective experiences of becoming or being life scientists in the age of “Big Biology”. The example of biohacking tells us that by becoming mainstream, the semiotic-material productions of computer hacking might have turned into a “reusable past,” if not worn-out semiotic-material productions; a practice that becomes so normal that it is easy to appreciate what it enables while it is

difficult to acknowledge what it obscures.¹ I conclude by inviting adopters of biohacking to engage with some hands-on fabrications drawn from companion accounts and agential heterogeneities rooted in feminist, race, environmental, and labor politics.

#NEOLOGISMS, ANALOGIES, AND EMBODIMENT IN SOCIO-TECHNOLOGICAL STORYTELLING

The composite neologism “biohacking” was first used by Michael Schrage in a minor article published in *The Washington Post* in 1988. Under the title “Playing God in the Basement,” Schrage, who now describes himself as “one of the world’s most innovative thought leaders on innovation,”² made a revelatory forecast. Based on the opinions of influential figures such as distinguished professors and chief scientists of major biotech companies, Schrage proposed that the analogy between personal computers and biotechnology was ripe, and as such, the “rise of the Bio-hacker” was to be expected. According to the director of BioTechnica International, recombinant DNA technologies were becoming generally easier to use and had declined in costs, thus begging a parallel with the microprocessor industry; sociologist Everett Rogers, who studied the subculture of computer hackers, claimed that as hackers found in the computer a medium to express themselves in creative and artistic ways, a similar subculture could soon arise around DNA. Another expert argued that the analogy was oversimplified and flawed; however, the same expert also mentioned that some genetic modifications were becoming routine and could be performed by high school students, especially if sponsored by biotech firms. In conclusion, a diffusion of biotechnology into the public domain was to be expected.

Discontinuously but incrementally, in the past two decades the tropes of homemade DNA, biotechnology as the next personal computer revolution, and the figure of the biohacker have gained momentum. Sequencing DNA and developing open source

1 The term “reusable past” refers to the next step of what Christopher Kelty (2008), in a seminal study of FLOSS communities, has called a “usable past.” A usable past “is a more charitable term for what might be called modern myths among geeks: stories that the tellers know to be a combination of fact and fiction. They are told not in order to remember the past, but in order to make sense of the present and of the future” (Kelty 2008:65). The use of the term “reusable” refers to the fact that usable pasts vested in present narratives, such as the ones related to computer hacking, can themselves be reused, such as in the case of biohacking.

2 Available at <http://executive.mit.edu/faculty/profile/77-michael-schrage>.



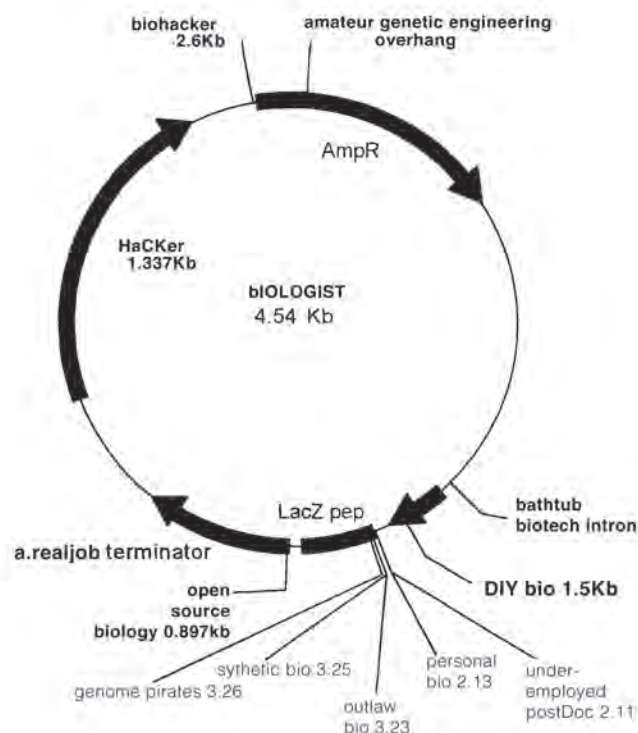
and
worn-out futures

software tools for bioinformatics were described as “hacking the mother code” (Regis 1995) or “hacking the genome” (Counsell 2004; Newitz 2002; Professor L. 2003). Authors occupied with the forecasting of biotechnology’s future announced the advent of “amateur genetic engineering” (Katz 1990) and “the coming wave of bathtub biotechnology” (Schrage 1992), whereas people practising various forms of genetic engineering at home were called “genome pirates” (Eudes 2002). Last, renowned science fiction writers published stories intertwining biopunk and biohacking narratives (McAuley 2000). What is revelatory about these practices of storytelling is that at the time of publication, there were no self-claimed biohackers on the scene. The term was a “prospecting neologism,” and yet in retrospect these narratives were quite accurate in describing what came next, thus rendering it necessary to ask what, in socio-technical storytelling, is “the already determined” in what is later recognized as “having been predicted.”

Beginning in 2005, this distinct rhetorical repertoire was embodied by the founders of synthetic biology (SB) and their closest PhD and graduate students at the Massachusetts Institute of Technology (MIT) beginning in 2005. According to Sophia Roosth (2010), SB founders in Boston were reared in MIT’s hacking tradition. This type of cultural circulation and borrowing was facilitated by the professional conversion of Tom Knight, an influential member of the first generation of computer hackers at MIT. Persuaded by a physicist that biology was not as complicated as he thought, Knight successfully requested a grant from the Defense Advanced Research Project Agency (DARPA) to test his idea of biobricks, or standardized genetic modules. At the same time, Drew Endy (a civil engineer) and two other colleagues, then at the Molecular Science Institute in Berkeley, California, were elaborating (also in a grant proposal proposal for DARPA) the socio-technical vision of an “open source biology.” They imagined a community that “will rely on individuals and small groups of people to take charge of...maintaining and improving the common technology, open to all, usable by all, modifiable by all” (Carlson and Brent 2000:1). As Endy moved to MIT and started to work with Tom Knight, his alignment with the Free Software/Open Source (FS/OS) movements and the representation of himself and his students as “outspokenly liberal members of these communities” (Roosth 2010:88) became more explicit. As Roosth writes:

Lab members peppered their speech with hacker lingo: a clever solution to a difficult problem was a “hack,” and to intuitively and deeply understand something was to “grok” it. Instead of “publishing” a paper, they talked about hurdling peer review as either “celebrating” their work or “sharing ideas” (Roosth 2010:90).

In brief, as Roosth proposes, “an MIT-specific, hackerly and Open Source approach to biological construction [is] one that trades on the equation of DNA to source code and then posits that such code must be editable and shareable” (Roosth 2010:94). Furthermore, historian Luis Campos and sociologist Adrian MacKenzie both argue that, in the context of the emergence of



synthetic biology as a global discipline, biohacking and, more broadly, open access were important semiotic-material borrowings used to establish several strategic institutional and educational initiatives (Campos 2012, 2013; MacKenzie 2009).

#BECOMING-LIFE-SCIENTIST IN THE BIG BIOLOGY ERA

Today, what Roosth calls the “hackerly sources of synthetic biology” (2010:83) have mostly faded away in what has become a fully institutionalized and global research field. Instead, the term has become part of a spinoff of synthetic biology, the Do It Yourself biology (DIYbio) network. Founded in 2008 and located largely in the western world, the DIYbio network is composed mainly of white, male, young, and/or disenfranchised academics from the life sciences and other natural sciences or computer engineering disciplines who see in the network an opportunity to revive their passion for science. They form community laboratories, but also work at home, or between university, corporate, and community laboratories. Frequent activities include the fabrication and selling of cheap and user-friendly laboratory instruments and kits; the extraction of DNA from fruits or buccal scrub samples using household ingredients; the genetic modification of bacteria or yeasts; the genetic identification of species, phenotype distributions, and gene variants; and the growth of bacterial and fungi biomaterials and the preparation of fermented products. These activities are often performed in collaboration with science festivals, sciart events, educational charities, and

modern craft fairs. The most advanced DIYbio groups collaborate with synthetic biologists or function as incubators for small biotech startups. DIYbio has attracted the attention of influential technology magazines as well as the mainstream media.

In the context of DIYbio, numerous scholars have described and commented on the use of the term “biohacking” and the borrowings of narratives and practices from computer hacking, and provide two main explanations. First, these borrowings reflect a further step in the diffusion of metaphors, models, and machines from the computer sciences into the life sciences. Second, these borrowings signal a specific crisis in the moral process of becoming a life scientist, which is one of the proprietary regimes of biotechnology (Delfanti 2013). Furthermore, most authors recognize in biohacking a counterpolitics that should be welcomed or itself borrowed to transform other fields of practice, for instance the field of science mediation and citizen science (Davies et al. 2015; Golinelli and Ruivenkamp 2015; Kera 2012, 2014; Landrain et al. 2013; Seifert 2015). I argue that the semiotic-material borrowings from computer hacking actually signals a broader phenomenon than just the expansion of metaphorical and methodological analogies between computer sciences and life sciences, or the moral ambiguities related to the proprietary regimes of biotechnology. This broader phenomenon is the experience of becoming or being a life scientist in the sociopolitical context of what is commonly called “Big Biology.”

#PERSONAL POLITICS AND REUSABLE PASTS

By considering the historical context in which the politics of personal computers emerged, rather than just the socialities or the ethics of computer hacking movements, most biohacking initiatives could instead be called a “personal biology.” The politics of freedom, decentralization, and empowerment that made the personal and networked computer into a revolutionary spoke-technology (Turner 2006) profoundly mark the politics of biohacking. A personal biology is a socio-technical vision that results from the implosion of the legacy of the Whole Earth Catalog, the spectacle of grassroots American innovation (Tocchetti 2012), and “entrepreneurial citizenship” (Irani 2015). In this sense, biohacking as a personal biology is a practice established by a group of young and/or disenfranchised scientists in their uncertain attempt to come up with a technoscience that they can live through, and live with.

For instance, in the middle of the 2013 European horse meat scandal, Thomas Landrain, a major figure of the DIYbio network, posted on the group’s blog what he called a “quick and dirty” version of DNA barcoding,³ with an aim to enable everyone to determine what was on their plates.

In the experiment described in the blog post, a cheap and quick hands-on version of a technique usually used in food laboratories becomes a demonstration of how science, when “put in the hands of people,” can enable individuals, including blog readers, to know the truth about what is on their plates. The convergence of post-financial crisis cuts in government-run food testing laboratories (Lawrence 2013a) and the breach in accountability of food supply chains under neoliberal economies and their collision with organized crime (Lawrence 2013b) are

possible, du DNA barcoding en mode Quick and Dirty! En sacrifiant de la sensibilité à la méthode, nous avons réussi à réduire le temps d'analyse à 4h (au lieu de 3j!) et à un cout que d'environ 3-5 euros (au lieu de 200 euros) par échantillon !



La documentation complète pour le protocole se trouve [ici](#) ou sur le wiki de La Paillasse. Je vous invite à le lire et à le commenter.



Pour l'article scientifique dont nous nous sommes inspirés pour mettre en place ce protocole, c'est [ici](#).

FIGURE 1: Industrial lasagna: the public question and the personal answer. On one side, a dish of appetizing lasagna is marked with a worrying question mark. On the other side, “the answer” is glowing out of an electrophoresis gel produced during one of the barcoding experiments carried out at La Paillasse, the DIYbio public laboratory based in Paris.

overshadowed by a joyful and empowering demonstration of a cheap and dirty genotyping workshop. The political complexity and contemporary crisis of institutionalized accountability in neoliberal democracies are not easy to blog about, nor is it easy to propose an interactive hands-on activity that can give an individual the impression of being able in some ways to address this crisis herself, even if only by analyzing the industrial lasagna on his or her plate. On the contrary, the activity of La Paillasse was suited to a blog post, literally giving the impression of putting agency back in the individual’s hands.

Similarly, the “networked bacterial incubator” designed by Avery Louie, a currently active member behind the resurrection/revivification of the Boston Open Source Science Laboratory, proposes to solve the problem of onerous weekend and late-night labwork by grad students by developing an incubator controlled via the Internet. On his blog, Louie writes:

This is an incubator re-imagined to be less horrible to use.... The problem here is that some poor soul (grad student) has to physically go to the incubator, and look at the plates and see if they are overgrown. If you think it will take 6 hours, and you put the cells in at 6 pm on Friday, that means you have to visit at midnight on Saturday morning, probably in a deserted building. Being in the lab alone is a bad idea. Rinse and repeat. That's like going to the post office every hour or so to check if you got mail—it is a silly thing to do. Besides being silly, there are better things to do on Friday nights. ⁴

Avery’s understanding that a technological intervention is also a political one is inscribed as a double meaning in his post’s title: “The Internet Enables Incubator Progress.” However, as in the previous example, a personal hands-on “solution” primes

3 DNA barcoding is a technique enabling the identification of species using their DNA. The term and the technique were proposed in the early years of this century by biologist Paul Hebert.

4 Available at <http://tequils0.wordpress.com/2014/03/23/internet-enabled-incubator-progress/>.

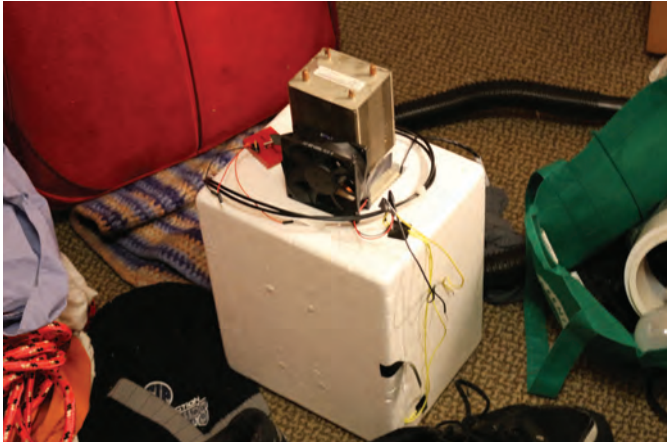


FIGURE 2. The Internet enables incubator progress.

other accounts of, for instance, collective labor struggles and reforms in the life sciences and other professional sectors.

Although brief, these examples illustrate that when understood as “personal biology,” the semiotic-material productions such as biohacking made possible by borrowing from computer hacking seem to be missing a structural and material critique

BIBLIOGRAPHY

- Bialski, Paula. 2017. “I Am Not a Hacker: The Hacking Practices of Self-Proclaimed Non-Hackers.” *LIMN* Number 8, this issue.
- Branwyn, Gareth. 2015. “On the Use of the Word ‘Hack’.” *Make:magazine*, October 11. <http://makezine.com/2015/10/11/on-the-use-of-the-word-hacks>
- Carlson, Robert, and Roger Brent. 2000. “DARPA Open Source Biology Letter.” http://synthesis.cc/DARPA_OSB_Letter.pdf
- Campos, Luis. 2012. “The Biobrick™ Road.” *Biosocieties* 7(2):115–139.
- . 2013. “Outsiders and In-Laws: Drew Endy and the Case of Synthetic Biology.” In *Outsider Scientists: Routes to Innovation in Biology*, edited by Oren Harman and Michael Dietrich (pp. 331–348). Chicago, IL: University of Chicago Press.
- Counsell, Damian. 2004. “Hacking the Code of Life.” *Linux User* 42:22–31.
- Cunningham, Collin. 2008. “How To—Macro Lenses Hack.” *Make:magazine*, September 28. <http://blog.makezine.com/archive/2008/09/how-to-macro-lens-hack.html>
- Davies, R. Sarah, Karin Tybjerg, Louise Whiteley, and Thomas Söderqvist. 2015. “Co-Curation as Hacking: Biohackers in Copenhagen’s Medical Museum.” *Curator the Museum Journal* 58:117–131.
- Delfanti, Alessandro. 2013. *Biohackers. The Politics of Open Science*. London: Pluto Press.
- Eudes, Yves. 2002. “Les pirates du génome.” *Le Monde*, September 18. http://www.lemonde.fr/societe/article/2007/09/13/des-tests-genetiques-pour-le-regroupement-familial_954621_3224.html
- Golinelli, Stefano, and Guido Ruivenkamp. 2015. “Do-It-Yourself Biology: Action Research within the Life Sciences?” *Action Research Journal* 1–17. doi:10.1177/1476750315586636.
- Jen, Clare. 2015. “Do-It-Yourself Biology, Garage Biology, and Kitchen Science: A Feminist Analysis of Bio-Making Narratives.” In *Knowing New Biotechnologies: Social Aspects of Technological Convergence*, edited by Mathias Wienroth and Eugénia Rodrigues (pp. 259–293). Abingdon, UK: Routledge.
- Haraway, Donna J. 1997. *Modest Witness@Second Millenium. FemaleMan@_Meets_Oncomouse™*. London, UK: Routledge.
- Irani, Lilly. 2015. “Hackathons and the Making of Entrepreneurial Citizenship.” *Science, Technology and Human Values* 40:799–824. doi:10.1177/0162243915578486.
- Katz Sylvan. 1990. “Forum: Roses Are Black, Violets Are Green—The Emergence of Amateur Genetic Engineering.” *New Scientist*, January 6.
- Katz, Sylvan. “Roses Are Black, Violets Are Green: The Emergence of Amateur Genetic Engineers.” *New Scientist* 125.1698 (1990): 66.
- Kelty, Christopher. 2008. *Two Bits: The Cultural Significance of Software*. Durham, NC: Duke University Press.
- Kera, Denisa. 2012. “Hackerspaces and DIYbio in Asia: Connecting Science and Community with Open Data, Kits and Protocols.” *Journal of Peer Production* 2:1–15.
- . 2014. “Innovation Regimes Based on Collaborative and Global Tinkering: Synthetic Biology and Nanotechnology in the Hackerspaces.” *Technology in Society* 37:28–37.
- Landrain, Thomas, Morgan Meyer, Ariel Martin Perez, and

that would take seriously the professional experiences of young and/or disenfranchised scientists by articulating those experiences with companion accounts of the epistemic and instrumental role of technoscience in the contemporary rearrangements of race, gender, social inequalities, and environmental struggles in our societies, which are becoming both increasingly neoliberal and conservative. To take this critique seriously does not prevent someone from taking a hands-on approach; instead, it entails thinking of these approaches in conjunction with a variety of individual and collective forms of civil disobedience and social organizing, including, for instance, demonstrations, occupations, strikes, petitions, direct action, investigations, whistleblowing, alternative and radical practices of science and technology, etc. These actions are largely ignored by individuals who claim to be biohackers.

#FICTIONAL CONCLUSIONS

Biohacking is a good case to question the notion of the politics of reusable pasts and how their politics retrofit the understanding of the present for the individuals who use them. From the very first techno-storytelling to their early embodiment in the emergence of synthetic biology and their stabilization in the politics of the personal biology of biohackers and members of the DIYbio network, the semiotic-material productions of computer hacking seem to favor the politics of personal technologies,

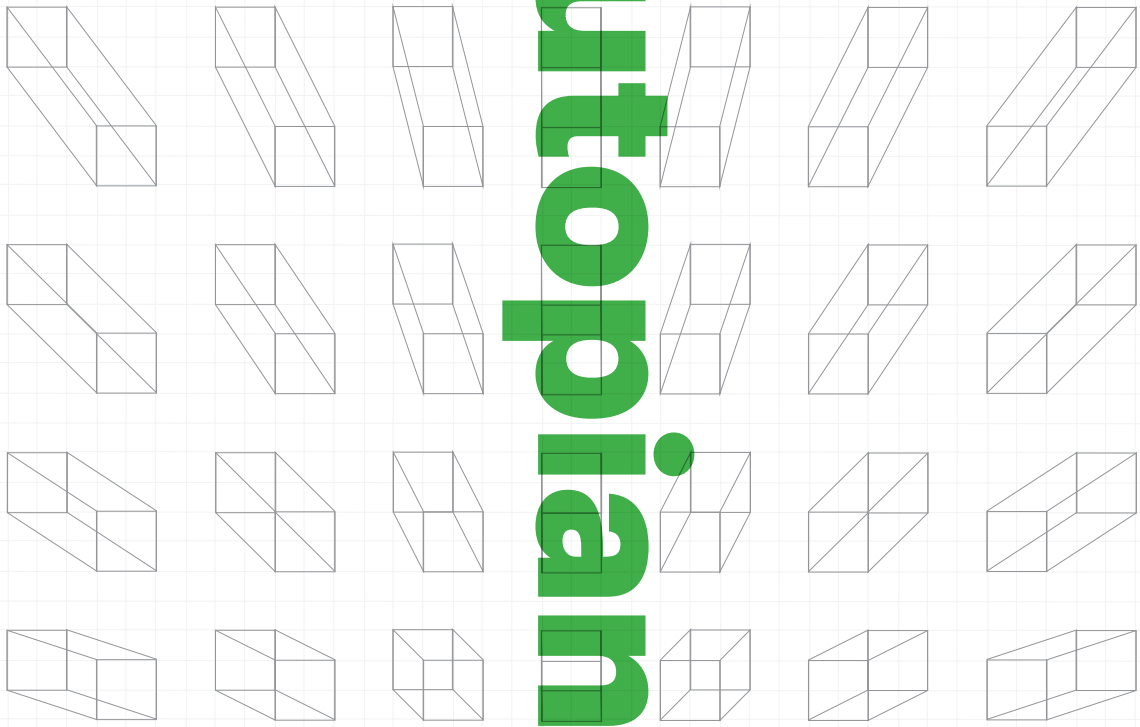
thus reducing the diversity of possible political fabulations about what it means to work and live in the era of Big Biology. In this sense, semiotic-material productions of computer hacking can be understood as a “reusable past,” if not actually worn-out semiotic-material productions. A bit like some of our favorite worn-out objects, these semiotic-material productions are not useless or meaningless; quite the contrary, their use and meaning is so normal and obvious that although we can appreciate the efficiency of the interpretations and actions that they enable, we become much less sensible to the interpretations and actions that these socio-material productions preclude.

