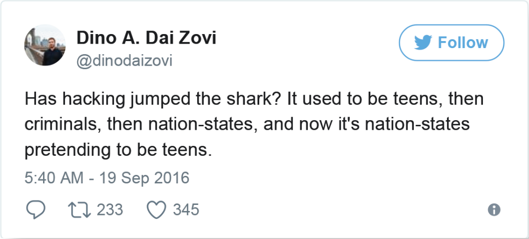
Preface

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:



Has hacking jumped the shark? It used to be teens, then criminals, then nation-states, and now it's nation-states pretending to be teens.

5:40 AM - 19 Sep 2016

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 Tocchetti (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 "cypherpunks" 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 hactivists 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.

limn is published as needed. Issue #8 is edited by **E. Gabriella Coleman** and **Christopher M. Kelty**. This issue is set using Christian Schwartz' Graphik, Dino dos Santos' Leitura and Velino Poster, and Hoefler & Co.'s Whitney typefaces. Layout by **Martin Hoyem/American Ethnography.** The General Editors of Limn are **Stephen J. Collier, Christopher M. Kelty,** and **Andrew Lakoff.**

Publication assistance provided by the Wolfe Chair in Scientific and Technological LIteracy at McGill University and the Institute for Society and Genetics at UCLA. More at http://limn.it/

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.

ILLUSTRATION: AMISHA GADANI

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.