In Bialski’s piece in this issue, we learn how the actions of corporate software developers resemble those commonly attributed to “hackers” although the developers themselves claim not to be “hackers” (Bialski 2017). Her examples show how the semiotic-material productions of hackers seems to transcend their linguistic and personal identification to be adopted implicitly despite not being explicitly recognized by the actors who adopt them. In the case of biohacking, it is another type of implicit identification at work through the borrowing of semiotic-material productions. What is implicitly but happily adopted are the politics of personal technologies and its specific theories and practices of social change through the technological empowerment of individuals. In this sense, we should be sensitive to the various shapes and forms of “hacking” as well

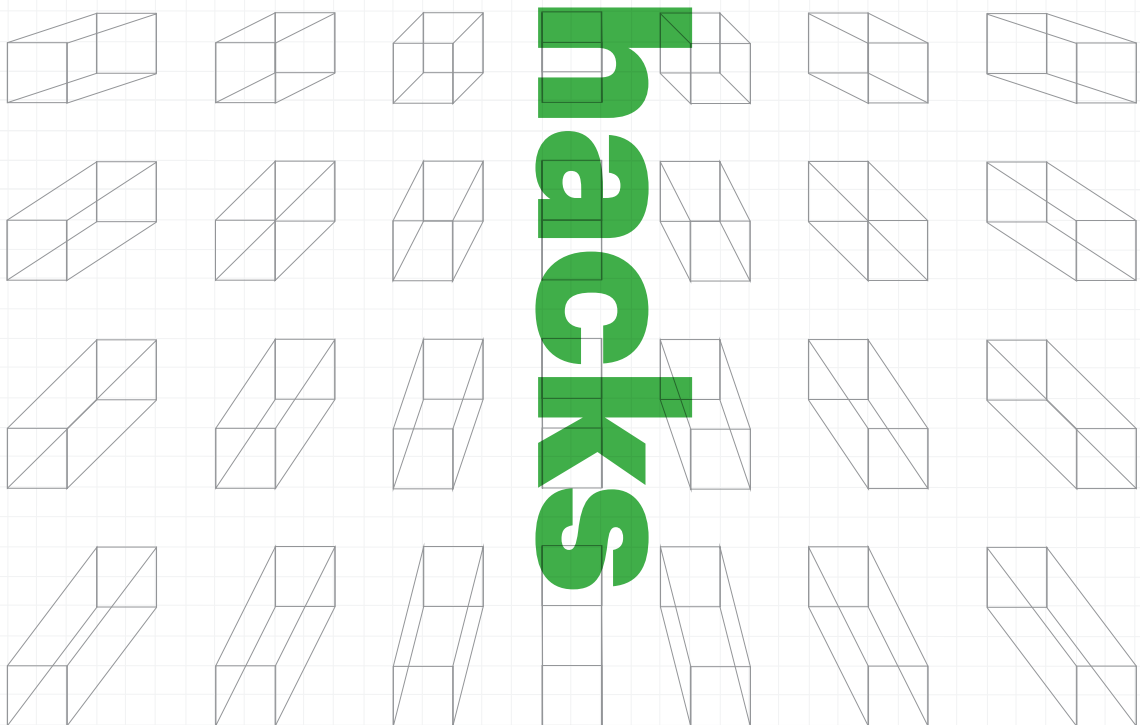
as to the conservative continuities of which semiotic-material productions are capable. Mine is an invitation to self-claimed biohackers (and DIYBio members sensible to this term), as well as to scholars who see in these initiatives an example of a truly participative science, to question the use of computer hacking as a usable past, and engage with forms of hands-on fabulations that are not only based on the politics of personal technologies but also seek to intertwine biohackers’ personal and collective experiences with feminist, race, environmental, and labor politics. Semantic-material fabulations such as, for instance, those by feminist hackers (SSL Nagbot 2016), and pragmatic critiques such as those proposed by feminist science scholars (Jen 2015) might well be the right tools to start the job. ■

SARA TOCCHETTI is an ex-biologist not yet turned into a science and technology scholar. She is an associate researcher at STSLab, University of Lausanne, Switzerland.

- Remi Sussan. 2013. “Do-It-Yourself Biology: Challenges and Promises for an Open Science and Technology Movement.” *System and Synthetic Biology* 7:115–126. doi:10.1007/s11693-013-9116-4.
- Lawrence, F. 2013a. “Horsemeat Burger Scandal: History Repeating Itself.” *The Guardian*, January 16. <http://www.theguardian.com/commentisfree/2013/jan/16/horsemeat-burger-scandal-history-repeating>
- . 2013b. “UK Warned of Another Horsemeat Scandal as Food Fraud Rises.” *The Guardian*, October 10. <http://www.theguardian.com/uk-news/2013/oct/10/uk-warned-another-horse-meat-scandal>
- MacKenzie, Adrian. 2009. “What Is Design in Synthetic Biology? From Techniques to Reflexive Meta-Materials.” [Unpublished paper] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.532.4406&rep=rep1&type=pdf>
- McAuley, P. 2000. “Danger—Hard Hack Area.” *Nature* 404(2):21.
- Newitz, Annalee. 2002. “Hacking the Genome.” *Wired*. <https://www.wired.com/2002/06/hacking-the-genome/>
- Professor L., 2003. “Hacking the Genome.” 2600 Magazine. Volume 20 Number 4 (Winter 2003–2004)
- Regis, Ed. 1995. “Hacking the Mother Code.” *Wired*, June 27. <http://archive.wired.com/wired/archive/3.09/hood.html>
- Roosth, Sophia. 2010. “Crafting Life: A Sensory Ethnography of Fabricated Biologies.” PhD dissertation, Massachusetts Institute of Technology, Cambridge, MA.
- Schrage, M. 1988. “Playing God in Your Basement.” *The Washington Post*, January 31.
- . 1992. “The Coming Wave of Bathtub Biotechnology.” *Los Angeles Times*, September 17. http://articles.latimes.com/1992-09-17/business/fi-683_1_biotech-industry
- Seifert, Franz. 2015. “Converging Technology and Critical Social Movements.” In *Knowing New Biotechnologies: Social Aspects of Technological Convergence*, edited by Mathias Wienroth and Eugénia Rodrigues (pp. 326–356). Abingdon, UK: Routledge.
- Söderberg, Johan, and Alessandro Delfanti. 2015. “Repurposing the Hacker: Three Temporalities of Recuperation.” (June 23, 2015). UC Davis Previously Published Works. <https://ssrn.com/abstract=2622106>
- SSL Nagbot. 2016. “Feminist Hacking/Making: Exploring New Gender Horizons of Possibility.” *Journal of Peer Production* 8. <http://peerproduction.net/issues/issue-8-feminism-and-unhacking/feminist-hackingmaking-exploring-new-gender-horizons-of-possibility/>
- Tocchetti, Sara. 2012. “DIYbiologists as ‘Makers’ of Personal Biologies: How MAKE Magazine and Maker Faires Contribute in Constituting Biology as a Personal Technology.” *Journal of Peer Production* 2. <http://peerproduction.net/issues/issue-2/peer-reviewed-papers/diybiologists-as-makers/archive/2006/11/banana-hook-hack.html>
- . 2010. “Mailing Yourself Money to Get Out of Paying Taxes Hack (Doesn’t Work).” *Make:magazine*, April 28. <http://makezine.com/2010/04/28/ mailing-yourself-money-to-get-out-o/>
- Torrone, Phillip. 2006. “Banana Hook Hack.” *Make:magazine*, November. Available at <http://blog.makezine.com/archive/2006/11/banana-hook-hack.html>
- . 2010. “Mailing Yourself Money to Get Out of Paying Taxes Hack (Doesn’t Work).” *Make:magazine*, April 28. <http://makezine.com/2010/04/28/ mailing-yourself-money-to-get-out-o/>
- Turner, F. 2006. *From Cyberculture to Counterculture, Steward Brand, the Whole Earth Catalog and the Rise of Digital Utopianism*. Chicago, IL, and London, UK: University of Chicago Press.



Not all engineers create equally. GÖTZ BACHMANN takes us inside the labs of “radical engineers” and the starkly different futures they imagine for us.





IN A LAB IN OAKLAND a group of engineers are building a “new kind of computer.” It is here, in this lab in Silicon Valley (or in close proximity to Silicon Valley, depending where you draw its boundaries), that I base my ongoing ethnography. The group, clustered around an engineer named Bret Victor, is part of YC Research’s Human Advancement Research Community (HARC), an industry-financed research lab devoted to open and foundational research. “Hacking” is for the members of this group, just as it is for many other engineers, at best a word for tentative work (as in: “This is just a hack”) or for using technologies for other purposes than those originally intended for them. It can also be a derogatory term for not thinking through the consequences of the accumulation of amateurish, low-quality tech development. Thus: when the engineers I research describe their work, “hacking” would not be one of the key terms they would choose. However, I want to make the case that some of their work practices share similarities with hacking, albeit in a different realm. This article asks: How do engineers hack imaginaries of what

technologies are and can be?

I argue this claim by analyzing these engineers as part of a tradition which I call, for lack of a better term, “radical engineering.” Radical engineers fundamentally challenge existing notions of (here, digital media) technologies: their basic features, purposes, and possible futures. Their radicality is not to be confused with political radicality, or the radicality of “disruption”, or the radicality of some of engineering’s outcomes. Theirs is a radicality that puts them outside of assumptions in the wider engineering field of what is obvious, self-evident, time-tested or desirable. Their positions are so heterodox that they often stop calling themselves “engineers.” But no other word can take its place. They might experiment with words like “artist” or “designer in the Horst Rittel way,” but neither stabilizes and both are prone to cause misunderstanding. After all, the people at stake here have their education in disciplines like electrical engineering, mechanical engineering, computer science or mathematics, and their work often comes with the need to tackle highly complex

ABOVE: Illustration (draft) by David Hellman, imagining jointly with Bret Victor’s group “Dynamic Land”, dynamic spatial media’s next iteration in 2017.

technical problems.

Bret Victor’s group tries to build a new computational medium. To get there is less a question of a sudden eureka, but more a permanent and stubborn process of pushing beyond what is thinkable now. The lab takes existing technologies such as projectors, cameras, lasers, whiteboards, computers, and Go stones, and recombines them with new or historic ideas about programming paradigms, system design and information design, as well as a range of assumptions and visions about cognition, communication, sociality, politics and media. The group is constructing a series of operating systems for a spatial dynamic medium, each building on the experiences of building the last one, and each taking roughly two years to build. The current OS is named “Realtalk” and its predecessor was called “Hypercard in the World” (both names pay respect to historical, heterodox programming

environments: Smalltalk in the 1970s and Hypercard in the 1980s). While the group develops such operating systems, it engages in a process of writing and rewriting code, as well as manifestos, lots of talking, even more moments of collective silence, of iterating and tweaking mantras, of digesting films and books, as well as huge amounts of technical papers, and building dozens—indeed hundreds—of hardware and software prototypes.

The lab is filled with prototypes, and new ones are added by the week. In one month, a visitor is able to point a laser at a book in the library, and a projector beams the inside of that book on the wall next to her. A few weeks later you will see people jumping around on the floor, playing “laser socks”: a game where people try to laser each other’s white socks. Months later, a desk becomes a pinball machine made out of light from a projector, and cat videos follow around every rectangle drawn on a piece of paper. Currently, the group experiments with “little languages” in the spatial medium: domain specific programming languages based on paper, pen and scissors, Go stones, or wires, all equipped with dynamic properties, thus having capabilities to directly steer computation or visualize complexity. The point of all such prototypes is not technical sophistication of the glitzy kind. In fact, it is the opposite. The prototypes aim for simplicity and reduction—as a rule of thumb, you can assume that the fewer lines of code involved, and the simpler these lines are, the more the prototype is deemed successful.

In all their playfulness, these prototypes remain “working artefacts” (Suchman et al 2002, 175), forming “traps” for potentialities with “illusions of self-movement” (Jiménez 2014, 391). In the research group of Bret Victor, the work of prototypes is to catch and demonstrate potential properties of a new, spatial, dynamic medium. As one of its desired properties is simplicity, those prototypes that show this property tend to be selected as successful. Furthermore, in the last four years the group has built two operating systems, and aims to keep up this tempo. Each experimental operating system is a prototype, too, albeit a bigger and more complex one. But it is also a purpose-built environment for prototyping applications. And the operating system is based on lessons from past prototyping, including prototyping of both applications and operating systems. These

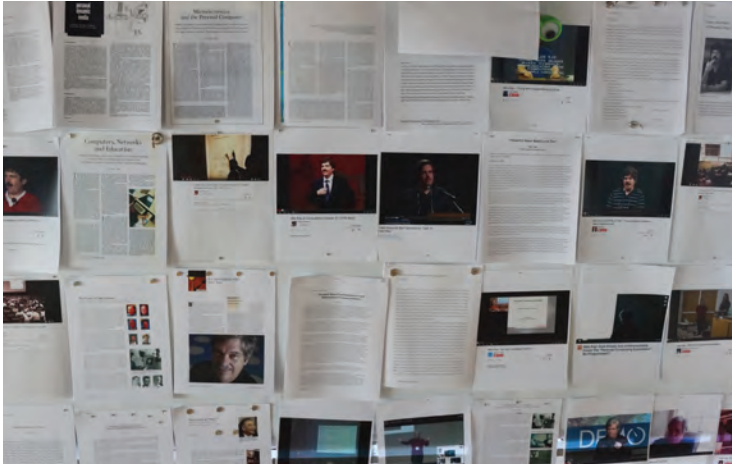
lessons consist of the exploration of desirable, new properties of applications and operating systems. If successful, a new operating system allows building new prototype applications with the desired properties. At the same time, these experiences might point to further desirable properties. This process is then iterated. The overall goal is to create a rupture of a fundamental kind, a jump in technology equivalent to the jump in the 1960s and early 1970s when the quadruple introduction of the microprocessor, the personal computer, the graphical user interface, and the internet revolutionized what computing could be by turning the computer into a medium. Turning computing into media was already in the 1960s and 1970s meant to work with technology against technology: by using new computational capabilities, a medium was carved out that complies less with perceptions at the time of what computing “is,” and more with what a medium that forms a dynamic version of paper could look like. This form of working *with* computing *against* computing is now radicalized in the work of Bret Victor’s research group.

The patron saint for this enterprise, both in spirit and as a real person, is Alan Kay, one of the most famous radical engineers and a key contributor to those ruptures in computing in the 1960s and 1970s that Bret Victor’s group tries to match today. So let’s zoom in on Kay. He started his work in the 1960s at the newly founded Computer Science Department at the University of Utah, writing what surely was one of the boldest doctoral dissertations ever written, a wild technological dream of a new form of computing. A reference to another radical engineer’s cry of despair—“I wish these calculations were executed by steam” (attributed to Charles Babbage and quoted in Kay 1969, III)—stands at its beginning, and after 250 pages of thinking through a “reactive engine,” it culminates in a “handbook” for an imaginary “Flex Machine”: a first iteration of a set of ideas that culminated a few years later in Kay’s vision for a “DynaBook” (1972). While still working on this thesis, Kay became one of the Young Turks in the research community funded by the Pentagon’s Advanced Research Project Agency’s (ARPA) Information Processing Techniques Office (IPTO), which was at that time making its first steps towards building the ARPANET. In the early 1970s, after a quick stint as a postdoc with John McCarthy at Stanford,

Kay joined Bob Taylor’s new Xerox PARC research lab, where engineering legends such as Lampson, Thacker, Metcalfe, and many others, were building the ALTO system, which was the first system of connected standalone machines with advanced graphic abilities.

Once the first iterations of the ALTO/Ethernet system—and it is essential to understand the latter as a system and not as standalone computers—were up and running, they provided Kay with a formidable playground. Kay went back to some of his work in the 1960s, when he had analyzed SIMULA (an obscure Norwegian programming language), and developed this, with Dan Ingalls and Adele Goldberg, among others, into a hybrid between a programming language, an operating system, and a kid’s toy called Smalltalk. The first iterations of Smalltalk were experiments in object orientation that aimed to model all programming from scratch after a distributed system of message passing (Kay 1993): later versions gave up on this, and after an initial phase of success Smalltalk eventually lost the battle over the dominant form of object orientation to the likes of C++ and Java. But in the mid 1970s the ALTO/Ethernet/Smalltalk system became a hotbed for an explosion of ideas about the graphical user interface (GUI) as well as dozens of now common applications. The work of Kay and his “Learning Research Group” can thus be seen as both a lost holy grail of computing before it was spoiled by a model of computing as capitalism cast in hard- and software, but also as one of the crucial genealogical hubs for its later emergence. And it is this double meaning that makes this work so unique and interesting to this day.

Alan Kay’s contributions to the history of computing are results of radical hacks of the computational paradigms and imaginaries of his time. Kay took heretodox programming techniques like the one pioneered by SIMULA, new visualization techniques like the ones developed by the Sutherland brothers, McCarthy cravings for “private computing” (1962:225) and Wes Clark’s lonely machines, the experiments in augmentation by Doug Engelbart’s group, and new ideas about distributed networks, to name a few. Such techniques were not common sense in the emerging professions of software engineering and programming, but had started to circulate in the elite engineering circles where Kay worked. Kay combined them with ideas about pedagogy,



psychology, and mathematics by Maria Montessori, Seymour Papert, and Jerome Bruner, and added further zest in form of the sassy media theoretical speculations of Marshall McLuhan. Kay was also very early in understanding the implications of what Carver Mead called “Moore’s Law,” an exponential line of ever smaller, faster, and cheaper forms of computing kicked off by the mass-produced integrated circuit, and now leading to the positive feedback of technical development and the creation of new markets. So Kay took all of these ideas, desires, technologies, and opportunities, and recombined them. The results were crucial contributions to a new and emerging sociotechnical imaginary, in many ways representing the computer as a digital medium, which we now have today. Kay’s work can thus be seen as a benchmark in radical engineering, as such enabling us to critique the stalemate and possible decline in quality of most currently available imaginaries about technologies.

But is it really that easy? Is radical engineering simply the result of a bit of remixing? Obviously it is a much more complicated process. One of the most convincing descriptions of this process stems from another legendary radical engineer, the aforementioned Doug Engelbart. In 1962, a few years before Alan Kay started his career, Engelbart set the program for his own U.S. Air Force-funded research group at the Stanford Research Institute (Bardini 2000:1-32), aiming for nothing less than to re-engineer the “HLAM-T,” the “Human using Language, Artifacts, Methodology, in which he is Trained” (Engelbart 1962:9). This HLAM-T was always a cyborg, and as such it can be engaged in a continuous

process of “augmenting human intellect.” According to Engelbart, the latter can be achieved through the process of “bootstrapping.” This is a term that can mean many things in the Silicon Valley, from initiating systems to kicking off startups, but in the context of Engelbart’s work, bootstrapping is the “...interesting (recursive) assignment of developing tools and techniques to make it more effective at carrying out its assignment. Its tangible product is a developing augmentation system to provide increased capability for developing and studying augmentation systems” (Engelbart and English 2003:234). Just as Moore’s so-called law, this is a dream of exponential progress emerging out of nonlinear, self-enforcing feedback. How much more Californian can you be?

For Engelbart and English’s description to be more than just a cybernetic pipedream, we need to remind ourselves that they were not only speaking about technical artifacts. Bootstrapping is a larger process in which “tools and techniques” are developing with social structures and local knowledge over longer periods of time. The processes are recursive, much like the “recursive publics” that Chris Kelty (2008:30) describes for the free software development community: in both cases developers create sociotechnical infrastructures with which they can communicate and cooperate, which then spread to other parts of life. Kelty shows how such recursive effects are not simply the magical result of self-enforcing positive feedback. Recursive processes are based on politics. And resources. And qualified personnel. And care. And steering. In short, they need to be continually produced.

ABOVE LEFT: A whiteboard in the lab of Bret Victor’s group filled with papers by Alan Kay.

ABOVE RIGHT: A detail in the HARC Lab: Above, Alan Kay, in white jeans. Below: Engelbart’s 1962 paper, glued on a wall in San Francisco’s Mission district by Bret Victor.

As such, bootstrapping can assume different scopes and directions. Bret Victor and his research group’s form of bootstrapping resembles a multi-layered onion. The kind of people who should be part of it, and at what moments, can lead to intense internal discussion. Once the group launches “Dynamic Land” (see image), it will reach its next stage (to be described in a future paper). Meanwhile, bootstrapping has already taken many forms. Prototypes relate to the process of bootstrapping as pointers, feelers, searchers, riffs, scaffolds, operating systems, jams, representations, imaginary test cases, demos and so on. The interplay of prototype operating systems and prototype applications drives the process forward. Forms of working and cooperation inside the group are evolving, too. There is, indeed, a bestiary of prototyping techniques contained in the larger process of bootstrapping. Together, inside the lab, they produce a feeling of sitting inside a brain. The lab as a whole—its walls, desks, whiteboards, roofs, machines, and the people inhabiting it—functions as a first demo for an alternative medium.

Building the iterations of the series of operating systems can require substantial engineering tasks in the more classical sense; such as, for example, programming a kernel in C, or a process host in Haskell. But the overall endeavor is decidedly not driven by technology. In the spatial medium to come, computing is

supposed to be reduced. Computing is to take the role of an infrastructure: much as books need light, but are not modeled after the light's logic, the medium might draw, where necessary, on the computing possibilities provided by the OS in the background, but it should not be driven by them. Instead, the dynamic spatial medium should be driven by properties of the medium itself, and as such, it should drive technology. The medium's properties are yet to be explored by the very process of bootstrapping it. In the parlance of the group, both the medium and the ways in which they produce this medium, are "from the future." That future is not given, but depends on the medium the group is imagining. It thus depends on the properties of the medium that the group is exploring, selecting, and practicing. On the one hand, technology enables a new medium, which is imagined as shaping the future, on the other hand the future is imagined as shaping the new medium, which then should drive technology.

While most of the group's work consists of building devices, speculative thought is part of their work as well. The latter enables the engineers to understand what the prototyping work unveils. It also gives the lab's work direction, motivates its enterprise, and is part of acquiring funding. The overall process has by now led to a set of interconnected and evolving ideas and goals: One cluster looks, for example, for new ways of representing and understanding complex systems. A second cluster aims for more access to knowledge by undoing contemporary media's restrictions (such as the restriction of the screen, which produces, with its peek-a-boo access to complexity, impenetrable forms of knowledge such as the trillions of lines of code, written on screens and then stared at on screens). A third cluster explores new forms of representing time, and a fourth one more effective inclusion of physical properties into the spatial media system. All these clusters would lead, so the goal and the assumption, to more seamless travels up and down the "ladder of abstraction" (Victor 2011.) As if to echo Nietzsche's, McLuhan's, or Kittler's media theoretical musings with engineering solutions, a larger goal is to make new thoughts possible, which have until now remained "unthinkable" due to contemporary media's inadequacies. Enhanced forms of embodied cognition, and better ways of cooperative generation of ideas could cure

the loneliness and pain that are often part of deep thought. And all of it together might, to quote an internal email, "prevent the world from taking itself apart."

One way to understand what's going on here is to frame all this as an alternative form of "hacking." When you "hack," you might be said to be hacking apart or hacking together. Hacking apart could then be seen as the practices evolving out of the refusal to accept former acts of black boxing. Transferred to radical engineering, hacking apart would translate into not accepting the black boxes of present technological paradigms such as screen-based computers, or ready-made futures such as, say, "Smart Cities, Smart Homes" or the "Internet of Things." Instead you would open such black boxes and dissect them: assumptions about what is deemed as technologically successful and about technological advances to come, matched by certain versions of social order, and often glued together with an unhealthy dose of business opportunity porn. The black boxes will most likely also contain ideas about the roles of the different types of engineers, programmers, designers, managers, and so on. If you take all this apart, you might look at the elements, throw away a lot of them, twist others, add stuff from elsewhere, and grow some on your own. You will look into different, often historical, technological paradigms, other ideas about what will become technologically possible (and when), different ideas of social order, the good life and problems that need addressing, other books to be read, alternative uses of the forces of media, and different ideas about the kind of people and the nature of their professions or non-professions, who should take charge of all this. If you are lucky, you have the conditions and abilities to work all this through in a process also known as bootstrapping, where you go through many iterations of hacking apart and hacking together, all the while creating fundamentally different ideas about what technologies should do, and could do, matched by a succession of devices and practices that help shape these ideas, and "demo" to yourself and others that some utopias might not be out of reach. This is what radical engineers do.

To prevent misunderstanding: neither I, nor the engineers I research, think that the actual future can be hacked together singlehandedly by a bunch of engineers in Palo Alto or Oakland. But I do think that radical engineers such as Engelbart's,

Kay's, or maybe Victor's research groups, in their specific, highly privileged positions, add something crucial to the complex assemblage of forces that move us in the direction of futures. My ongoing fieldwork makes me curious about what is produced here, and many people who visit the lab agree that the first "arrivals" are stunning and mind boggling indeed. If we believe the group's self-perception, their technologies are, just like hacks, tentative interim solutions for something bigger that might arrive one day. The radical engineers would also be the first to state that the same interim solutions, if stopped in their development and reified too early, are potential sources of hacks in the derogatory sense. The latter is, according to their stories, exactly what happened when, 40 years ago, the prototypes left the labs too soon, and entered the world of Apple, IBM, and Microsoft, producing the accumulation of bad decisions that led to a world where people stare at smartphones.

Within such stories, radical engineers might employ a retrospective "could have been," a "Möglichkeitssinn" (sense of possibility, Musil 1930/1990, 14-18) in hindsight, mixed with traces of distinction against "normal" engineers. While they make considerable efforts to evade techno-solutionist fantasies, they don't abandon engineering's approach of addressing problems by building things. Even though they distance themselves from Silicon Valley's entrepreneurial cultures, their isolation against the "Californian ideology" (Barbrook 2007; Barbrook and Cameron 1995) might not always be 100% tight. Indeed, they might

BELOW: Alan Kay in a Japanese manga by Mari Yamazaki.



provide the Silicon Valley mainstream with the fix of heterodoxy it so desperately needs. Yet the same radical engineers are potential allies to those, who aim to hack apart the libertarian, totalitarian and toothless imaginaries that Silicon Valley so often provides us with, be it the “Internet of Shit” or the “crapularity” (Cramer 2016). The conceptual poverty of most of Silicon Valley’s currently available futures surely can become visible from the perspectives of critical theory, from viewpoints of social movements, or through political economy’s analysis. But Silicon Valley’s timidity in thinking,

which is only thinly veiled by the devastation it causes, also becomes apparent, if we compare it to radical engineering’s utopias. ■


GÖTZ BACHMANN is based at Leuphana University, Germany and is currently a Visiting Fellow at Stanford. He is an ethnographer, with former fieldwork among warehouse workers, saleswoman, and cashiers in Germany, and among Japan’s Nico Chuu. He also authors the German children’s comic series KNAX.

BIBLIOGRAPHY

- Barbrook, Richard. 2007. *Imaginary Futures: From Thinking Machines to the Global Village*. London, UK: Pluto.
- Barbrook, Richard, and David Cameron. 1995. “The Californian Ideology.” *Mute* 1(3) (republished in *Proud to be Flesh*, edited by Josephine Berry Slater and Pauline van Mourik Broekman, pp.27–34. London, UK: Mute Publishing)
- Bardini, Thierry. 2000. *Bootstrapping. Douglas Engelbart, Co-evolution and the Origin of Personal Computing*. Stanford, CA: Stanford University Press.
- Cramer, Florian. 2016. “Crapularity Hermeneutics.” http://cramer.pleintekst.nl/essays/crapularity_hermeneutics/
- Engelbart, Doug. 1962. *Augmenting Human Intellect: A Conceptual Framework. Summary Report*. AFO SR 3223. Stanford, CA: Stanford Research Institute.
- Engelbart, Doug, and William English. 2003. “A Research Center for Augmenting Human Intellect.” In *The New Media Reader*, edited by Noah Wardrip-Fruin, pp. 231–246. Cambridge, MA: MIT Press.
- Jiménez, Alberto Corsín. 2014. “Introduction – The Prototype: More than many and less than one.” In *Journal of Cultural Economy* 7(4):381–398
- Kay, Alan C. 1969. “The Reactive Engine.” PhD dissertation, The University of Utah, Salt Lake City.
- . 1972. “A Personal Computer for Children of all Ages.” In *Proceedings of the ACM National Conference, Boston* (typed manuscript, no page numbers)
- . 1993. “The Early History of Smalltalk.” *SIGPLAN Notices* 28(3):69–95.
- Kelty, Chris. 2008. *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.
- McCarthy, John. 1962. “Time-Sharing Computer Systems.” In *Management and the Computer of the Future*, edited by Martin Greenberger, pp. 221–236. Cambridge, MA: MIT Press.
- Musil, Robert. 1930. *Der Mann ohne Eigenschaften* (The Man without Qualities.) Vol. 1. Berlin, Germany: Rowohlt.
- Suchman, Lucy, Randall Trigg, and Jeanette Blomberg. 2002. “Working artefacts: ethnomethods of the prototype.” In *British Journal of Sociology* 53(2):163–179.
- Victor, Bret. 2011. “Up and Down the Ladder of Abstraction. A Systematic Approach to Interactive Visualisation” <http://worrydream.com/LadderOfAbstraction/> accessed 8.2.17.



61 11 2 13
HERBERT E. CLIFF
26 NOTTINGHAM RD.
SHORT HILLS N. J.
RSG 818 20004 135790
1/6/64 2448
RS 818 00004 246882
1/6/64 8774



The term “hacker” is notoriously slippery. **Paula Bialski** dives into the practices and micropolitics of self-proclaimed non-hackers.

I am not a hacker

NOAH, A CORPORATE SOFTWARE DEVELOPER, AND I MET AT

a German language class when we were both living in Hamburg. As the years went by, our friendship flourished through our love for hummus and our mutual interest in tech culture. He graciously fielded my endless tech questions, and was the first techie I ever met who wasn't bored by my ignorance, but rather reveled in my queries about the logics and logistics of computing. When speaking to Noah, I came alive: my mind racing, picking apart the world of our smartphones that we (as regular users) wouldn't normally see when simply looking down at the object sitting in our hands.

Thanks to Noah's stories about where he worked and how he worked, I finally could picture the people behind that screen: their frustrations, the tests they were doing on us, the conversations they were having over one feature or the other. Each button, each little tiny object suddenly had a backstory, even a logic to it. My chat app, whose features once struck me as odd, even arbitrary—a particular swipe capability, specific colors, certain moments of flashing on and off, and other bizarre ways of behaving—finally made some sense. Who made my thumb able to swipe left and not right? When my phone collects my GPS data when I run, where does the data go, and what group of people are making the decision that my data will trigger another feature that allows me to listen to music at the speed of my running pace? Noah made me want to meet those people like him who designed the technologies saturating our daily lives, to talk to them and see what exactly they looked like, what food they ate for lunch, where they were born, and what music they listened to while coding. Through Noah, digital media technology became nonstatic, viscose, constantly shifting like a ball of clay that a group of previously mysterious and magical people were collectively pushing and pulling on, reshaping its size, purpose, and scope.

CORPORATE SOFTWARE DEVELOPERS ARE a rather enigmatic bunch of tech workers, at least when compared with the hacker, who has received far more academic and public scrutiny. Still, these technologists make all

sorts of design choices and decisions that shape the way our practices or certain forms of sociality unfold when using the digital media they create. They also hold “control over a valuable skill” (Ensmenger 2010: 231), meaning at times they—and only they—know what the heck is going on. For example, some developers are the only ones who know what beta version of an app feature is being run at what time on what specific group of users. To their bosses, their managers, their partners and mothers, and all other nondevelopers, the systems they build can even resemble the stuff of magic. After starting fieldwork at Noah's workplace—a large (1000-plus employee) software company I call BerlinTech—I also began to uncover myriad moments when they exerted their “control over a valuable skill.” I became attuned to these moments where developers used their skillful power over those who had less (e.g., their managers), or no skill at all (e.g., the user experience [UX] designers in their team). Their power and skill may seem nothing but hackish, especially in the eyes of nondevelopers who often only know about the world of technology from sensationalistic headlines and increasingly popular TV shows like *Mr. Robot*.

Yet this is where things get tricky: corporate software developers vehemently deny they are hackers. During our conversations, or overhearing their discussions online, in team meetings, or by the coffee machine, developers wanted nothing to do with the label “hacker,” and would shake their heads when asked if they “hacked.”

In the words of Sam, one of the coders I worked with, most corporate software developers associate the term “hacker” to two specific behaviors: “(1) Anarchist activism against oppressing institutions in order to regain in a way a certain flavor of human liberty; (2) direct work with security systems...either trying to break or to protect.” (Sam, BerlinTech developer, December 2016).

Sam explained that the word “hack” is merely used for “dirty coding, in order to conceptualize and create quick solutions” (field notes, December 2016), and other developers, during my conversations with them at work, linked the “hacker” with criminal activity.

Here I present an apparent paradox, common to ethnographers, through a tongue-and-cheek retelling of three stories from my field: what your respondents tell you often fails to match their actions and behavior. When asked if a software developer is a hacker, or identifies with being a hacker, they will quite often say “No.” Yet after months of observation, many of their actions resemble those we commonly attribute to the hacker. As we have seen in many other ethnographies of hacker communities, hacking is about experimentation, political gestures, and craftiness (Coleman 2013, 2014). Software developers are no exception. Sometimes the only difference lies in their verbal disavowal of this identity or, if pressed, they may admit to some limited resemblance: at most, they may frame their activities as a species of micro-hacking, intended for their own personal use, or only for their employer.

CONTROL OF A VALUABLE SKILL

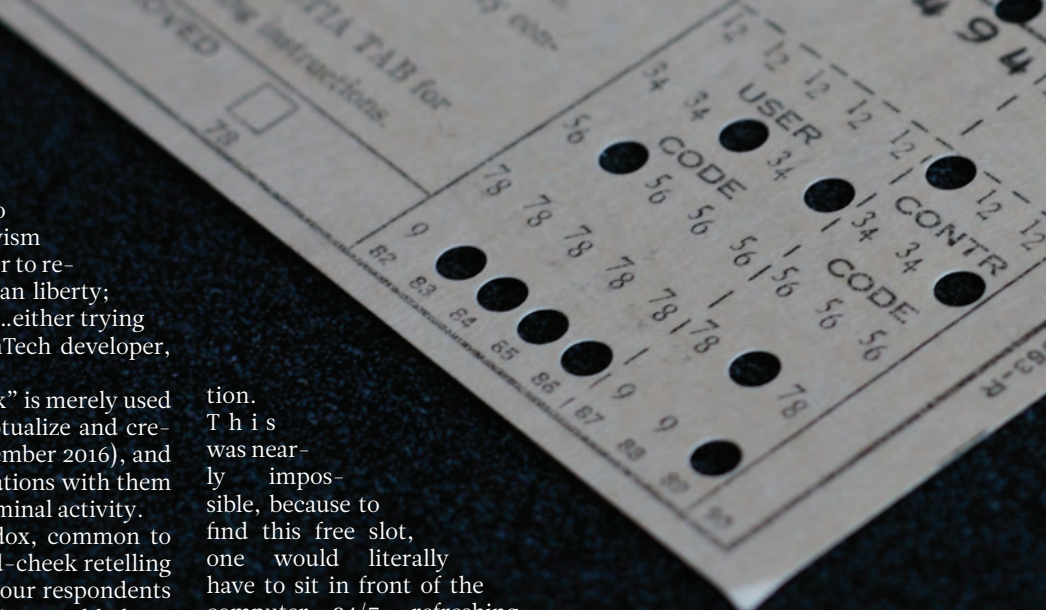
With this in mind, I rewind a few months back to a moment before I started my ethnography at BerlinTech. Noah and I were sitting together on the grass, enjoying the heat of July. Noah started mid-sentence as if he opened his head for me to see what was mulling through his brain: “I really doubted what you said last week. I doubted that programmers are really superstars, the new and powerful class of worker. I wasn’t so sure.” I nodded, listening, returning to the moment that Noah questioned my thesis that all programmers—not only the geniuses and those deemed “superhackers”—command more power not only for building technologies but maneuvering and outmaneuvering these systems. But then Noah offered a recent revelation: after years of having one foot in Tel Aviv and one foot in Berlin, Noah decided to really move to Berlin, register himself as a resident, gain a German driver’s license, and start taking intense German courses. To do so, he would have to register himself in the *Stadtamt* (city office), infamous for its very annoyingly snail-slow bureaucracy. The city of Berlin offers an online sign-up system for appointments, yet the downside is that the system has a three-month-long waiting list. The previous week, Noah explained, he had logged onto the Berlin city hall website, and managed to get an appointment for late August (which, being early July, was already pretty awesome). The only way to land an earlier spot is through a cancella-

tion.

This was nearly impossible, because to find this free slot, one would literally have to sit in front of the computer 24/7, refreshing the page and checking for cancellations. Frustrated, Noah coded a script that automatically scanned for cancellations in the city hall’s appointment schedule. “So, Paula, in this moment I realized that we are sort of a new upper class. Not in a big way, but in all the little tiny ways like being able to create a script that helps you make a driver’s license appointment, or making a script to help with booking a cheap train ticket. There are all sorts of little everyday examples that help us get in the backdoor of all sorts of systems that run our lives.” This skill is obviously shared by hackers (for example, in their “craftiness” to break through various systems), yet the difference among software developers like Noah is that they do not use the common vocabulary to frame this activity like hackers do.

In my months at BerlinTech, I encountered numerous other examples of developers who built apps for their own personal enjoyment and needs (without ever “releasing” the app for general public use) or, in the case of Noah, building a program that would help circumvent the limitations of a given system like a city infrastructure or customize the infrastructure they were being paid to build without the knowledge of their employers or managers. Although I don’t want to paint every developer as always able to enter the backdoors of every system, the developers I encountered explained these practices with such ease, as if building or breaching was part of their being in the world. It struck me as something similar to how the well traveled explain navigating through an airport, or how a marathon runner effortlessly describes the 15-kilometer run they just completed. This effortlessness or ease of building a new digital tool, customizing an existent piece of infrastructure, or breaching a seemingly closed system was part of the life of being a developer in an increasingly digital society.

If this “control over a valuable skill” can help exert a certain power over an infrastructure, or an organizational system, then why this perceived paradox? Why are software developers not “hackers”?





1 “I’M NOT A HACKER BECAUSE WHAT I BUILD IS DONE FOR FUN”

“Creating apps [in one’s] free time is like having a Lego in your computer,” remarked Sam during an online conversation. Software development, he insisted, is about building, about creativity, about craftiness, and about playfulness. Whereas hackers break or build as a means to get to a specific ends (we “break” *something* to get *into* “somewhere”), software developers claim that they create just to make something, without a specific desired outcome of “breaking down” or “breaking in.” The irony of this approach is that both interacting with a computer in an exploratory way, as well as building something to produce exactly what is needed, are both definitions of hacks, but not seen as such in the eyes of these developers (see <http://catb.org/jargon/html/H/hack.html>).

Sam said that indeed, they do “gain power” with the competences to manipulate a certain technical system, but they do so:

...to regain a space for creativity. In the end, it’s our space, we do it in our free time, and by doing that we are not affecting the processes, or the institutions, just our status with ourselves” (Sam, BerlinTech, December 2016).

According to Sam, personal pet projects don’t mix well with the heady and serious world of protest and politics. Protest must be seen and heard, and what he builds for “fun” or “to be creative” is often invisible, for his eyes only: “Creating an app at home during my free time is as political as silently protesting on a Sunday afternoon on the streets.” In silence, in hiding, Sam can create for fun. Hackers, on the other hand, are not silent. Hackers create for something, to achieve a certain end.

2 “I’M NOT A HACKER BECAUSE MY POLITICS ARE TOO ‘NANO-SCALE’ TO BE NOTICED”

Sam and a few of his colleagues made their own feature for the app they were building for their company. Their product managers didn’t commission this feature, nor was their company ever going to use it. Yet when they finished what they were doing for work, they would (sometimes during office hours) breach their work system, subvert their bosses, and go behind their backs and built it anyway. They’d do so in their free time, when their bosses weren’t looking. While this gesture has everything resembling a hack, breach, or skillful subversive act done to regain a certain sense of power, Sam and his friends did not perceive it that way: “It’s really nano-political,” Sam explained.

We try to transcend either the process or the product. But that rarely happens.... [T]he culture is very heavily impacted by the hierarchical organisational structure.... [S]ometimes you try to bring those ideas to the normal working environment, which often acts as a bouncing wall [at least in this company, at the moment].... You throw ideas, but often those ideas bounce back to you, with no way to impact the structures or the culture.

These “nano-political” moments of breaching are attempts to regain power (or is *agency* the better word?), but they are humble, and done in a smaller scope. Sam explained that these acts couldn’t be seen as true hacking because they “barely impact their work processes,” let alone a larger scale. Hackers, on the other hand, act big. Hackers hack on a large scale.

3 “I’M NOT A HACKER, I’M JUST EXPERIMENTING”

Software developers would sometimes hack, breach, and break systems “by mistake” or during the process of learning. The software developers at BerlinTech, much like many tech companies, were encouraged by their managers to experiment. As one manager explained, it is their “responsibility” to allow their software developers to experiment during hack-a-thons, team-coding sessions, and “research weeks.” During these sessions and others, “you experiment, you learn, and based on this, you bring ideas to your environments,” explained Sam. Yet Sam reiterated that his technical “experimentation” is *not* hacking. These experiments might involve breaking certain systems or breaching territory that is not generally intended for that specific use (mainly a system within one’s own company). What differentiates this from “true hacking” is that a company like BerlinTech can capitalize on whatever arises out of this experimentation, “bringing your ideas back into your environment.” Developers perceive that what they are doing is just experimenting to directly benefit the output of their company. Real hackers just hack, without a third party intending to capitalize on what they are doing.

SOME CONCLUSIONS

As ethnographies of corporations (e.g., Wittel 1997) or the working class (Bachmann 2014; Kracauer [1930]1998) have shown, the seemingly mundane, everyday practices of work—whether those of a software developer or clerical manager—are also about power, construction, destruction, dreams, fears, and foes. The ability for a developer to secretly create a feature, or cleverly bypass/route around government bureaucracy, can be political without being an “epiphenomenon, or a manifestation or instrument of grander movements” that affect a larger society or group (Burns 1961:264). The developer’s persistent efforts to improve their chances, or use of their skills in protesting the way in which an institution functions, can be seen, as sociologist Tom Burns explained more than 50 years ago, as “micropolitical” (Burns 1961): where physical and human resources present in institutions, corporations, or organizations “accumulate and then widen and alter the possibilities of political action” (Burns 1961:281). If the managing director or product owner is the central source of visible power, the software developer’s invisible power lies in acting in hidden ways, behind their field of knowledge. This is how they gain a sense of agency and power, which can become political. Today, with the protest, scandal, and criminality circling around the term “hacker,” developers perhaps have attempted to distance themselves from the term

when speaking to me (their ethnographer), much like the Certified Ethical Hacker attempts to destigmatize their own practice by disassociating themselves with the “political hacker,” as Rebecca Slayton describes in this issue.

Not all corporate software developers are powerful technological agents. Many also work with constraints and even through states of ignorance (because developers often don’t know what’s going on within the software system they are working on). Moreover, more than ever, automation and artificial intelligence makes their “power” in some ways obsolete. Still, software developers do enact agency and power with their skills and capacities; their actions, however small they may seem to be, are neither mundane nor inconsequential. Understanding the technologist’s “agency” and the micropolitics of software development can help us understand the various shapes and forms “hacking” takes on, as well as the weapons, skill, and control that is intrinsic to the culture of software development. ■

PAULA BIALSKI is a postdoctoral researcher at Leuphana University’s Digital Cultures Research Lab (DCRL), where she bides her time pestering students in the Digital Media BA program and conducting an organizational ethnography of a corporate tech company in Berlin.

BIBLIOGRAPHY

- Bachmann, G. (2014). *Kollegialität: Eine Ethnografie der Belegschaftskultur im Kaufhaus*. (Collegiality: An ethnography of employee culture in a department store). Frankfurt, Germany: Campus Verlag.
- Burns, T. (1961). “Micropolitics: Mechanisms of Institutional Change.” *Administrative Science Quarterly*. Vol. 6. No. 3. 257–281.
- Coleman, E. Gabriella. (2013). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.
- . (2014). *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London, UK: Verso Books.
- Ensmenger, N. L. (2010). *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise*. Cambridge, MA: MIT Press.
- Kracauer, S. (1998). *The Salaried Masses: Duty and Distraction in Weimar Germany*. Originally published 1930. London, UK: Verso Books.
- Wittel, A. (1997). *Belegschaftskultur im Schatten der Firmenideologie. Eine ethnographische Studie*. (trans: Employee culture under the shadows of company ideology: An ethnographic study) Berlin: Stigma.



Interview: Kim Zetter

Cybersecurity journalist **Kim Zetter** talks with *Limn* about infrastructure hacking, the DNC hacks, the work of reporting on hackers and much more.

Christopher Kelty: So our first question is: What kind of technical or political thresholds have we crossed, and have you seen, in your time reporting on hacking and information security? Is Stuxnet [2010] a case of such a threshold, or the DNC [Democratic National Committee] hack? Since you've been doing this for a long time, maybe you have a particular sense of what's changed, and when, over the last, say, decade or so?

Kim Zetter: I think we have a number of thresholds in the last decade. And the DNC hack definitely is a threshold of a sort. But it's not an unexpected threshold. There's been a build up to that kind of activity for a while. I think what's surprising about that is really how long it took for something like that to occur. Stuxnet is a different kind of threshold, obviously, in the military realm. It's a threshold not only in terms of having a proof-of-concept of code that can cause physical destruction—which is something we hadn't seen before—but also it marks a threshold in international relations because it opens the way for other countries to view this as a viable option for responding to disputes instead of going the old routes: through the UN or attacking the other nation, or sanctions or something like that. This is a very attractive alternative because it allows you to do something immediately and have an immediate effect, and also to do it with a plausible deniability because of the anonymity and attribution issues.

CK: Why do you say this is long overdue?

KZ: With regard to the DNC hack, we've seen espionage and political espionage is not something new. The only thing that's new here is the leaking of the data that was stolen rather than, let's say, the covert usage of it. Obviously, the CIA has been involved in influencing elections for a long time, and other intelligence agencies have as well. But it's new to do it in this very public way, and through a hack, where it's almost very transparent. You know, when the CIA is influencing an election, it's a covert operation—you don't see their hand behind it—or at least that's what a covert operation is supposed to be. You don't know who did it. And in this way, [the DNC hack] was just so bold.

But we've seen sort of a step and progression of this in the hacking world. We saw when Anonymous hacked HBGary [2011] and leaked email spools there. We saw the Sony hack [2014] where they leaked email spools. And both of these put private businesses on notice that this was a new danger to executives. And then we saw the Panama Papers leak [2016], where it became a threat to wealthy individuals and governments trying to launder or hide money. And now that practice has moved into a different realm. So that's why I'm saying that this is long overdue in the political realm, and we're going to see a lot more of it now. And the DNC hack

is a bit like Stuxnet in that it opens the floodgates—it puts a stamp of approval on this kind of activity for nations.

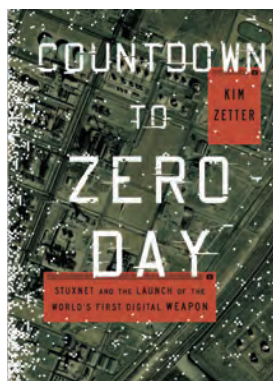
CK: This is at the heart what I think a lot of people in the issue are trying to address. It seems that the nexus between hacking as a technical and practical activity and the political status of the leaks, the attacks, etc., is somehow inverting, so there's a really interesting moment where hacking moved from being something fun...[with] occasionally political consequences to something political...[with] fun as a side effect.

KZ: Right. I've been covering security and hacking since 1999. And we started off with the initial hacks; things like the "I Love You" virus, things...that were sort of experimental, that weren't necessarily intentional in nature. People just...testing the boundaries of this realm: the cyber realm. And then e-commerce took off after 2000 and it became the interest of criminals because there was a monetary gain to it. And then we had the progression to state-sponsored espionage—instead of doing espionage in the old ways with a lot of resources, covert operatives, physical access, things like that. This opened a whole new realm; now we have remote destructive capabilities.

CK: So, let me ask a related question: in a case like the DNC hack, do we know that this wasn't a case of someone who had hacked the emails and then found someone, found the right person to give them to, or who was contracted to do the hacking?

KZ: Yes. I think that's a question that we may not get an answer to, but I think that...you're referring to something that we call "hybrid attacks." There are two scenarios here. One is that some opportunistic hacker is just trying to get into any random system, finds a system that's valuable, and then decides to go find a buyer, someone who's interested in [what was obtained]. And then the stuff gets leaked in that manner. If that were the case in DNC, though, there probably would have been some kind of exchange for money, because a hacker—a mercenary hacker like that—is not going to do that for free.

But then you have this other scenario, where you have what I'm referring to now as hybrid attacks. We saw something similar in the hack of the Ukraine power grid [2015–2016], where forensic investigators saw very distinct differences between the initial stages of the hack, and the later stages of the hack which were more sophisticated. The initial hack, which was done through a phishing attack in the same way [as the DNC was hacked], got them into a system and they did some reconnaissance and they discovered what they had. And then it looks like they handed the access off to more sophisticated actors who actually understood the industrial control systems that were controlling the electrical grid.



Kim Zetter is the author of the definitive book on the StuxNet virus, *Countdown to Zero Day* (Broadway Books, 2015).

And they created sophisticated code that was designed to overwrite the firmware on the grid and shut it off and prevent them from turning it back on.

So there is a hybrid organization where front groups are doing the initial legwork; they aren't necessarily fully employed by a government or military, but are certainly rewarded for it when they get access to a good system. And then the big guys come in and take over.

When you look at the hack of the DNC and the literature around it—the reporting around it—they describe two different groups in that network. They describe an initial group that got in around late summer, early fall, around 2015. One group gets in and then the second group comes in around March 2016. And that's the group that ultimately leaked the emails. It's unclear if that was a cooperative relationship or completely separate. But I think we're going to have this problem more and more, where you have either a hybrid of groups cooperating, or problems with multiple groups independently being in a system. And this is because there are only so many targets that are really high-value targets, who could be of interest to a lot of different kinds of groups.

CK: What I find interesting about hacking are some of the parallels to how we've dealt with preparedness over the last couple of decades, independent of the information security realm. You know, thinking about very unlikely events and needing to be prepared, whether that's climate change-related weather events or emerging diseases. Some of the work that we've done in Limn prior to this has been focused on the way those very rare events have been restructuring our capacity to respond and prepare for things. Is there something similar happening now with hacking, and with events—basically starting with Stuxnet—where federal agencies but also law enforcement are reorienting around the rare events? Do you see that happening?

KZ: I suppose that's what government is best at, right? Those big events that supposedly we can't tackle ourselves. So I think it's appropriate if the government focuses on the infrastructure issues. And I don't mean just the critical infrastructure issues like the power grid and chemical plants, but the infrastructure issues around the internet. I don't think that we should give it over entirely to them. But in some cases, they are the only ones that actually can have an influence. One example is the FDA [U.S. Food and Drug Administration], and its recent rules around securing medical devices for manufacturers and vendors who create medical devices. It's so remarkable to think that there was never a security requirement for our medical devices, right? It's only in the last year that they thought it appropriate to actually even look at security. But it shouldn't be a surprise because we had the same thing with electronic voting machines.

CK: Yeah, it's a shock and laughter moment, it seems to repeat itself. Switching gears a little bit: one of the questions we have for you has to do with your experience in journalism, doing this kind of work. Do you see interesting new challenges that are emerging, issues of finding sources, verifying claims, getting in touch with people? What are some of the major challenges you've encountered as a journalist trying to do this work over the last couple of decades?

KZ: I think that one of the problems that's always existed [in] reporting [about] hackers is that unlike most other sources they're oftentimes anonymous. And so you are left as a journalist to take the word of a hacker, what they say about themselves. You obviously put things in context in the story, and you say, "According to the hacker," or "He is a 20-year-old student," or "He's based in Brazil." There's not a lot of ways you can verify who you're talking to. And you also have the same kind of difficulties in verifying their information. Someone tells you they hacked a corporation and you ask, "Can you give me screenshots to show that you have access inside this network?" Well, they can doctor screenshots. What else can they give you to verify? Can they give you passwords that they used, can they tell you more about the network and how they got in? Can they give you a sample of the data that they stole? And then of course you have to go out and verify that. Well, the victim in many cases is often not going to verify that for you. They're going to deny that they were hacked; they're going to deny that they had security problems that allowed someone in. They may even deny that the data that came from them is their data. We saw that with parts of the DNC hack. And it was true that some of the data hadn't come from them. It had come from someone else.

CK: Do you find that—do you think that—finding sources to tell you about this stuff is different for studying hacking than for other domains? Do you basically go back to the same sources over and over again once you develop a list of good people, or do you have to find new ones with every event?

KZ: In terms of getting comments from researchers, those are the kinds of sources I would go back to repeatedly. When you're talking about a hacker, of course, you can only generally talk with them about the hacks that they claimed to have participated in. And then of course they can just disappear, like the Shadow Brokers. After that initial release and flurry of publicity, several journalists contacted the Shadow Brokers, got some interviews, and then the Shadow Brokers disappeared and stopped giving interviews. So that's always the problem here. Your source can get arrested and disappear that way, or willfully disappear in other ways. You may only end up having part of the information that you need.

CK: We have a number of articles about the difficulty of interpreting hacks and leaks and the expectation that the content of the leaks will have an immediate and incontrovertible effect—Pentagon Papers-style, or even Snowden-style. A leak that will be channeled through the media and have an effect on the government. We seem to be seeing a change in that strategic use of leaks. Do you see that in your own experience here too? That the effectiveness of these leaks is changing now?

KZ: You know, I think we're still working that out. We're trying to figure out the most effective way of doing this. You have the WikiLeaks model that gets thousands of documents from Chelsea Manning, and then just dumps them online and is angry that no one is willing to sift through them to figure out the significance of them. And then you have the model, like the Snowden leak, where they were given in bulk to journalists, and then journalists sifted through them to try

and find documents and create stories around them. But in that case, many of the documents were still published. Then we have the alternative, which is the Panama Papers, where the data is given to journalists, but the documents don't get published. All we see are the stories around them. And so we're left to determine from the journalists: Did they interpret them correctly? Do they really say what they think they say?

We saw that problem with the Snowden documents. In the initial story that the Washington Post published about the Prism program, they said that, based on their interpretation of the documents, the NSA [National Security Agency] had a direct pipeline into the servers of these companies. And they misinterpreted that. But because they made the documents available it was easy for the public to see it themselves and say, "I think you need to go back and re-look at this." With the Panama Papers we don't have that. So there are multiple models happening here, and it's unclear which is the most effective. Also, with the DNC, we got a giant dump of emails, and everyone was sifting through them simultaneously. The same with the Ashley Madison emails: everyone was trying to find something significant. There is sort of the fatigue factor: if you do multiple stories in a week, or even two weeks, people stop reading them because it feels like another story exactly like the last one.

And that's the problem with large leaks. On the one hand you expect that they're going to have big impact; on the other hand, the reading public can only absorb or care about so many at a time, especially when so many other things are going on.

CK: The DNC hacks also seem to have a differential effect: there was the sort of Times and Post readers who may be fatigued hearing about it and who fell away quickly. But then there's the conspiracy theory-Breitbart world of trying to make something out of the risotto recipes and spirit cooking. And it almost feels like the hack was not a hack of the DNC, but a hack of the media and journalism system in a way.

KZ: Yeah, it was definitely manipulation of the media, but only in the sense that they knew what media would be interested in, right? You're not going to dump the risotto recipes on the media (although the media would probably start up with that just a bit, just for the humor of it). But they definitely know what journalists like and want. And I don't think that journalists should apologize for being interested in publishing stories that could expose bad behavior on the part of politicians. That exists whether or not you have leaked emails. That's what leaking is about. And especially in a campaign. There's always manipulation of the media; government-authorized leaks are manipulation of the media as well.

CK: I think I like that connection, because what's so puzzling to me is to call the DNC hacks "manipulating the presidential election" suggests that we haven't ever manipulated the presidential election through the media before, which would be absurd, [Laughter.] So there's a sort of irony to the fact that we now recognize it as something that involves statecraft in a different way.

KZ: And also that it was from an outsider: I mean, usually it's the opposite party that's manipulating the media to affect the

outcome. I think they're all insulted that an outside party was much more effective at it than any of them were. [Laughter.]

CK: Okay, one last question. What's happening to hacker talent these days? Who's being recruited? Do you have a sense in talking to people that the sort of professional landscape for hackers, information security professionals, etc., has been changing a lot? And if so, where are people going? And what are they becoming?

KZ: The U.S. government has been recruiting hackers from hacker conferences since hacker conferences began. From the very first DEFCON, undercover FBI and military were attending the conferences not only to learn what the hackers were learning about, but also to find talent. The problem of course is that as the cybersecurity industry grew, it became harder and harder for the government and the military to hold onto the talent that they had. And that's not going to change. They're not going to be able to pay the salaries that the private industry can pay. So what you see, of course, is the NSA contracting with private companies to provide the skills that they would have gotten if they could have hired those same people.

So what's always going to be a problem is that the government is not always going to get the most talented [people]. They may get them for the first year, or couple of years. But beyond that, they're always going to lose to the commercial industry. Was that your question? I'm not sure if I answered it.

CK: Well, it was, but I'm also interested in what kinds of international recruitment, what shake-up in the security agencies is happening around trying to find talent for this stuff? I know that the NSA going to DEFCON goes all the way back, but now even if you're a hacker and you're recruited by NSA, you may also be recruited by other either state agencies or private security firms who are engaged in something new.

KZ: Right. In the wake of the Snowden leaks, there may be people who would have been...willing to work for the government before who aren't willing to work there now. And certainly Trump is not going to help the government and military recruit talents in the way that past administrations might have been able to appeal to patriotism and, you know, national duty. I think that that's going to become much more difficult for the government under this administration.

KIM ZETTER *is an award-winning, senior staff reporter at Wired covering cybercrime, privacy, and security. She is the author of Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.*

Interview conducted February 2017.

THIS HAS BEEN AN UNAUTHORIZED CYBERNETIC ANNOUNCEMENT

Start with an archetypal story: a single brave hacker with phenomenal technical chops liberates the suppressed information, and with it society as a whole. “More bits are being added automatically as it works its way to places I never dared guess existed,” says the hacker of his epic exfiltration program (Brunner 1995:251). “In other words, *there are no more secrets.*” He will bring down every rotten institution, expose every lie, open government to the governed. “As of today, whatever you want to know, provided it’s in the data-net, you can now know.” (Brunner 1995:248) He will launch the leak to end all leaks, one that will not only overturn but replace the government itself.

All this is from John Brunner’s 1975 science fiction novel *The Shockwave Rider*. Set in the early 21st century, the book imagines a state-corporate surveillance and identity-management system and a hopelessly distracted and media-saturated population of flexible tech and service industry workers unable to think about anything in the long term. These days, it barely qualifies as fiction; it’s a lot more prescient than anything involving a lunar base. His protagonist—intelligent, brilliant, but also isolated and consumed by an identity crisis and suicidal impulses—makes him instantly recognizable as drawn from real-life figures like Len Sassaman (a privacy advocate and systems engineer who tragically committed suicide in 2011) and fictional representations like Elliot Alderson, the anxiety-afflicted main character in the TV hacker drama *Mr. Robot*. Even the liberating hack Brunner postulates is not too improbable in the centralized data apparatus he envisions: later computer scientists adopted his term for “worm programs”—or just worms—incorporating networked machines into a larger distributed computation (Shoch and Hupp 1982). There is one glaring fantasy element in this story, though, one giant fire-breathing dragon on what could otherwise pass as the 21st-century city skyline: the leak happens *after* the leak.

First, the data that are found and distributed are clear and unambiguous. Here, there are no fundraising dinners that may or may not correspond to political influence, no unethical behavior that would need witness testimony to corroborate, no fog of war. The data are a picture of evil. Second, and far more improbable than the mega-hack itself, all the data are delivered by the worm program in plain, polemical English, linked to the outrage in question (the protagonist’s program has also infiltrated all publishing tools): a corporate report comes with documentation of fraud, canned food is labeled with all the dangers to health it contains, a cosmetic product is accompanied by its known carcinogens and a history of legal cover-ups. “This is a cybernetic datum derived from records not intended for publication,” the notes say. “This has been

an unauthorized cybernetic announcement.” (Brunner 1995:245) If you ask the worm system about a politician or a scandal, it returns a cogent summary of precise and documented malfeasance in the style of an investigative journalist. Finally, this leak to end all leaks provokes the population to rational and exactly targeted outrage. Everyone investigates and discusses and sorts through the worm’s data and dismantles the existing society. In its place, using hidden economic data found by the worm, they build a kind of cybernetic communism, ruled by distributive algorithms and total informational transparency: “Therefore none shall henceforth gain illicit advantage by reason of the fact that we together know more than one of us can know.” (Brunner 1995:280)

Of course actual leaks don’t play out like this. Even the Pentagon Papers, which would seem like a model for *The Shockwave Rider*, required an enormous amount of informational labor to organize, shape, and explain, both by Ellsberg and by Woodward and Bernstein (Ellsberg 2003). Gigabytes of data taken from enterprise resource planning software do not return one-click results of “fraud” or “not fraud.” (Forensic accounting is a multiregional career for a reason.) The WikiLeaks “Collateral Murder” video was exceptional precisely because it was an unambiguous video of a battlefield killing, and even that was edited and framed with text. The most recent WikiLeaks releases, as of this writing, seem heavily redacted and organized to put the Clinton campaign in the worst possible light. (Pick some choice investigative out of thousands of messages, set it in Courier typewriter font so it looks more “official,” highlight a couple random passages, and you too can stun the world with your revelations.) The Guardians of Peace hack, which released material from Sony Pictures Entertainment, turned up a few things seeming to demand public action (lobbying efforts to coerce internet service providers [ISPs] into blocking sites and traffic) but mostly offered a salacious opportunity to read the correspondence of executives being awful to each other on their iPads. It also exposed the data of thousands of innocent people. If we count doxes (the public release of identifying information for online identities) as leaks, then the work of leaking has grown to encompass the lazy man’s death threat: to reveal all the information about someone you dislike, and wait for someone else to call in a fake active shooter and incite a SWAT team raid.

Somewhere along the line, between the 1975 science fiction vision and the realization in the 2010s, a threshold was crossed. Hacking, leaking, and the fantasy of the effects of secret knowledge have taken on a very different cast. I think there are two related components to

this change, a cause and a consequence: the volume of data, and the space of available interpretations. (These two components share an interesting symmetry with Gorham’s argument about *episteme* and *doxa*—truth and opinion—and the consequence includes the distinct forms of slow and fast leaks described by Adam Fish, both in this issue of *Limn*.) Broadcast media technology gave us the fantasy of the single decisive leak—“Lonesome” Rhodes unwittingly insulting his public in *A Face in the Crowd* on a hot mic, or newspapers breaking the mistress story in *Citizen Kane*—but Podesta-size, Cablegate-size leaks (hundreds of thousands of messages, millions of user accounts) work differently. They speak to the corresponding media fantasy of our time, the daydream of big data: information at the gigabyte scale, millions of rows or nodes, will provide a new insight, unavailable by other means—a social graph of call metadata and CC’d messages exposing a conspiracy, or dissimulation revealed in keyword analysis across an industry.

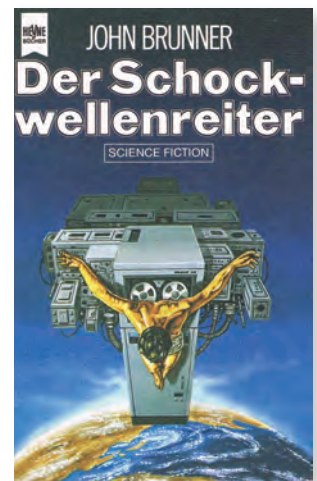
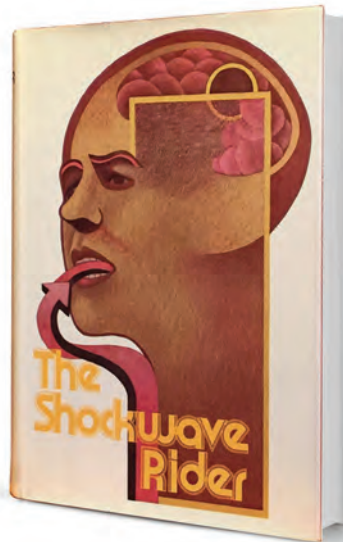
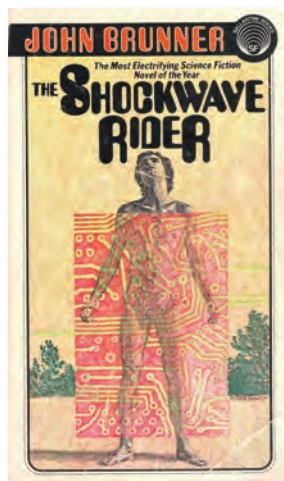
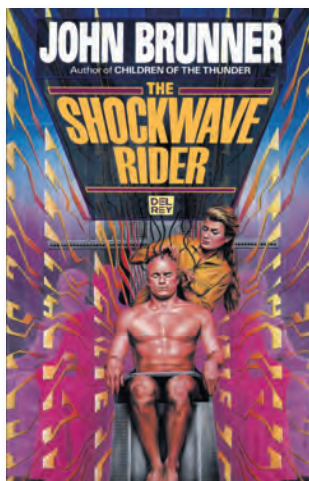
In practice, though, the increase in quantity by orders

there was a group who deserved no privacy, with a comically evil company, a lie to be exposed, and a righteous cause where the mega-leak’s information could speak for itself?

I HAVE A COPY IF YOU DON’T PAY

Avid Life Media was a Toronto-based “leading business in the online dating industry.”¹ (Since the events described here, they’ve rebranded as the lowercase “ruby Corp.”) They ran a slate of remarkably sleazy dating/hookup sites, including Established Men, Cougar Life, Man Crunch (really), and Ashley Madison. This last promised easy and straightforward extramarital affairs, thriving on its scandalous publicity with slogans like “Life is short. Have an affair.”

In fact, the Ashley Madison business model was a 21st-century version of the early pornographic film loops studied by the cinema scholar Linda Williams. She explained that you don’t see representations of orgasm in most of these early porno films because they were screened



"NONE SHALL HENCEFORTH GAIN ILLICIT ADVANTAGE BY REASON OF THE FACT THAT WE TOGETHER KNOW MORE THAN ONE OF US CAN KNOW."

of magnitude—combined with immediate and widespread distribution—has not made for *bigger* truths. Instead, it has enabled *more* truths...or “truths.” It has expanded the space of available interpretations, analysis, and consequences, from journalistic exposés of internal party discipline advancing Clinton’s candidacy, to a troll-fueled, gun-toting showdown at a pizza place in Washington, DC. To substantiate this argument for the importance of volume and interpretation, I want to challenge it: What if there was one paradigmatic hack-and-leak case where the *Shockwave Rider* fantasy could really work? What if

nickelodeon-style in brothels to arouse the patrons but not satisfy them, so they’d pay for services (Williams 1989:74). They were tantalizing frustration machines. Likewise Ashley Madison: setting up an account was free, but sending messages, giving “virtual gifts” (the usual social network chintz), and initiating instant message sessions all cost “credits,” which users could buy in blocks from \$49 to \$249 (which came with an “affair guarantee”). In other words, it was bad for the company’s income for users to proceed swiftly to an in-person affair. The optimal arrangement was a closed loop of back-and-forth

1 See their original LinkedIn page—neither deleted nor edited, bafflingly—at <https://www.linkedin.com/company/avid-life-media>.

messaging and flirting that never went anywhere. Luckily for Avid Life Media, Ashley Madison’s userbase included almost no actual women; the company used chatbots instead to sustain endless routines of ELIZA-like flirting with men.²

This marvelously depressing but lucrative strategy, where the creepiness of RealDoll porn-chat bots meets the repetitive, inescapable time of *Last Year at Marienbad*, had a final sting. The frustration machine produced a lot of records: profiles, sexual preferences and fantasies, photos, and messaging and chat transcripts, all linked to a credit card and a single identity. When the customer eventually felt guilt and regret, or fear of discovery, they would shut down their account and be obligated to take advantage of the “Full Delete” option—for only \$19—which would entirely delete every record of their activity on Ashley Madison.

Avid Media did not fulfill their end of this final sale. The technical challenges involved in completely removing records like this are considerable, especially on a social network (of sorts) that accepted credit card payments. The Ashley Madison team didn’t bother, instead settling for the appearance of deleted accounts. The user would receive a confirmation message that alluded obliquely to this, stating that the profile “has been successfully permanently hidden from our system”: a run of imprecise weasel words that didn’t add up to the total data destruction one had been led to expect. Nineteen dollars to set “AccountHidden=” to “TRUE” for everyone who ever got drunk in a hotel room, started a free account in a moment of weakness, and regretted it the next day was a fantastic way to make money.

On July 19, 2015, Ashley Madison’s website and internal network displayed a new landing page. Their banner had been the lower half of a woman’s face with her finger to her lips: *shhhh* (with a wedding band, naturally). The new page completed the upper half of the banner with the gory exploding head from David Cronenberg’s vengeful-teleshop movie *Scanners*, and a demand: “AM AND EM MUST SHUT DOWN IMMEDIATELY PERMANENTLY.” (EM, Established Men, was Avid Life’s “sugar daddy” network, here identified as a “prostitution/human trafficking website.”) “We are the Impact Team. We have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails,” the page began. They were holding Avid Life hostage, demanding not money but the shutdown of the two sites. Their objections against Ashley Madison were based on the failure to deliver on the “Full Delete” promise: “[Avid Life Media] management is bullshit and has made millions of dollars from complete 100% fraud.” But the Impact Team’s strategy was not to release information about the company itself. It was to leak information about the *users*: “We will release all

customer records....” They included 40 megabytes of Ashley Madison data as proof.

Avid Life did not comply. On August 18, the Team released almost 10 gigabytes of data on the so-called “dark web” Tor network; it was indexed and searchable on the open web the next day. The company began issuing Digital Millennium Copyright Act (DMCA) takedown requests, the kind of thing normally sent by copyright holders to have movies and music pulled from the web. On August 20, another 19 gigabytes of data were leaked.

Within hours of the data’s release, the first projects allowing the casual browser to easily search the data began to launch. These were front ends for the leak, comparable in outline with the landmark Diary Dig project for searching the leaked data in the Iraq War Diaries. People would enter email addresses, searching for celebrities, politicians, their spouses, bosses, or themselves. Within days, the scams and blackmail began. The scams (some of them products of those search sites) announced that you—which is to say, any email address used as a search—were indeed in the Ashley Madison leak, with all the salacious, marriage-ending, life-ruining information attached to your identity. The scammers promised to *really* fully delete your information, just in time to save you, for a fee.

The blackmail was far more sophisticated: a ransom strategy, with an email sent to addresses in the database.³ “I now have ALL your information,” the blackmailer wrote: “I have also used your profile to find your Facebook profile, using this I now have a direct line to get in touch with all your friends and family.” The blackmailer’s system would automatically forward all your Ashley Madison records to your social network (“and perhaps even your employers too?”) unless it received a payment in Bitcoin within 72 hours. Like the false “Full Delete” option, it was a straightforward way to make good money from desperate people. It also marked the final step of something remarkable, read from beginning to end as a linked series of software components: the extortion stack. You could be tempted, tantalized, sign up to betray, betray (in spirit if not in flesh), create evidence, go through guilt and regret



MESSAGE FROM THE HACKERS:

"Trevor, ALM's CTO, once said 'protection of personal information' was his biggest 'critical success factors' and 'I would hate to see our systems hacked and/or the leak of personal information.' Well Trevor, welcome to your worst fucking nightmare."

2 Annalee Newitz (2015) broke the story about the fembot population. I’ve also written about aspects of this engagement software (Brunton 2015).

3 There have been several reported variations in the blackmail messages. These quotes are taken from the letter distributed to the press by the Toronto Police Service. See Price (2015) for a high-resolution version of the document shared during the press conference, and Krebs (2015) for commentary.

and concealment, and finally be shamefully and secretly blackmailed, all without ever interacting with a person, conducted completely by software: entrapment as a service.

The blackmailers also provided thoughtful advice on how to update your Facebook privacy settings to head off their competitors, but of course, “I have a copy if you don’t pay.” Or rather, the system has a copy, and will pull the trigger if the ransom isn’t paid. The whole process was automated (or claimed to be): this had been an unauthorized cybernetic announcement.

WE WILL RELEASE ALL CUSTOMER RECORDS

If you step far enough back and let the details blur, these stories from 1975 and 2015 have a lot in common as heroic tales of hacking. Anonymous hackers completely compromise an evil corporation, exfiltrate and collate all their data, hold them to account, and then release all to the public. They reveal fraud and hypocrisy in all corners of society, with a combination of general dumps and targeted disclosure. They destroy their target, more or less. As we selectively bring details forward, the story becomes even more canonically a tale of hacker glory: they open-source a vast tranche of records of misdeeds, for which others provide friendly user interfaces and crowd-sourced analysis, sidestepping legal challenges with mirrors and torrents of the data (*information wants to be free, man*), automating repetitive tasks and making use of tools like Tor and Bitcoin.

“Evil” isn’t really the right word for Avid Life Media, though: their online properties were tawdry and exploitative, and at least one of their promises was straightforwardly fraudulent, but they’re small fry compared with Wells Fargo or Dow Chemical. In practice, Ashley Madison was in the business of *preventing* actual extramarital affairs, diverting those impulses into expensive, go-nowhere flirty chats with crude software. (It would have been much easier to break your vows with the help of Craigslist or Grindr.) Their userbase is easy to mock and deride, but the data carry no context, no human nuance: accounts could be made as pranks on friends or coworkers, or from a benign curiosity about a notorious site often in the news, or for reasons, unpleasant as they may be, that are no one else’s business. “We will release all customer records,” said the Impact Team’s landing page demand. “Avid Life Media will be liable for fraud and

extreme harm to millions of users.” If Avid Media did not comply, therefore, and possibly even if they did, it would prove necessary for millions of users to come to harm. Their marriages, careers, and public lives would have to be imperiled and rendered vulnerable to blackmailers and extortionists to bring the adversary down. And so it proved indeed.

Set aside the question of good or bad intentions on the part of users, Avid Life Media’s executives and developers, the Impact Team, and those making use of the leak after the fact (journalists and blackmailers alike). The sheer volume of leaked data dwarfs intentions. It was used to expose the hypocrisy of religious media figures, to provide trenchant evidence of a company’s fraudulent behavior, to ruin the lives of random individuals, to threaten personal revenge on particular attorneys in the Department of Justice, and to build a blackmail machine. *This* was the threshold crossed between 1975 and 2015, to return to the argument: not just that of white hat/black hat, or private individual/state agency, or corporation/country, but the volume of data that could be found, released, and easily explored by amateurs, and with it the space of available interpretations.

To its contemporary reader, *The Shockwave Rider*’s most improbable element might have been a computerized society running over phone networks, or the immense consolidated power of transnational tech companies. Looking back, the fantastic element is that all the data in the single mega-leak was so perfectly legible in its meaning. The public knew precisely what it meant, which is to say that all of it meant only one thing: an arrow pointing to a better government. Did the Impact Team want to destroy Avid Life Media for their fraudulent behavior, to punish cheaters, to amuse themselves, or all of the above? It doesn’t matter. Writers, journalists, extortionists, scammers, spouses, and opposition researchers all made their own interpretative uses of the leak, as they and others have interpreted the mass of data of other mega-leaks. “As of today, whatever you want to know, provided it’s in the data-net, you can now know”: Brunner’s promise contains its own latent disaster in that unspecified, second-person *you*. ■

FINN BRUNTON is an assistant professor in Media, Culture, and Communication at NYU.

BIBLIOGRAPHY

- Brunner, John. 1975. *The Shockwave Rider*. Reprint, New York: Del Rey, 1995.
- Brunton, Finn. 2015. “An Affair to Remember.” *Artforum*, December: 236–239.
- Ellsberg, Daniel. 2003. *Secrets: A Memoir of Vietnam and the Pentagon Papers*. New York: Penguin.
- Krebs, Brian. 2015. “Extortionists Target Ashley Madison Users.” *Krebs on Security*, August 15. Available at link.
- Newitz, Annalee. 2015. “How Ashley Madison Hid Its Fembot Con from Users and Investigators.” *Gizmodo*, September 8. Available at link.
- Price, Rob. 2015. “Ashley Madison offers a \$500,000 reward for hackers as police reveal there have been 2 unconfirmed suicides in wake of the data dump.” *Business Insider*, August 24. Available at link.
- Shoch, John, and Jon Hupp. 1982. “The ‘Worm’ Programs—Early Experience with a Distributed Computation.” *Communications of the ACM* 25(3): 172–180.
- Williams, Linda. 1989. *Hard Core: Power, Pleasure, and the Frenzy of the Visible*. Berkeley: University of California Press.

hacker



madness

Defense lawyer **Tor Ekeland** gives us an up-close, first-person view of a widespread pathology: how misplaced fear and hysteria is driving an over-reaction to the positive work that hackers can do.

Hackers induce hysteria. They are the unknown, the terrifying, the enigma. The enigma that can breach and leak the deepest secrets you've carelessly accreted over the years in varied fits of passion, desperation, boredom, horniness, obsession, and jubilation on your computers, phones and the internet. Maybe you're the government, maybe you're just some innocent schmuck—maybe you're both. Maybe you don't deserve to be exposed, maybe you do. The common fear is that you will never know who exposed you. Is it a he, a she, or an it? The FBI? The NSA? You feel vulnerable and it feels as though what happened is black magic because you understand nothing about how it was done. Terrifying, fascinating, excruciating black magic, practiced by an enigma.

Or maybe you do know how the enigma did it, and you feel stupid: because the enigma exposed your lazy information security—maybe because your password was just “1234”, or your birthday, or maybe you logged into a public Wi-Fi network without VPN, and maybe, just maybe, you used the same password for all your accounts. You're a moron for doing that, and you know it; but it never occurred to you that anyone would bother to hack you at Starbucks. You're hysterical over an enigma that could be anywhere in the world; or perhaps your roommate, child, or lover in your own home.

I regularly observe this hysteria. I'm a defense lawyer who represents hackers in federal courts across the United States. I'm writing this in an airport in Kentucky after the sentencing of a client. He and his colleague hacked a cheap high school football fan website to protest the rape of a minor in Steubenville, Ohio by members of the high school football team. They posted a video of my client in a Guy Fawkes mask decrying the rape. They helped organize protests over the rape in the town. It attracted national media attention. It led to the federal government indicting my client for felony computer crime. The federal government never

prosecuted anyone involved in the rape.

My client was part of a movement protesting what they viewed as the small town's attempted cover up of the extent of the rape. Much ire was directed at the local county prosecutor (not to be confused with the federal prosecutors in Kentucky who indicted my client) who initially handled the case. The perception was that she was intentionally limiting the scope of the prosecution because she was closely connected to the football team through her son. Social media postings of football team-members seemed to implicate more than the two football players she initially went after. Eventually, she recused herself from the case. After this, the town's school superintendent, the high school principal, the high school wrestling coach, and the high school football coach were indicted on various felony and misdemeanor charges including obstruction of justice and evidence tampering. It's unlikely any of this would have happened without the attention my client, along with many others, helped bring to the case.

The local prosecutor wasn't even the one who got hacked. That person, perhaps out of fear, stayed out of it. Yet this prosecutor, in a letter submitted to the court at my client's sentencing, breathlessly condemned my client as a terrorist—yes, a terrorist—for bringing attention to the sordid details of the attempted cover-up of the extent of a 16-year-old girl's rape. A rape that involved the girl incapacitated by alcohol being publicly and repeatedly penetrated and urinated on by members of the football team, their jocular enthusiasm captured in the photos they posted on social media. No one died, no one except the rape victim was physically hurt, yet my client was called a terrorist and thrown in jail because a \$15 website with an easily guessed password got hacked. All of this, because of the embarrassment, the shame, and the vulnerability—not that of the rape victim, but of a town whose dark secrets had been breached and leaked.

My client got two years – the two rapists got one and

“THE TROLL ON
KARL JOHAN
STREET”

BY THEODOR KITTELSEN,
1892.

two years respectively. My client didn't physically or financially harm anyone. At best the damage was reputational, but that was self-inflicted by people in the town. My client didn't rape a minor. Metaphorically, the town did, and in reality, members of its high school football team did. Nonetheless, in that case and most I deal with, the federal criminal "justice" system hysterically treats hackers on par with rapists and other violent felons.

Including the Steubenville rape case, I've now had two clients called "terrorists" in open court. In the second case, the former boss of a client of mine, in a moment that almost made me laugh out loud in court, called him a terrorist at his sentencing. I suspect the boss was a bit jealous of my client's journalistic talent and was ruefully avenging his own feelings of inadequacy and loss of control. This particular client had quit his job in a pique after justifiably accusing his boss at the local TV station of engaging in crappy journalistic practices. After departing his job, he helped hack (allegedly) the *LA Times* website, owned by the same parent company and sharing the same content management system; a few words were changed in a story about tax cuts.

The edits—the government liked to refer to it as the "defacement"—were removed and the article restored to its original state within forty minutes. For this, the sentencing recommendation from pre-trial services was 7 1/2 years, the government asked for 5, and the judge gave him 2. Again, no one was physically hurt, the financial loss claims were dubious, and the harm was reputational, at best. But my client was sentenced more seriously than if he'd violently, physically assaulted someone. In fact, he'd probably have faced less sentencing exposure if he'd beaten his boss with a baseball bat.

Unsurprisingly, his actions were portrayed as a threat to the freedom of the press. There was some pious testimony from an *LA Times* editor about the threat to a so-called great paper's integrity. But when the cries of terrorism are stripped away, a more mundane explanation for all the sanctimony emerges: the "victim's" information security sucked. They routinely failed to deactivate passwords and system access for ex-employees. After the hack, they discovered scores of still active user accounts for ex-employees that took them months to sort through and clean up. They stuck my terrorist client with the bill for fixing their bad infosec, of course. All of this, because of the embarrassment, the shame, and the vulnerability—not of an employee, but that of a powerful organization.

Another one of my clients who lived in a corrupt Texas border town was targeted by a federal prosecutor. The talented young man had committed the egregious sin of running a routine port scan on the local county government's website using standard commercially available software. Don't know what a port scan is? Don't worry, all you need to know is that it's black magic. This client had also gotten into it a tiff with a Facebook admin, exchanged some testy emails with the admin, but walked away from it while the admin

continued to send him emails. A routine internet catfight of little import that wouldn't raise eyebrows with anyone mildly experienced with the internet's trash talking and petty squabbles.

But this client, like most of my clients, was purportedly affiliated with Anonymous. This led to an interesting state of affairs that demonstrates both the fear and the contempt the government has for enigmatic hackers. In essence, the FBI detained my client and threatened him with a felony hacking prosecution unless he agreed to hack the ruthlessly violent Mexican Zeta Cartel.¹ Fearing for his loved ones and himself, my client sensibly declined this death wish. But the FBI persisted. The FBI specifically wanted a document that purportedly listed all the U.S. government officials on the take from the Zetas. No one even knew if this document existed, but the FBI didn't care much about that fact. After my client declined, he was charged with 26 felony counts of hacking and 18 felony counts of cyberstalking based on his interaction with the Facebook admin.

Naturally, this case was brought to my attention. After examining the Indictment and engaging in a few interesting discussions with the federal prosecutor, my client pleaded guilty to a single misdemeanor count of hacking related to his port scanning of the local government website. Better to take a misdemeanor than run the risk of a federal criminal trial where the conviction rate is north of 90%. But the fact that this hysterical prosecution was brought in the first place reflects poorly on the exercise of prosecutorial discretion about hacking on the part of the Department of Justice. Again, no one was hurt, no one lost money, but my client was facing a maximum of 440 years in jail under the original Indictment.

My hands down favorite example of hacker-induced hysteria was directed at me and my co-counsel in open court. I couldn't hack my way out of a paper bag, but prosecutors love to tar me by association with my clients. In this instance, on the eve of trial on a Friday in open federal court, the prosecutor—along with the FBI agent on the case—accused my co-counsel and me of hacking the FBI, downloading a top-secret document, removing the top-secret markings on it, and then producing it as evidence we wanted to use at trial. Co-counsel and I were completely baffled, exchanged glances, and then told the court we would give the court an answer on Monday as to the document's origins—and to this criminal, law license jeopardizing accusation.

It turns out we'd downloaded the document in question from the FBI's public website. The FBI had posted the document because it was responsive to a Freedom of Information Act request. The FBI had removed the top-secret markings in so doing. Needless to say, we corrected the record on Monday. Pro-tip for rookie litigators: If your adversary produces a document you have a serious question about, it's best to confer with your adversary off the record about it before you cast

¹ <https://www.wired.com/2015/02/hacker-claims-feds-hit-44-felonies-refused-fbi-spy/>

accusations in open court that implicate them in felony hacking and Espionage Act violations. But, such is the hysteria that hacking induces that it spills over to the lawyers that defend them. How many lawyers who defend murderers are accused of murder?

The feelings of vulnerability, fear of the unknown, and embarrassment that feed the hysterical reaction to hackers also lead to the fetishizing of hackers in popular culture. T.V. shows like *Mr. Robot*, *House of Cards*, and movies like *Live Free or Die Hard*, where the hackers are both villains and heroes, all exacerbate this fetish. And this makes life harder for me and my clients because we have to combat these stereotypes pre-trial, at trial, and during their incarceration should that come to be. Pre-trial, my clients are subjected to irrational, restrictive terms of release that rest on the assumption that mere use of a computer will lead to something nefarious. During trial, we have to combat the jury's preconceptions of hackers. And if and when they're put in jail, convicted hackers are often treated on par with the worst, most violent felons. Almost all of my incarcerated clients were thrown in solitary for irrational, hacker-induced hysteria reasons. But those are stories for another day.

The hysteria hackers induce is real, and it is dangerous. It leads to poorly conceived and drafted draconian laws like America's Computer Fraud and Abuse Act. It distorts our criminal justice system by causing prosecutors and courts to punish mundane computer information security acts on par with rape and murder. Often, I receive phone calls from information security researchers, with fear in their voice, worried that some routine, normally accepted part of their profession is exposing them to felony liability. Usually I have to tell them that it probably is.

And the hysteria destroys the lives of our best computer talents, who should be cultivated and not thrown in jail for mundane activities or harmless pranks. All good computer minds I've met do both. Thus, not only is hacker-induced hysteria detrimental to our criminal justice system in that it distorts traditional notions of fairness, justice, and punishment based on irrational fears. It is fundamentally harmful to our national economy. And that should give even the most ardent defenders of the capitalistic order at the Department of Justice and the FBI pause, if not stop them dead in their tracks, before pursuing hysterical hacking

prosecutions.

The best proof that this hysteria is unwarranted and unnecessary most of the time is the fate of persecuted hackers and hacktivists themselves. Most of those arrested for pranks, explorations, and even risky, hardcore acts of hacktivism aren't a detriment to society, they're beneficial to our society and economy. After their youthful learning romps, they've matured their technical skills—unlearnable in any other fashion—into laudable projects. Robert Morris was author of the Morris Worm. He's responsible for one of earliest CFAA cases because his invention got out of his control and basically slowed down the internet, such as it was, in 1988. Now he's a successful Silicon Valley entrepreneur and tenured professor at MIT who has made significant contributions to computer science. Kevin Poulsen is an acclaimed journalist; Mark Abene and Kevin Mitnick are successful security researchers. And those're just the old-school examples from the ancient—in computer time—1990's.

Younger hackers are doing the same. From the highly entertaining hacker collective Lulzsec, Mustafa Al Bassam is now completing a PhD in cryptography at University College London; Jake Davis is translating hacker lore, culture, and ethics to the public at large; Donncha O'Cearbhaill, is employed at a human rights technology firm and is a contributor to the open source project Tor (no relation); Ryan Ackryod and Darren Martyin are also successful security researchers. Sabu, the most famous member of Lulzsec, of course, has enjoyed a successful career as a snitch, hacking foreign government websites on behalf of the FBI and generally basking in the fame and lack of prison time his sell out engendered. And I'm not going to talk about the young, entertaining hackers that haven't been caught yet. But the ones I care about, the ones I think are important, aren't interested in making money off your bad infosec. They're just obsessed by how the system works, and a big part of that is taking the system apart. Perhaps I share that with them as a federal criminal defense lawyer.

All these hackers exemplify the harms that hysteria can have: misdirecting the energy of exactly the people who can help test, secure and transform the world we occupy in the name of public values that we share: values our own government should be defending, instead of destroying. ■

*Tor's parents are from Norway, hence his name. Yes, it's real. The only reason you think it should have an "H" in it is because you've watched that movie. Tor is way sexier than Chris Hemsworth. His name also precedes the invention of The Onion Router and him becoming a computer lawyer. Don't know what The Onion Router is? That's ok, just know it's black magic. Tor didn't know what it was until everyone starting asking if Tor was his real name when he repped weev, one of the most famous internet trolls in the English language. They still talk, despite the fact that weev is basically a neo-Nazi and the Gestapo tortured Tor's dad for four days and then threw him in a concentration camp. His dad taught him resistance techniques and the value of a sense of humor in the face of the moral smugness of the state. Since weev, Tor has also represented a bunch of hackers in federal courts across the United States, and is going to take the non-public part of that and his other off-the-record representations to his grave. At which point—the point of his death—perhaps there will be an information dump, just for the Lulz. Or his name isn't **TOR EKELAND**.*

What can you do with a Tor exploit? **Renée Ridgway** discusses an ethical dilemma for security researchers, a surreptitious game of federal investigators, and the state of online anonymity today.



WHO'S HACKING WHOM?

WHO IS HACKING WHOM? The case of Brian Farrell (a.k.a. “Doctor Clu”) raises a host of interesting questions about the nature of hacking, vulnerability disclosure, the law, and the status of security research. Doctor Clu was brought to trial by FBI agents who identified him by his Internet Protocol (IP) address. But Clu was using Tor (The Onion Router) to hide his identity, so the FBI had to find a way to “hack” the system to reveal his identity. They didn’t do this directly, though. Allegedly, they subpoenaed some information security researchers at Carnegie Mellon University’s Software Engineering Institute (SEI) for a list of IP addresses. Why did SEI have the IP addresses? Ironically, these Department of Defense-funded researchers had bragged about a presentation they would give at the Black Hat security conference on de-anonymising Tor users “on a budget.” For whatever reason, they had Clu’s IP address as a result of their work, and the FBI managed to get it from them. Clu’s defense team tried to find out how exactly it was obtained and argued that this was a violation of the 4th amendment, but the judge refused: IP addresses are public, he said; even on Tor, where users have no ‘expectation of privacy.’

In this case, security researchers ‘hacked’ Tor in a technical sense; but the FBI also hacked the researchers in a legal sense – by subpoenaing the exploit and its results in order to bring Clu to trial. As in the recent WannaCry ransomware attack, or the Apple iPhone vs. FBI San Bernardino terrorism investigation of summer 2016, this case reveals the entanglement of security research, the hoarding of exploits and vulnerabilities, the use of those tools by law enforcement and spy agencies, and ultimately citizens’ right to privacy online. The rest of this piece explores this entanglement, and asks: what are the politics of disclosing vulnerabilities? What new risks and changed expectations exist in a world where it is not clear who is

hacking whom? What responsibilities do researchers have to protect their subjects and what expectations do Tor users have to be protected from such research?

“TOR’S MOTIVATION FOR THREE HOPS IS ANONYMITY”

“Tor is a low-latency anonymity-preserving network that enables its users to protect their privacy online” and enables “anonymous communication” (AlSabah et al., 2012: 73). The Tor p2p network is a mesh of proxy servers where the data is bounced through relays, or nodes. As of this writing, more than 7,000 relays enable the transferral of data, applying “onion routing” as a tactic for anonymity (Spitters et al., 2014).² Onion routing was first developed and designed by the US Naval Research Laboratory in order to secure online intelligence activities. Data is sent using Tor through a proxy configuration (3 relays: entry, middle, exit) adding a layer of encryption at every node whilst decrypting the data at every “hop” and forwarding it to the next onion router. In this way, the “clear text” does not appear at the same time and thereby hides the IP address, masking the identity of the user and providing anonymity. At the end of a browsing session the user history is deleted along with the HTTP cookie. Moreover, the greater the number of people using Tor, the higher the anonymity level for users who are connected to the p2p network; volunteers around the world provide servers and enable the Tor traffic to flow.

There is also controversy surrounding the Tor network, connecting it to the so-called “Dark Net” and its “hidden services” that range from the selling of illegal drugs, weapons, and child pornography to sites of anarchism, hacktivism, and politics (Spitters et al., 2014: 1). All of this has increased the risks involved in using Tor. As shown in numerous studies (AlSabah et al., 2012, Spitters et al., 2014, Çalışkan et al., 2015, Winter et al., 2014

and Biryukov et al., 2013), different actors have compromised the Tor network, cracking its anonymity. These actors potentially include the NSA, authoritarian governments worldwide, and multinational corporations: all organisations that would like to discover the identity of users and their personal information (see for example, the case of Hacking Team).³ Specifically, it should not be discounted that Tor exit node operators have access to the traffic going through their exit nodes, whoever they are (Çalışkan et al., 2015: 29). Besides governmental actors in the security industries, activists, dissidents and whistle-blowers using Tor, there are also academics that carry out research attempting to “hack” Tor.

THE RESEARCHERS’ ETHICAL DILEMMA

In January 2015, Brian Farrell aka “Doctor Clu,” was arrested and charged with one count of conspiracy to distribute illegal “hard” drugs such as cocaine, methamphetamine and heroin at a “hidden service” marketplace (Silk Road 2.0) on the so-called “Dark Net” (Geuss 2015).⁴ His IP address (along with other users) was purportedly captured in early 2014 by researchers, Alexander Volynkin and Michael McCord, when they were carrying out their empirical study at SEI, a non-profit organisation at Carnegie Mellon University (CMU) in Pittsburgh, U.S.A. The SEI researchers were supposedly able to bypass security and with their hack, obtain around 1000 IP addresses of users.

Since the beginning of 2014, an unnamed source had been giving authorities the IP address of those who accessed this specific part of the site (Vinton 2015).

The researchers from SEI at CMU were invited to present their methods and findings on how to “de-anonymize hundreds of thousands of Tor clients and thousands

1 (Winter et al., 2014: 6).

2 <https://torstatus.blutmagie.de/>

3 “The Italian organisation, which even its CEO called a “notorious” provider of government spyware, was looking to expand its line of products, Rabe said. That included targeting the anonymizing Tor network, where civil rights activists, researchers, pedophiles and drug dealers alike try to hide from the global surveillance complex” (Fox-Brewster 2015).

4 (U.S. v. Farrell, U.S. District Court, W.D. Wash., No. 15-mj-00016) Complaint for Violation. <https://cdn.arstechnica.net/wp-content/uploads/2015/01/5498263-0-14302.pdf>

A Schedule Update:

For more than 16 years, Black Hat has provided a venue for attendees and the larger community to find the very latest in information security research, developments and trends. We strive to deliver one of the most empirically selected lineups of content in the industry. One of our selected talks, "You Don't Have to be the NSA to Break Tor: Deanonymizing Users on a Budget" by CERT/Carnegie Mellon researcher Alexander Volynkin was scheduled for a Briefing at Black Hat USA this August in Las Vegas. Late last week, we were informed by the legal counsel for the Software Engineering Institute (SEI) and Carnegie Mellon University that: "Unfortunately, Mr. Volynkin will not be able to speak at the conference since the materials that he would be speaking about have not yet approved by CMU/SEI for public release." As a result, we have removed the Briefing from our schedule.



FIGURE 1 (ABOVE AND LEFT): Black Hat 2014 website Schedule Update.

FIGURE 2 (BELOW): Black Hat 2014 Briefings.

YOU DON'T HAVE TO BE THE NSA TO BREAK TOR: DEANONYMIZING USERS ON A BUDGET

The Tor network has been providing a reasonable degree of anonymity to individuals and organizations worldwide. It has also been used for distribution of child pornography, illegal drugs, and malware. Anyone with minimal skills and resources can participate on the Tor network. Anyone can become a part of the network. As a participant of the Tor network, you can choose to use it to communicate anonymously or contribute your resources for others to use. There is very little to limit your actions on the Tor network. There is nothing that prevents you from using your resources to de-anonymize the network's users instead by exploiting fundamental flaws in Tor design and implementation. And you don't need the NSA budget to do so. Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild...

In this talk, we demonstrate how the distributed nature, combined with newly discovered shortcomings in design and implementation of the Tor network, can be abused to break Tor anonymity. In our analysis, we've discovered that a persistent adversary with a handful of powerful servers and a couple gigabit links can de-anonymize hundreds of thousands Tor clients and thousands of hidden services within a couple of months. The total investment cost? Just under \$3,000. During this talk, we will quickly cover the nature, feasibility, and limitations of possible attacks, and then dive into dozens of successful real-world de-anonymization case studies, ranging from attribution of botnet command and control servers, to drug-trading sites, to users of kiddie porn places. The presentation will conclude with lessons learned and our thoughts on the future of security of distributed anonymity networks.

PRESENTED BY

Alexander Volynkin & Michael
McCord

of hidden services” at the *Black Hat* security conference in July 2014, but they never showed up and the reason of their cancellation is still posted on the website (Figure 1). As the next screenshot of the Internet Archive’s Way Back Machine reflects (Figure 2), the researcher’s abstract elucidated their braggadocio of a low budget exploit of Tor for around \$3000, as well as a call out to others to try:

Looking for the IP address of a Tor user? Not a problem. Trying to uncover the location of a Hidden Service? Done. We know because we tested it, in the wild... (Volynkin 2014).

With regard to ethical research considerations, the researchers’ “anonymous subjects” didn’t realize or know they were participating in a study-cum-hack. Many in the security research community regard this as an infringement of ethical standards included in the *IEEE Code of Ethics* that prohibits “injuring others, their property, reputation, or employment by false or malicious action” (IEEE n.d.: section 2.4.2). Even when following such an officially recognized IEEE ethical code, “failure, discovery, and unintended or collateral consequences of success” (Greenwald et. al. 2008:78) could potentially harm “objects of study” – in this case the visitors to the Silk Road 2.0. The Dark Net is perhaps trickier than other fields but there are also academics carrying out research there, contacting users, building their trust and protecting their sources.⁵ Supposedly SEI started hosting part of Tor’s relays, but intentionally set up “malicious actors” so that they could carry out their research. According to one anonymous source reported at *Motherboard*, SEI

had the ability to deanonymize a new Tor hidden service in less than two weeks. Existing hidden services required upwards of a month, maybe even two months. The trick is that you have to get your attacking Tor nodes into a privileged position in the Tor network, and this is easier for new hidden services than for existing hidden services (Cox 2015).

It is crucial that the Tor Project is always informed of the exploit even before it is released so that they can fix potential flaws that enable deanonymization. During the past several years, researchers have continuously shared their data with the Tor Project and reported their findings, such as malicious attacks, or what is called “sniffing” – when the exit relay information is compromised. Once a study is published, patches are developed and Tor improves upon itself as these breaches of security are uncovered. Unlike other empirical studies, the SEI researchers did not inform the Tor Project of their exploits. Instead Tor discovered the exploits and contacted the researchers, who declined to give details. Only after the abstract for *Black Hat* (late June 2014) was published online did the researchers “give the Tor Project a few hints about the attack but did not reveal details” (Felten 2014). The Tor Project ejected the attacking relays and worked on a fix for all of July 2014, with a software update release at the end of the month, along with an explanation of the attack (Dingledine 2014). As this case shows, not only “malicious actors,” but also certain researchers can collect data on Tor users. According to the Tor Project director Roger Dingledine the SEI researchers acted inappropriately:

Such action is a violation of our trust and basic guidelines for ethical research. We strongly support independent research on our software and network, but this attack crosses the crucial line between research and endangering innocent users (Dingledine 2014).

A SUBPOENA FOR RESEARCH

In November 2015, the integrity of these two SEI researchers was again brought into question when the rumour circulated that they had been subpoenaed by the FBI to hand over their collated IP addresses. According to an assistant researcher at CMU Nicolas Christin, SEI is a non-profit and not an academic institution and therefore the researchers at SEI are not academics but instead are “focusing specifically on software-related security and engineering issues” and in 2015 the SEI renewed a 5-year governmental contract for 1.73 billion dollars (Lynch 2015). In an official media statement, CMU’s SEI

responded by explaining that their mission encompassed searching and identifying “vulnerabilities in software and computing networks so that they may be corrected” (CMU 2015). Important to note is that the US government (specifically the Departments of Defense and of Homeland Security) funds many of these research centers, such as CERT (Computer Emergency Response Team), a division of SEI which has existed ever since the Morris Worm first created a need for such an entity (Kelty 2011). To be precise, it is one of the Federally Funded Research and Development Centers (FFRDC), which are

unique non-profit entities sponsored and funded by the U.S. government that address long-term problems of considerable complexity, analyze technical questions with a high degree of objectivity, and provide creative and cost-effective solutions to government problems (Lynch 2015).

Legally, in the U.S., the FBI, SEC and the DEA can all subpoena researchers to share their research. However, the obtained information was not for public consumption, but for an agency within the U.S. Department of Justice, the FBI. Matt Blaze, a computer scientist at the University of Pennsylvania made the following statement about conducting research:

When you do experiments on a live network and keep the data, that data is a record that can be subpoenaed. As academics, we’re not used to thinking about that. But it can happen, and it did happen (Vitáris 2016).

Besides the ethical questions regarding the researchers handing over their findings to the governments that have supported them (ostensibly with tax-payer money), the politics of security research and vulnerability disclosure continues to be a heated debate within academia and the general public. It seems that issuing subpoenas by law enforcement might provide a means to gather data on citizens and to obtain knowledge of academic research – which then remains hidden from the public. Computer security defense

5 I refer here specifically to Jamie Bartlett’s ‘The Dark Net’ research.

GRAND JURY
Subpoena Duces Tecum

SUBPOENA DUCES TECUM
United States District Court
For the District of Columbia

Misc. #47-73

THE UNITED STATES
vs.
JOHN DOE

REPORT TO UNITED STATES DISTRICT COURT HOUSE
Between 3d Street and John Marshall Place
and on Constitution Avenue NW.
~~ROOM 312X~~ Grand Jury Room 3
Washington, D.C.

To: Richard M. Nixon, The White House, Washington, D. C., or any subordinate officer, official, or employee with custody or control of the documents or objects hereinafter described on the attached schedule.

FILED
JUL 24 1973
JAMES F. DAVEY, Clerk

You are hereby commanded to attend before the Grand Jury of said Court on Thursday the 26th day of July, 19 73, at 10 o'clock A. M., to testify on behalf of the United States, and not depart the Court without leave of the Court or District Attorney, and to bring with you the documents or objects listed on the attached schedule. WITNESS: The Honorable John J. Sirica, Chief Judge of said Court, this 23rd day of JULY, 19 73.

ARCHIBALD COX
Attorney for the United States

By Robert L. Line Deputy Clerk.

Form No. USA-9x-184 (Rev. 7-1-71)

34

LEFT: Richard Nixon's 1973 Grand Jury subpoena.

lawyer Tor Ekeland gave this comment:

It seems like they're trying to subpoena surveillance techniques. They're trying to acquire intel[ligence] gathering methods under the pretext of an individual criminal investigation (Vitáris 2016).

It is not clear whether the FBI was using a subpoena to acquire exploits, or if the CMU (SEI) researchers were originally hired by the FBI and only later disclosed what happened, stating that they had been subpoenaed?⁶ Either way, it would raise the issue of whether the FBI required

a search warrant in order to obtain the evidence – the IP addresses.

INTERNET SEARCH AND SEIZURE

In January 2016, Farrell's defense filed a motion to compel discovery, in an attempt to understand exactly how the IP address was obtained, as well as the past two-year history of the relationship between the FBI and SEI through working contracts. In February 2016, the Farrell case came to court in Seattle where it was finally revealed to the public that the "university-based research institute" was confirmed to be SEI at CMU, subpoenaed by the FBI (Farivar 2016). The court denied the defense's motion to compel discovery.

This statement from the order – *Section II, Analysis* – written by US District Judge Richard A. Jones answered the question of whether a search warrant was needed to obtain IP addresses:

SEI's identification of the defendant's IP address because of his use of the Tor network did not constitute a search subject to Fourth Amendment scrutiny (Cox 2016).⁷

In order to claim protection under the Fourth Amendment, there needs to be a demonstration of an "expectation of privacy," which is not subjective but

6 February 24, 2016: "When asked how the FBI knew that a Department of Defence research project on Tor was underway, so that the agency could then subpoena for information, Jillian Stickels, a spokesperson for the FBI, told Motherboard in a phone call that 'For that specific question, I would ask them [Carnegie Mellon University]. If that information will be released at all, it will probably be released from them.'" (Cox 2016)

7 Scrutiny of the Fourth Amendment shows the original text of 1789 that was later ratified in the Bill of Rights, the first 10 amendments to the US Constitution: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. <https://www.archives.gov/founding-docs/bill-of-rights-transcript>

recognized as reasonable by other members of society. Furthermore, Judge Jones claimed that the IP address “even those of Tor users, are public, and that Tor users lack a reasonable expectation of privacy” (Cox 2016).

Again, according to the party’s submissions, such a submission is made despite the understanding communicated by the Tor Project that the Tor network has vulnerabilities and that users might not remain anonymous. Under these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network. In other words, they take a significant gamble on any real expectation of privacy under these circumstances (Jones 2016:3).

Judge Jones reasoned that Farrell didn’t have a reasonable expectation of privacy because he used Tor; but he also stated that IP addresses are public because he willingly gave his IP address to an Internet Service Provider (ISP), in order to have internet access. Moreover, the citation (precedent) that Judge Jones drew upon to uphold his order, namely, *United States v. Forrester*, ruled that individuals have no reasonable ‘expectation of privacy’ with internet IP addresses and email addresses:

The Court reaches this conclusion primarily upon reliance on United States v. Forrester, 512 F.2d 500 (9th Cir. 2007). In Forrester, the court clearly enunciated that: Internet users have no expectation of privacy in ...the IP address of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information (Jones 2016:2-3).

TRUST

In March 2016, Farrell eventually pleaded guilty to one count of conspiracy regarding the distribution of heroin, cocaine and amphetamines in connection with the hidden marketplace Silk Road 2.0 and

received an eight-year prison sentence. In this case, the protection of an anonymous IP address was thwarted in various ways (a hack, a subpoena, a ruling) with regard to governmental intrusion. Privacy technologists, such as Christopher Soghoian, have provided testimony in similar cases, explaining that the government states that obtaining IP addresses “isn’t such a big deal,” yet the government can’t seem to elucidate how they could actually obtain them (Kopstein 2016).

Whoever wanted to know the IP address would have to be in control of many nodes in the Tor network, around the world; and one would have to intercept this traffic and then correlate the entry and exit nodes. Besides the difficulty factor, these correlation techniques cost time and money and these exploits, including the one from the SEI researchers, were possible in 2014. Even if IP addresses are considered public when using Tor, they are anonymous unless they are correlated with a specific individual’s device.⁸ To correlate Farrell’s IP address, the FBI had to obtain the list of IP addresses from Farrell’s ISP provider, Comcast.

The judge’s cited reason for denying the motion to compel disclosure was that IP addresses are in and of themselves not private, as people willingly provide them to third parties. Nowadays people increasingly use the internet (and write emails) instead of the telephone; and in order to do so, they must divulge their IP address to an ISP in order to access the internet. When users are outside of the Tor anonymity network, their IP is exposed to an ISP. However, when inside the “closed field” of Tor, is there no expectation of privacy along with the security of the content? And by extension, is there not an expectation of anonymity with the security of users’ identity?

Judge Jones also argued that that Farrell didn’t have an expectation of privacy because he handed over his IP address to strangers running the Tor network.

[I]t is the Court’s understanding that in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes,

so that their communications can be directed towards their destinations. Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers (Jones 2016:3).

Herewith the notion of trust surfaces and plays a salient role. When people share information with ethnographers, anthropologists, activists or journalists and it takes months, sometimes years to gain people’s trust; and the anonymity of the source often needs to be maintained. These days when people choose to use the Tor network they trust a community that can see the IP address at certain points, and they trust that the Tor exit node operators do not divulge their collected IP addresses nor make correlations. In an era of so-called Big Data, as more user data is collated (by companies, governments and researchers) correlation becomes easier and deanonymization occurs more frequently. With the Farrell case, researchers’ ethical dilemmas, the politics of vulnerability disclosure and law enforcement’s “hacking” of Tor all played a role in obtaining his IP address. Despite opposing judicial rulings, it can be argued that Tor users do have an expectation of privacy whereas the capture of IP addresses for users seeking anonymity online has been expedited. ■

RENÉE RIDGWAY is presently a PhD candidate at Copenhagen Business School (MPP) and a research affiliate with the Digital Cultures Research Lab (DCRL), Leuphana University, Lüneburg. Her research investigates the conceptual as well as technological implications of using search, ranging from the personalisation of Google to anonymous browsing using Tor. Recent contributions to publications include Ephemera, SAGE Encyclopaedia of the Internet, Hacking Habitat, Money Labs (INC), OPEN!, APRJA and Disrupting Business.

BIBLIOGRAPHY

- AlSabah, Mashael; Bauer, Kevin and Goldberg, Ian. 2012. "Enhancing Tor's Performance using Real-time Traffic Classification." presented at CCS'12, Raleigh, North Carolina, USA. October 16–18.
- Bartlett, Jamie. 2014. *The Dark Net: Inside the Digital Underworld*. Portsmouth: Heinemann.
- Biryukov, A., Pustogarov, I. and Weinmann, R.P. 2013. "Trawling for tor hidden services: Detection, measurement, deanonymization," in *Security and Privacy (SP)*. 2013 IEEE Symposium on. IEEE, pp. 80–94.
- Çalışkan, Emin, Minárik, Tomáš, and Osula; Anna-Maria. 2015. *Technical and Legal Overview of the Tor Anonymity Network*. Tallin: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.
- Carnegie Mellon University (CMU). 2015. "Media Statement." November 18th. <http://www.cmu.edu/news/stories/archives/2015/november/media-statement.html>
- Cox, Joseph. 2015. "Tor Attack Could Unmask New Hidden Sites in Under Two Weeks." November 13th. https://motherboard.vice.com/en_us/article/tor-attack-could-unmask-new-hidden-sites-in-under-two-weeks
- . 2016 "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds." February 24th. https://motherboard.vice.com/en_us/article/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds
- Dingledine, Roger a.k.a. arma. 2014. "Tor security advisory: "relay early" traffic confirmation attack," *Tor Project Blog*. July 30th. <https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack#comment-66781>
- Dittrich et. al. 2009. *Towards Community Standards for Ethical Behavior in Computer Security Research*. Stevens CS Technical Report 20091, April 20th. <http://mdbailey.ece.illinois.edu/publications/dbd2009tr1.pdf>
- Farivar, Cyrus. 2016. "Top Silk Road 2.0 admin "DoctorClu" pleads guilty, could face 8 years in prison." *Ars Technica*, April 4th. <https://arstechnica.com/tech-policy/2016/04/top-silk-road-2-0-admin-doctorclu-pleads-guilty-could-face-8-years-in-prison/>
- Felten, Ed. 2014 "Why were CERT researchers attacking Tor?" *Freedom to Tinker Blog*. July 31. <https://freedom-to-tinker.com/2014/07/31/why-were-cert-researchers-attacking-tor/>
- Fox-Brewster, Thomas. 2015. "\$30,000 to \$1 Million — Breaking Tor Can Bring In The Big Bucks." *Forbes Magazine*. November 12th <https://www.forbes.com/sites/thomasbrewster/2015/11/12/earn-money-breaking-tor>
- Geuss, Megan. 2015 "Alleged "right hand man" to Silk Road 2.0 leader arrested in Seattle." *Ars Technica*. January 21st. <https://arstechnica.com/tech-policy/2015/01/alleged-right-hand-man-to-silk-road-2-0-leader-arrested-in-seattle>
- Greenwald, Stephen J. et. al. 2008. "Towards an Ethical Code for Information Security?" NSPW'08, September 22–25 <http://www.nspw.org/papers/2008/nspw2008-greenwald.pdf>
- IEEE. N.d. *IEEE Code of Ethics*. <https://www.ieee.org/about/corporate/governance/p7-8.html>
- Jones, Richard A. 2016b. Order on Defendant's Motion to Compel *United States v. Farrell*, CR15-029RAJ. U.S. District Court, Western District of Washington, Filed 02/23/16. <https://assets.documentcloud.org/documents/2719591/Farrell-Weds.pdf>
- Kelty, Christopher M. 2011. "The Morris Worm." *Limn. Issue Number One: Systemic Risk*. <http://limn.it/the-morris-worm/>
- Kopstein, Joshua. 2016. "Confused Judge Says You Have No Expectation of Privacy When Using Tor." *Motherboard*, https://motherboard.vice.com/en_us/article/confused-judge-says-you-have-no-expectation-of-privacy-when-using-tor-playpen-fbi-michaud
- Lynch, Richard. 2015. "CMU's Software Engineering Institute Contract Renewed by Department of Defense for \$1.73 Billion." Press Release, Carnegie Mellon University. July 28th. <https://www.cmu.edu/news/stories/archives/2015/july/sei-contract-renewed.html>
- Spitters, Martijn, Verbruggen, Stefan and van Staaldin, Mark. 2014. "Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services," presented at *2014 IEEE Joint Intelligence and Security Informatics Conference*, Los Angeles, CA, USA; 15–17 Dec 2014
- Vinton, Kate. 2015. "Alleged Silk Road 2.0 Operator's Right-Hand Man Arrested On Drug Charges." *Forbes Magazine*. January 21. <https://www.forbes.com/sites/katevinton/2015/01/21/silk-road-2-0-administrator-doctorclu-arrested-on-drug-charges/#7e4e8fc73cc5>
- Vitáris, Benjamin. 2016. "FBI's Attack On Tor Shows The Threat Of Subpoenas To Security Researchers." *Deep Dot Web Blog*. March 8 <https://www.deepdotweb.com/2016/03/08/fbis-attack-on-tor-shows-the-threat-of-subpoenas-to-security-researchers/>
- Volynkin, Alexander and McCord, Michael. 2014. "Deanonymizing users on a budget." *Black Hat 2014 Briefings*. <https://web.archive.org/web/20140625125021/https://www.blackhat.com/us-14/briefings.html#you-dont-have-to-be-the-nsa-to-break-tor-deanonymizing-users-on-a-budget>
- Winter, Philipp; Köwer, Richard, et. al. 2014. "Spoiled Onions: Exposing Malicious Tor Exit Relays." In: *Privacy Enhancing Technologies Symposium*. Springer.

— WHAT IS TO BE HACKED?

At the beginning of 2017 information security researcher, Amnesty International technologist, and hacker Claudio (“nex”) Guarnieri launched “Security without Borders,” an organization devoted to helping civil society deal with technical details of information security: surveillance, malware, phishing attacks, etc. Journalists, activists, nongovernmental organizations (NGOs), and others are all at risk from the same security flaws and inadequacies that large corporations and states are, but few can afford to secure their systems without help. Here Guarnieri explains how we got to this stage and what we should be doing about it.

COMPUTER SYSTEMS WERE DESTINED FOR a global cultural and economic revolution that the hacker community long anticipated. We saw the potential; we saw it coming. And while we enjoyed a brief period of reckless banditry, playing cowboys of the early interconnected age, we also soon realized that information technology would change everything, and that information security would be critical. The traditionally subversive and anti-authoritarian moral principles of hacker subculture increasingly have been diluted by vested interests. The traditional distrust of the state is only meaningfully visible in some corners of our community. For the most part—at least its most visible part—members of the security community/industry are enjoying six-figure salaries, luxurious suites in Las Vegas, business class traveling, and media attention.

The internet has morphed with us: once an unexplored space we wandered in solitude, it has become a marketplace for goods, the primary vehicle for communication, and the place to share cat pictures, memes, porn, music, and news as well as an unprecedented platform for intellectual liberation, organization, and mobilization. Pretty great, right? However, to quote Kevin Kelly:

There is no powerfully constructive technology that is not also powerfully destructive in another direction, just as there is no great idea that cannot be greatly perverted for great harm.... Indeed, an invention or idea is not really tremendous unless it can be tremendously abused. This should be the first law of technological expectation: the greater the promise of a new technology, the greater is the potential for harm as well (Kelly 2010:246).

Sure enough, we soon observed the same technology of liberation become a tool for repression. It was inevitable, really.

Now, however, there is an ever more significant technological imbalance between states and their citizens. As billions of dollars are poured into systems of passive and active surveillance—mind you, not just by the United States, but by every country wealthy enough to do so—credible defenses either lag, or remain inaccessible, generally only available to corporations with deep enough pockets. The few ambitious free software projects attempting to change things are faced with rather unsustainable funding models, which rarely last long enough to grow the projects to maturity.

Nation states are well aware of this imbalance and use it to their own advantage. We have learned through the years that technology is regularly used to curb dissent, censor information, and identify and monitor people, especially those engaged in political struggles. We have seen relentless attacks against journalists and

activists in Ethiopia, the crashing of protest movements in Bahrain, the hounding of dissidents in Iran, and the tragedy that became of Syria, all complemented with electronic surveillance and censorship. It is no longer hyperbole to say that people are sometimes imprisoned for a tweet.

As a result, security can no longer be a privilege, or a commodity in the hands of those few who can afford it. Those who face imprisonment and violence in the pursuit of justice and democracy cannot succeed if they do not communicate securely, or if they cannot remain safe online. Security must become a fundamental right to be exercised and protected. It is the precondition for privacy, and a key enabler for any fundamental freedom of expression. While the security industry is becoming increasingly dependent—both financially and politically—on the national security and defense sector, there is a renewed need for a structured social and political engagement from the hacker community.

Some quarters of the hacker community have long been willing to channel their skills toward political causes, but the security community lags behind. Eventually some of us become mature enough to recognize the implications and social responsibilities we have as technologists. Some of us get there sooner, some later; some never will. Having a social consciousness can even be a source of ridicule among techies. You can experience exclusion when you become outspoken on matters that the larger security and hacking communities deem foreign to their competences. Don't let that intimidate you.

As educated professionals and technicians, we need to recognize the privilege we have, like our deep understanding of the many facets of technology; we must realize that we cannot abdicate the responsibility of upholding human rights in a connected society while continuing to act as its gatekeepers. Whether creating or contributing to free software, helping someone in need, or pushing internet corporations to be more respectful of users' privacy, dedicating your time and abilities to the benefit of society is concretely a political choice and you should embrace that with consciousness and pride.

TODAY WE FACE UNPRECEDENTED challenges, and so we need to rethink strategies and re-evaluate tactics.

In traditional activism, the concept of “bearing witness” is central. It is the practice of observing and documenting a wrongdoing, without interfering, and with the assumption that exposing it to the world, causing public outcry, might be sufficient to prevent it in the future. It is a powerful and, at times, the only available and meaningful tactic. This wasn't always the case. In activist movements, the shift of tactics is generally observed in reaction to the growth, legitimization, and structuring of the movements themselves as

they conform to the norms of society and of acceptable behavior.

Similarly, as we conform too, we also “bear witness.” We observe, document, and report on the abuses of technology, which is a powerful play in the economic tension that exists between offense and defense. Whether it is a journalist’s electronic communications intercepted or computer compromised, or the censorship of websites and blocking of messaging systems, the exposure of the technology empowering such repressions increases the costs of their development and adoption. By bearing witness, such technologies can be defeated or circumvented, and consequently re-engineered. Exposure can effectively curb their indiscriminate adoption, and factually become an act of oversight. Sometimes we can enforce in practice what the law cannot in words.

The case of Hacking Team is a perfect example. The operations of a company that produced and sold spyware to governments around the world were more effectively scrutinized and understood as a result of the work of a handful of geeks tracking and repeatedly exposing to public view the abuses perpetrated through the use of that same spyware. Unfortunately, regulations and controls never achieved quite as much. At a key moment, an anonymous and politicized hacker mostly known by the moniker “Phineas Phisher” (Franceschi-Bicchierai 2016) arrived, hacked the company, leaked all the emails and documents onto the internet, and quite frankly outplayed us all. Phineas, whose identity remains unknown almost two years later, had previously also hacked Gamma Group, a British and German company and competitor of Hacking Team, and became a sort of mischievous hero in the hacktivist circles for his or her brutal hacks and the total exposure of these companies’ deepest secrets. In a way, one could argue that Phineas achieved much more attention from the public, and better results, than anyone had previously, myself included. Sometimes an individual, using direct action techniques, can do more than a law, a company, or an organization can.

However, there is one fundamental flaw in the practice of bearing witness. It is a strategy that requires accountability to be effective. It requires naming and shaming. And when the villain is not an identifiable company or an individual, none of these properties are available to us in the digital world. The internet provides attackers plausible deniability and an escape from accountability. It makes it close to impossible to identify them, let alone name and shame them. And in a society bombarded with information and increasingly reminded by the media of the risks and breaches that happen almost daily, the few stories we do tell are becoming repetitive and boring. After all, in front of the “majesty” of the Mirai DDoS attacks (Fox-Brewster 2016), or the hundreds of millions of online accounts




compromised every other week, or even in front of the massive spying infrastructure of the Five Eyes (Wikipedia 2017c), who in the public would care about an activist from the Middle East, unknown to most, being compromised by a crappy trojan (Wikipedia 2017d) bought from some dodgy website for 25 bucks?

We need to stop, take a deep breath, and look at the world around us. Are we missing the big picture? First, hackers and the media alike need to stop thinking that the most interesting or flamboyant research is the most important. When the human rights abuses of HackingTeam or FinFisher are exposed, it makes for a hell of a media story. At times, some of the research I have coauthored has landed on the front pages of major newspapers. However, those cases are exceptions, and not particularly representative of the reality of technology use as a tool for repression by a state. For every dissident targeted by sophisticated commercial spyware made by a European company, there are hundreds more infected with free-to-download or poorly written trojans that would make any security researcher yawn. Fighting the illegitimate hacking of journalists and dissidents is a never-ending cat and mouse game, and a rather technically boring one. However, once you get past the boredom of yet another DarkComet (Wikipedia 2017b) or Blackshades (Wikipedia 2017a) remote administration tool (RAT), or a four-year-old Microsoft Office exploit, you start to recognize the true value of this work: it is less technical and more human.

I have spent the last few years offering my expertise to the human rights community. And while it is deeply gratifying, it is also a mastodontic struggle. Securing global civil society is a road filled with obstacles and complications. And while it can provide unprecedented challenges to the problem-solving minds of hackers, it also comes with the toll of knowing that lives are at stake, not just some intellectual property, or some profits, or a couple of blinking boxes on a shelf.

How do you secure a distributed, dissimilar, and diverse network of people who face different risks, different adversaries, and operate in different places, with different technologies, and different services? It’s a topological nightmare. We—the security community—secure corporations and organizations with appropriate modeling, by making uniform and tightening the technology used, and by watching closely for anomalies in that model. But what we—the handful of technologists working in the human rights field—often



do is merely “recommend” one stock piece of software or another and hope it is not going to fail the person we are “helping.”

For example, I recently traveled to a West African country to meet some local journalists and activists. From my perennial checklist of technological solutionism to preach everywhere I go, I suggested to one of these activists that he encrypt his phone. Later that night, as we met for dinner, he waved his phone at me upon coming in. The display showed his Android software had failed the encryption process, and corrupted the data on his phone, despite his having followed all the appropriate steps. He looked at me and said: “I’m never going to encrypt anything ever again.” Sometimes the technology we advocate is inadequate. Sometimes it is inaccessible, or just too expensive. Sometimes it simply fails.

However, tools aside, civil society suffers a fundamental lack of awareness and understanding of the threats it faces. The missing expertise and the financial inability to access technological solutions and services that are available to the corporate world certainly isn’t making things any easier. We need to approach this problem differently, and to recognize that civil society isn’t going to secure itself.

To help, hackers and security professionals first need to become an integral part of the social struggles and movements that are very much needed in this world right now. Find a cause, help others: a local environmental organization campaigning against fracking, or a citizen journalist group exposing corruption, or a global human rights organization fighting injustice. The help of security-minded hackers could make a significant impact, first as a conscious human being, and only second as a techie, especially anywhere our expertise is so lacking.

And second, we need to band together. Security Without Borders is one effort to create a platform for like-minded people to aggregate. While it might fail in practice, it has succeeded so far in demonstrating that there are many hackers who do care. Whatever the model will be, I firmly believe that through coordinated efforts of solidarity and volunteering, we can make those changes in society that are very much needed, not for fame and fortune this time, but for that “greater good” that we all, deep down, aspire to. ■

CLAUDIO GUARNIERI, *aka Nex*, is a security researcher and human rights activist. He is a technologist at Amnesty International, a researcher with the Citizen Lab, and the co-founder of Security Without Borders.

BIBLIOGRAPHY

- Fox-Brewster, Thomas. 2016. “How Hacked Cameras are Helping Launch the Biggest Attacks the Internet Has Ever Seen.” *Forbes*, September 25. <https://www.forbes.com/sites/thomasbrewster/2016/09/25/brian-krebs-overwatch-ovh-smashed-by-largest-ddos-attacks-ever/#32d0f3c35899>
- Franceschi-Bicchierai, Lorenzo. 2016. “Hacker ‘Phineas Fisher’ Speaks on Camera for the First Time—Through a Puppet.” *Motherboard*, July 20. https://motherboard.vice.com/en_us/article/hacker-phineas-fisher-hacking-team-puppet
- Kelly, Kevin. 2010. *What Technology Wants*. New York: Viking Press.
- Wikipedia. 2017a. “Blackshades.” Wikipedia, last updated March 23. <https://en.wikipedia.org/wiki/Blackshades>
- . 2017b. “DarkComet.” Wikipedia, last updated May 14. <https://en.wikipedia.org/wiki/DarkComet>
- . 2017c. “Five Eyes.” Wikipedia, last updated April 19. https://en.wikipedia.org/wiki/Five_Eyes
- . 2017d. “Trojan horse.” Wikipedia, last updated May 12. [https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/Trojan_horse_(computing))



CAR WARS

A self-driving car is a computer you put your body in.
A fiction story by **Cory Doctorow**.

CHAPTER 1: ZERO TOLERANCE

Dear Parents,

I hate to start the year with bad news, but I'd rather it be this than a letter of condolence to a parent whose child has been killed in a senseless wreck.

As you were notified in your welcome packet, Burbank High has a zero-tolerance policy on unsafe automotive practices. We welcome healthy exploration, and our ICT program is second to none in the county, but when students undertake dangerous modifications to their cars, and bring those cars to campus, they are not only violating Board of Education policy, they're violating federal laws, and putting other students and our wider community at risk. Though the instructional year has only just started, we've already confiscated three student vehicles for operating with unlicensed firmware, and one of those cases has been referred to the police as the student involved was a repeat offender. Tomorrow, we will begin a new program of random firmware audits for all student vehicles, on- and off-campus. These are NOT OPTIONAL. We are working with Burbank PD to make these as quick and painless as possible, and you can help by discussing this important issue with your child. Burbank PD will be pulling over vehicles with student parking tokens and checking their integrity throughout the city. As always, we expect our students to be polite and respectful when interacting with law enforcement officers.

This program starts TOMORROW. Students caught with unlicensed vehicle modifications will face immediate 2-week suspensions for a first offense, and expulsion for a second offense. These are in addition to any charges that the police choose to lay.

Parents, this is your chance to talk to your kids about an incredibly serious matter that too many teens don't take seriously at all. Take the opportunity, before it's too late: for them, for you, and for the people of our community.

Thank you,

Dr Harutyunyan

CHAPTER 2: STATUS UPDATES (ON THE ROAD)

```
if you can read this call help #notajoke
seriously i don't know wtf is going on i was going home then stupid car's
emergency override kicked in
thot we were gon pull over like an ambulance or f-truck etc but we turned &
im like wtf detour?
now i'm seeing signs for lerderberg state park n theres a ton of cars around me
its like a convoy all heading to arse end of nowhere evry1 looking out of win-
dows looking scared
car sez batterys almost flat which means ill have to stop eventually i guess
but its hot out there like 40'
anyl know whats going on DM me pls #notajoke
bin tryin to call my mum 4 30m but she's not picking up
if you can reach her tell her yan said everything will be fine
mum if you see this dont worry i love you
```



ILLUSTRATION: AMISHA GADANI

CHAPTER 4: PLAUSIBLE DENIABILITY

“We’re dead.”

“Shut up Jose, we’re not dead. Be cool and hand me that USB stick. Keep your hands low. The cop can’t see us until I open the doors.”

“What about the cameras?”

“There’s a known bug that causes them to shut down when the LAN gets congested, to clear things for external cams and steering. There’s also a known bug that causes LAN traffic to spike when there’s a law-enforcement override because everything tries to snapshot itself for forensics. So the cameras are down inside. Give. Me. The. USB.”

Jose’s hand shook. I always kept the wireless jailbreaker and the stick separate — plausible deniability. The jailbreaker had legit uses, and wasn’t, in and of itself, illegal.

I plugged the USB in and mashed the panic-sequence. The first time I’d run the jailbreaker, I’d had to kill an hour while it cycled through different known vulnerabilities, looking for a way into my car’s network. It had been a nail biter, because I’d started by disabling the car’s wireless — yanking the antenna out of its mount, then putting some Faraday tape over the slot — and every minute that went by was another minute I’d have to explain if the jailbreak failed. Five minutes offline might just be transient radio noise or unclipping the antenna during a car-wash; the longer it went, the fewer stories there were that could plausibly cover the facts.

But every car has a bug or two, and the new firmware left a permanent channel open for reconnection. I could restore the car to factory defaults in 30 seconds, but that would leave me operating a vehicle that was fully un-initialized, no ride history — an obvious cover-up. The plausibility mode would restore a default firmware load, but keep a carefully edited version of the logs intact. That would take 3-5 minutes, depending.

“Step out of the vehicle please.”

“Yes sir.”

I made sure he could see my body cam, made it prominent in the field of view for his body cam, so there’d be an obvious question later, if no footage was available from my point of view. It’s all about the game theory: he knew that I knew that he knew, and other people would later know, so even though I was driving while brown, there were limits on how bad it could get.

“You too, sir.”

Jose was nervous af, showed it in every move and the whites of his eyes. No problem: every second Officer Friendly wasted on him was a second more for the plausibility script to run.

“Everything all right?”

“We’re late for class is all.” Jose was the worst liar. It was 7:55, first bell wasn’t until 8:30 and we were less than 10 minutes away from the gates.

“You both go to Burbank High?” Jose nodded. I kept my mouth shut.

“I would prefer to discuss this with an attorney present.” It was the cop’s turn to roll his eyes. He was young and white and I could see his tattoos peeking out of his collar and cuffs.

“IDs, please.”

I had already transferred my driver’s license to my shirt-pocket, so that there’d be no purse for him to peep, no chance for him to insist that he’d seen something to give him

probable cause to look further. I held it out in two fingers, and he plucked it and waved it past the reader on his belt. Jose kept his student card in a wallet bulging with everything, notes and paper money and pictures he'd printed (girls) and pictures he'd drawn (werewolves). The cop squinted at it, and I could see him trying to convince himself that one or more of those fluttering bits could be a rolling paper and hence illegal tobacco paraphernalia.

He scanned Jose's ID while Jose picked up all the things that fell out of his wallet when he removed it.

"Do you know why I stopped you?"

"I would prefer to answer any questions through my attorney." I got an A+ on my sophomore Civics term paper on privacy rights in the digital age.

"Baylea."

"Shut up, Jose."

The cop smirked. I could tell that he was thinking words like "spunky," which I hate. When you're black, female, and five-foot-nothing, you get a lot of spunky, and its ugly sister, "mouthy."

The cop went back to his car for his roadside integrity checker. Like literally every other gadget in the world, it was a rectangle a little longer and thinner than a deck of cards, but because it was cop stuff, it was ruggedized, with black and yellow rubber bumpers, because apparently being a cop makes you a klutz. I snuck a look at the chunky wind-up watch I wore, squinted through the fog of scratches on the face for the second hand. Two minutes.

Before the cop could scan the car's plates with his IC, I stepped in front of him. "May I see your warrant, please?"

Spunky turned into mouthy before my very eyes. "Step aside please miss." He eschewed commas for the sake of seriousness.

"I said I want to see your warrant."

"This type of search does not require a warrant, ma'am. It's a public safety check. Please step aside." I side-eyed my watch again, but I'd forgotten where the minute-hand had been when I started, because I'm not the coolest cucumber in the crisper. My pulse thudded in my throat. He tapped the reader-plate on the car door — we still called it the "driver door" because language is funny that way.

The car powered down with an audible thunk as the suspension relaxed into its neutral state, the car shaking a little. Then we heard its startup chime, and then another, flatter sound accompanied by three headlight blinks, three more, two more. It was booting off the cop's diagnostic tool, which would then slurp in its entire filesystem and compare its fingerprint to the list of known-good fingerprints that had been signed by both the manufacturer — Uber — and the US National Highway Traffic Safety Administration.

The transfer took a couple minutes, and, like generations before us, we struggled with the progress bar lull, surreptitiously checking each other out. Jose played particularly urgent eyeball hockey with me, trying to ascertain whether the car had been successfully reflashed before the cop checked. The cop, meanwhile, glanced from each of us to the display on his uniform's wrist to the gadget in his hand. We all heard the file-transfer complete chime, then watched as the cop tapped his screen to start the integrity check. Generating a fingerprint from the copy of the car's OS took a few seconds, while the log files would be processed by the cop cloud and sent back to Officer Friendly as a pass/fail grade. When your end-users

are nontechnical cops standing on a busy roadside, you need to make it all easier to interpret than a home pregnancy test.

The seconds oozed by. Ding! “All right then.”

All right then, I’m taking you to jail? All right then, you’re free to go? I inched toward the car, and the cop twinkled a toodle-oo at us on his fingers.

“Thank you, officer.”

Jose smelled of flop-sweat. The car booted into its factory-default config, and everything was different, from the visualizer on the windscreen to the voice with which it asked me for directions. It felt like someone else’s car, not like the sweet ride I’d bought from the Uber deadstock auction and lovingly rebuilt with junk parts and elbow grease. My own adrenaline crash hit as we pulled into traffic, the car’s signaling and lane-changes just a little less smooth than they had been a few minutes before (if you take good care of the transmission, tires and fluids, you can tweak the settings to give you a graceful glide of a ride).

“Man, I thought we were dead.”

“That was painfully obvious, Jose. You’ve got a lot of fine points, but your cool head is not one of them.” My voice cracked as I finished this. Some cool customer I was. I found a tube of coffee in the driver’s compartment and bit the end off it, then chewed the contents. Jose made pleading puppy eyes at me and I found one more, my last one, the emergency pre-pop-quiz reserve, and gave it to him as we pulled into the school lot. What are friends for?

CHAPTER 4: A REAL RIB-CREAKER

Yan’s mum had gone spare and then some when he finally made it home, leaping up from the sofa with her eyes all puffy and her mouth open and making noises like he’d never heard before.

“Mum, mum, it’s okay, I’m okay.” He said it over and over while she hugged him fiercely, squeezing him until his ribs creaked. He’d never noticed how short she was before, not until she wrapped her arms around him and he realized that he could look down on the crown of her head and see the grey coming in. He’d matched her height at 14 and they’d stopped measuring. Now at 19, he suddenly understood that his mother wasn’t young anymore — they’d celebrated her sixtieth that year, sure, but that was just a number, something to make jokes about —

She calmed down some and he was crying too by then, so he fixed them both some coffee, his mum’s favourite from the roaster in St Kilda, and they sat down at the table and drank coffee while they snotted and cried themselves dry. It had been a long walk back, and he’d been by no means the only one slogging down a freeway for ages, lost without mobile service and maps, trying to find someone with a live battery he could beg for a navigational check.

“All my feeds are full of it, it’s horrible. Hundreds of people smashed into each other, into the railing or run off the freeway. I thought —”

“I know Mum, but I was okay. The bloody car ran out of juice and just stopped. Rolled to a stop, got a little bump from the fella behind me, then his car swerved around me and took off like blazes. Poor bugger, looked terrified. I had to get out and walk.”

“Why didn’t you call?”

“Flat battery. Flat battery in the car, too. Same as everyone. I plugged my phone in soon as I sat down, right, but I think the car was actually draining my battery, cos everyone else I

met walking back had the same problem.”

She contemplated Yan for a moment, trying to figure out whether she was upset or relieved, plumped for relieved, set down her coffee and gave him another one of those hugs that made him gasp for air.

“I love you, Mum.”

“Oh, my boy, I love you too. God, what’s going on, hey?”

CHAPTER 5: REVOLUTION, AGAIN

There was another revolution so all our fourth period classes were canceled and instead we were put into tiger teams and sent around the school to research everything we could find about Syria and present it to another group in one hour, then the merged groups had to present to two more teams, and so on, until we all gathered in the auditorium for final period.

Syria is a mess, let me tell you. My rule of thumb for easy credit on these world affairs real-time assignments is to look for Wikipedia articles with a lot of [citation needed] flags, read the arguments over these disputed facts, then fill in the footnotes with some quick googling. Being someone who didn’t actually give a damn about the issue let me figure out which citations would be acceptable to all the people calling each other monsters for disagreeing about it.

Teachers loved this, couldn’t stop praising me for my “contributions to the living record on the subject” and “making resources better for everyone.” But the Syria entry was longer than long, and the disputed facts had no easy resolution — was the government called ISIL? ISIS? IS? What did Da’esh even mean? It had all been a big mess back when I was in kindergarten, and then it had settled down... Until now. There were tons of Syrian kids in my class, of course, and I knew they were like the Armenian kids, super-pissed about something I didn’t really understand in a country a long way away, but I’m an American, which means that I didn’t really pay attention to any country we weren’t at war with.

Then came the car thing. Just like that one in Australia, except this wasn’t random terrorists killing anyone they could get their hands on — this was a government, and we all watched the livestreams as the molotov-chucking terrorists or revolutionaries or whatever in the streets of Damascus were chased through the streets by the cars that the government had taken over, some of them — most of them! — with horrified people trapped inside, pounding on the emergency brakes as their cars ran down the people in the street, spattering the windcreens with blood.

Some of the cars were the new ones with the sticky stuff on the hood that kept the people they ran down from being thrown clear or tossed under the wheels — instead, they stuck fast and screamed as the cars tore down the narrow streets. It was the kind of thing that you needed a special note from your parents to get to see in social studies, and luckily my moms is cool like that. Or unlucky, because nightmares, but better to be woke than asleep. It’s real, so it’s something I need to know about.

CHAPTER 6: WE'RE ARTISTS, NOT PROGRAMMERS.

Huawei's machine-learning division thought of themselves as artists more than programmers. That was the first slide in their deck, the one the recruiters showed at the big job-fairs at Stanford and Ben-Gurion and IIT. It was what the ML people said to each other, so repeating it back to them was just good tactics.

When you worked for Huawei, you got access to the firehose: every scrap of telemetry ever gleaned by a Huawei vehicle, plus all the licensed data-sets from the other big automotive and logistics companies, right down to the driver-data collected from people who wore court-ordered monitors: paroled felons, abusive parents under restraining orders, government employees. You got the post-mortem data from the world's worst crashes, you got all the simulation data from the botcaves: the vast, virtual killing-field where the machine-learning algorithms duked it out to see which one could generate the fewest fatalities per kilometer.

But it took a week for Samuel to get the data from the mass hijackings in Melbourne and Damascus. It was all national-security-ied up the arse of course, of course, but Huawei was a critical infrastructure partner of the Seven Eyes nations, and Samuel kept his clearances up with the four countries where he had direct-line reports working in security.

Without that data, he was left trying to recreate the attack through the Sherlock method: abductive reasoning, where you start with a known outcome and then come up with the simplest possible theory to cover the facts. When you have excluded the impossible, whatever remains, however improbable, must be the truth. If only that was true! The thing that never happened to Sherlock, and always happened to machine learning hackers, was that they excluded the impossible and then simply couldn't think of the true cause — not until it was too late.

For the people in Damascus, it was too late. For the people in Melbourne, it was too late. No pressure, Samuel.

Machine learning always started with data. The algorithm ingested the data, crunched it, and spat out a model, which you could test by feeding it some of the data you'd held back from the training set. Feed it 90 percent of the traffic info you had, ask it to model responses to different traffic circumstances, then test the model in the reserved set to see if it could correctly — that is, nonfatally — navigate the remaining traffic.

Data could be wrong in many ways. It was always incomplete, and whatever was left out could bias the model. Samuel always explained this to visiting school groups by inviting them to imagine training a model to predict height from weight by feeding it data from a Year Three class. It didn't take the kids long to get how that might not produce good estimates for the height of adults, but the kicker was when he revealed that any Third Years who wasn't happy about their weight could opt out of getting on the scales. "The problem isn't the algorithm, it's the data used to make the model." Even a school-kid could get that.

But it was more complicated than just biased data. There were also the special cases: what to do if an emergency vehicle's siren was sensed (because not all emergency vehicles could transmit the lawful interception overrides that would send all traffic to the kerb lanes), what to do if a large ruminant (a deer, a cow, even a zebra, because Huawei sold cars all over the world) stepped into the car's path, and so on. In theory, there was no reason not to use machine learning to train this too — just tell the algorithm to select for behaviours that resulted

in the shortest journeys for simulated emergency vehicles. After all, there would always be circumstances when it was quicker for vehicles to drive a little further before pulling over, to prevent congestion, and the best way to discover those was to mine the data and run the simulations.

Regulators did not approve of this: nondeterministic, “artistic” programming was a cute trick, but it was no substitute for the hard and fast binary logic of law: when this happens, you do that. No exceptions.

So the special cases multiplied, because they were like crisps, impossible to stop at just one. After all, governments already understood how special cases could be policy instruments.

Special cases were how pirate sites and child porn were excluded from search-results, how sensitive military installations were excluded from satellite photos in mapping apps, how software defined radios stayed clear of emergency bands when they were hunting for interference-free channels. Every one of those special cases was an opportunity for mischief, since so many of them were secret by definition — no one wanted to publish the world’s most comprehensive directory of online child porn, even if it was supposed to serve as a blacklist — so the special case bucket quickly filled up with everything that some influential person, somewhere, wanted. From gambling and assisted suicide sites being snuck into the child-porn list to anti-Kremlin videos being added to the copyright filters, to all the “accident-prevention” stuff in the cars.

Since 1967, ethicists had been asking hypothetical problems about who should be killed by runaway trolleys: whether it was better to push a fat man onto the tracks (because his mass would stop the trolley) or let it crash into a crowd of bystanders, whether it made a difference if the sacrificial lamb was a good person or a bad one, or whether the alternative fatalities would be kids, or terminally ill people, or...

The advent of autonomous vehicles was a bonanza for people who liked this kind of thought-experiment: if your car sensed that it was about to get into an accident, should it spare you or others? Governments convened secret round-tables to ponder the question and even come up with ranked lists: saving three children in the car topped saving four children on the street, but three adults would be sacrificed to save two kids. It was a harmless and even cute diversion at first, and it gave people something smart-sounding to say at lectures and cocktail parties.

But outside the actual software design teams, no one asked the important question: if you were going to design a car that specifically tried to kill its owners from time to time, how could you stop those owners from reconfiguring those cars to never kill them?

But Samuel had been in those meetings, where half-bright people from the old-line automotive companies reassured quarter-bright bureaucrats from the transport ministries that there’d be no problem designing “tamper-proof” cars that would “resist end-user modification.” Meanwhile, much brighter sorts from the law-enforcement side of the house licked their chops and rubbed their hands together at all the non-trolley problems that could be solved if cars could be designed to do certain things when they got signals from duly authorised parties. Especially if the manufacturers and courts would collaborate to keep the inventory of those special cases as secret as the child-porn blocklists on the national firewalls.

He’d been in the design sessions after, where they debated how they’d hide the threads and files for those programs, how they’d tweak the car’s boot-cycle to detect tampering and

alert the authorities, how the diagnostic tools provided to mechanics for routine service-checks could be used to double-check the integrity of all systems.

But then he'd started getting signed, obfuscated blobs from contractors who served governments around the world, developing "emergency priority" apps he was just supposed to drop in, without inspecting them. Of course he ran unit-tests before Huawei shipped updates, and when they inevitably broke the build, Samuel would go around and around with the contractors, who'd want access to all his source code without letting him see any of theirs.

It made sense for them to behave that way. If he failed to help them get their code into Huawei's fleet, he'd have to answer to governments around the world. If they failed to help him, they'd have to answer to precisely no one.

Unit-tests were one thing, real-world performance was something else. Sensors couldn't tell a car whether it was about to crash into some pedestrians, or a school bus, or an articulated lorry full of dynamite. All sensors could do was sense, and then feed data to machine-learning systems that tried to draw conclusions from those data. Even with all the special cases about what the car must and must not do under which circumstances, machine learning systems were how it knew what the circumstances were.

That's how Melbourne happened.

It had taken him a long time to figure this out. At first, he assumed that finally, the worst had come to pass: the cryptographic keys that were used to sign police override equipment had leaked, and the wily criminals had used them to hijack 45 percent of the cars on the roads of one of the biggest cities in Australia. But the forensics didn't show that at all.

Rather, the crooks had figured out how to spoof the models that invoked the special cases. Samuel figured this out by accident, his third day at his desk, running sim after sim on Huawei's high-confidentiality cloud, which was protocol, even though it was the slowest and least-provisioned cloud he could have used. But it was only available to a handful of senior internal Huawei groups, not even contractors or partners.

He'd been running the raw telemetry from a random sample of the affected cars looking for anomalous behaviour. He'd nearly missed it, even so. In St Kilda, someone — face in shadow beneath a hat, thermal profile obscured — stepped in front of a subject car, which slowed, but did not brake, and emitted two quick horn-taps.

Regression analysis on accident data had shown that hard braking was more likely to result in rear-end collisions and frozen pedestrians who couldn't get out of the way. The cartasked more compute time to the dorsal perimeter to see if it could shift into an adjacent lane without a collision, and if that wasn't possible, to estimate the number of affected vehicles and passengers based on different maneuvers.

The pedestrian fainted towards the car, which triggered another model, the "suicide by car" system, which invoked a detailed assessment of the pedestrian, looking for clues about sobriety, mental health and mood, all of which were difficult to ascertain thanks to the facial obfuscation. But there were other signals, a mental health crisis clinic 350 metres away, six establishments licensed for serving or selling alcohol with 100 metres, the number of redundancies in the past quarter, that gave it a high weighted score.

It initiated hard braking, and the pedestrian leapt back with surprising nimbleness. Then, across the road, another pedestrian repeated the dance, with another car, again in a

shadowing hat and thermal dazzle makeup.

The car noticed this, and that triggered another model, which some analyst had labeled “shenanigans.” Someone was playing silly buggers with the cars, which was not without precedent, and well within the range of contingencies that could be managed. Alertness rippled through the nearby cars, and they began exchanging information on the pedestrians in the area: gait profiles, silhouettes, unique radio identifiers from Bluetooth devices. Police were notified, and the city-wide traffic patterns rippled, too, as emergency vehicles started slicing through the grid while cars pulled over.

All these exceptions to the norm were putting peak load on the car’s internal network and processors, which were not designed to continue operating when crises were underway — freeze-and-wait being the optimal strategy that the models had arrived at.

But before the car could start hunting for a place to pull in until the law arrived, it got word that there was another instance of shenanigans, a couple roads down, and the police would need a clear path to reach that spot, so the car had best keep moving lest it create congestion. The cars around it had come to similar conclusions, and were similarly running out of processor overhead, so they fell into mule-train formation, using each others’ perimeters as wayfinding points, turning their sensors into a tightly-coupled literal grid that crept along with palpable machine anxiety.

Here’s where it got really interesting, because the attackers had forced a situation where, in order to keep from blocking off the emergency vehicles behind them, these cars had completely shut down the road and made it impossible to overtake them. This increased the urgency of the get-out-the-way messages the city grid was sending, which tasked more and more of the cars’ intelligence and sensors to trying to solve the insoluble problem.

Gradually, through blind variation, the cars hivemind discovered that the faster the formation drove, the more it could satisfy the overriding instructions to clear things.

That was how 45 percent of Melbourne’s vehicles ended up in tight, high speed formation, racing for the city limits as the emergency vehicles behind them spurred them on like sheepdogs, while frantic human planners tried to figure out exactly what was going on and how to stop it.

Eventually, the sheer quantity of compromised vehicles, combined with the minute variations in lane-spacing, small differences in car handling characteristics and, finally, a blown tyre, led to a pile up of ghastly proportions, a crash that they would study for decades to come, that would come to stand in for the very worst that people could do.

Samuel had always said that machine learning was an art, not a science, that the artists who designed the models needed to be able to work without official interference. He’d always said it would come to a bad end. Some of those meetings had ended in shouting matches, Samuel leaning over the table, shouting at bureaucrats, shouting at his bosses, even, in a way that would have horrified his parents in Lagos, where jobs like Samuel’s were like lottery jackpots, and shouting like his was an unthinkable act of economic suicide.

But he’d shouted and raged and told them that the fact that they wished that there was a way to put a back-door in a car that a bad guy couldn’t exploit didn’t mean that there was a way to do it.

He’d lost. If Samuel wanted to argue for a living, he’d have been a lawyer, not an algorithm whisperer.

Now he was vindicated. The bad ideas baked into whole nations' worth of infrastructure were now ready to eat, and they would be a feast that would never end.

If this is what victory felt like, you could keep it. Elsewhere in the world, there were other Samuels, poring over their own teams' reports: GM, VW-Newscorp, Toyotaford, Yugo. He'd met some of those people, even tried to recruit a few of them. They were as smart as Samuel or smarter, and they'd certainly shouted as loudly as he had when the time had come. Enough to satisfy their honor, before capitulating to the unstoppable force of non-technical certitude about deeply technical subjects. The conviction that once the lawyers had come up with the answer, it was the engineers' job to implement it, not trouble them with tedious technical wheedles about what was and wasn't possible.

CHAPTER 7: GRAND THEFT AUTO

Burbank High had a hard no-phones policy: it was a zero tolerance expulsion offense to step over the property line with a phone that hadn't been apped to reject unapproved packets. It made the school day into a weird kind of news vacuum. There was the day that I'd emerged from fourth period and stepped across the threshold to discover that the governor had been shot by Central Valley separatists and the whole state had gone bananas, seeing water-warriors behind every potted plant and reporting every unexplained parcel as a potential bomb.

You never get used to that feeling of emerging from a news-free zone and into a real world that's been utterly transformed while you were blissfully unaware. But you do get better at recognizing it.

When the final bell rang 3,000 students (me included) poured out of the school doors, it was obvious that there was something wrong. The streets were empty, missing the traffic that hummed along Third Street with perfect, orderly following distance. That was the first thing we noticed. It was only after a second of gawping at the empty road that everyone turned their attention to the parking lots, the small faculty lot and the sprawling student lot, and realized, in unison, that all the cars had gone missing, every single one.

As they pushed out of the doors and toward the lot, I saw that it wasn't quite all the cars that had driven themselves away while we'd been good little students at our lessons.

One car remained.

As in a dream, I pulled out my phone and fingerprinted it into wakefulness, sent the car its unlock signal. The car, alone in the vast lot, blinked its headlights and came to attention on its suspension. Gradually, the students turned to look at me, then my car, then back at me, first crowding around, then opening a path between me and that stupid little Uber hatchback, unlovely and lonely in the field of tarmac. They watched me as I drifted towards it, opened the door, tossed in my school bag, and slid into the front seat. The car, running my rambunctious, forbidden software, started itself with a set of mechanical noises and vibrations, then backed smoothly out of the lot, giving the humans around it a cautious berth, sliding onto the empty roads, and aiming towards home.

I was sure I'd be pulled over — the only car on the road, what could be more suspicious — but I didn't pass a single cop car. Dialing into the news, I watched — along with the rest of the world — as every car in the San Fernando Valley formed a fast-moving migratory herd that sped toward the Angeles National Forest, which was already engulfed in the wildfires

from the crashed cars that had gone over the cliff-edged winding roads.

The cops were apparently a little busy, just then.

CHAPTER 8: EVERY TIME. NO EXCEPTIONS

It was Yan's mum who found the darknet site with the firmware fiddler image, though Yan had to help her getting it installed on a thumbdrive. They made two, one for each of them, and clipped them to their phones, with the plausible deniability partitions the distributor recommended.

The lecture she gave Yan about using it every single time, no matter whether he was in a friend's car or a auto-taxi was as solemn as the birth-control lecture she'd given him on his fourteenth birthday.

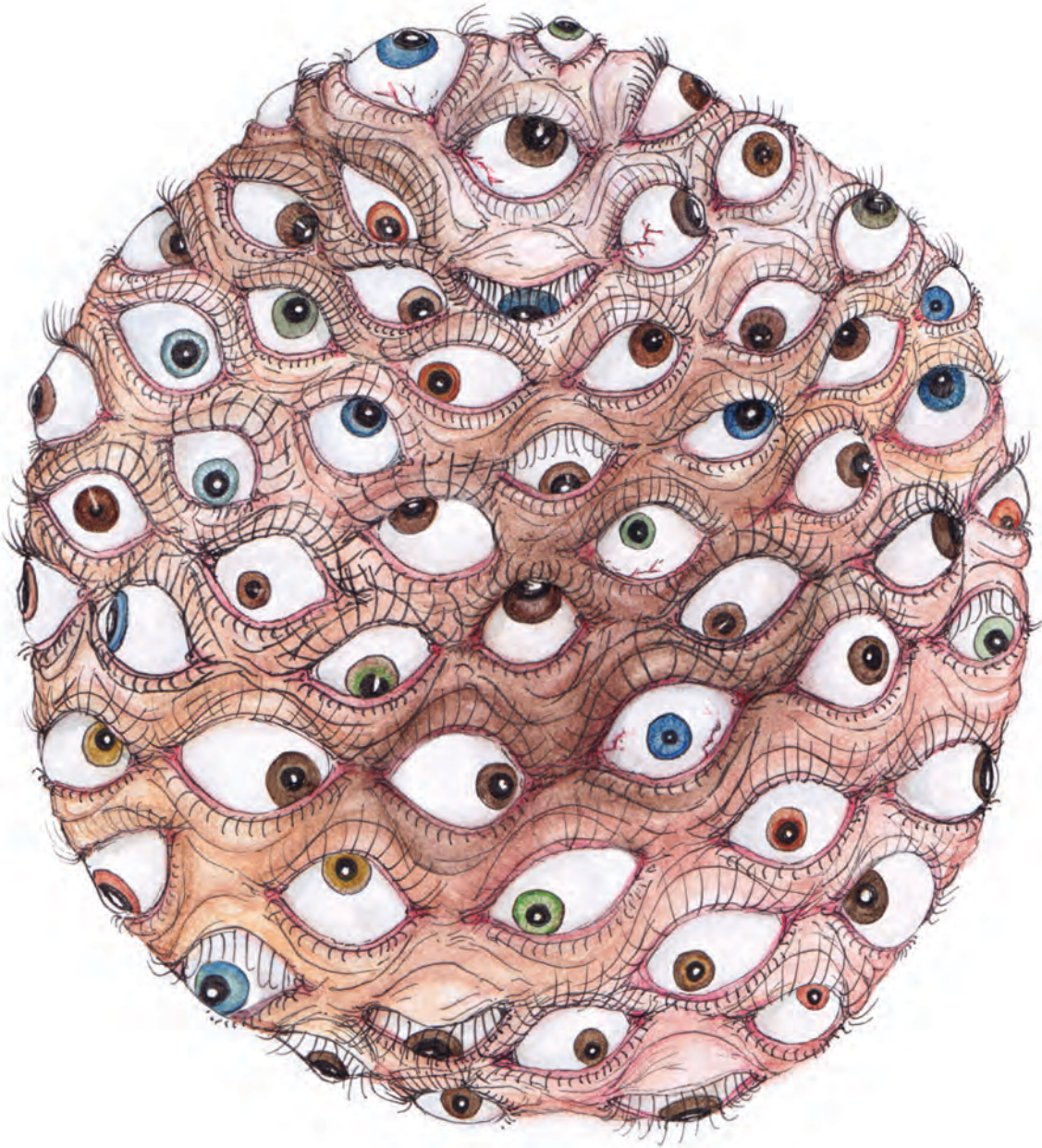
"If the alternative is walking all night, then you will walk, my boy. I want you to promise."

"I promise, Mum."

She hugged him so fiercely it made his ribs creak, squeezing his promise into his bones. He hugged her back, mindful of her fragility, but then realised he was crying for no reason, and then for a good reason, because he'd nearly died, hadn't he?

Jailbreaking a car had real legal risks, but he'd take his chances with those, considering the alternative.

This piece was originally commissioned by Deakin University.



<http://limn.it/>