State Hacking at the Edge of Code, Capitalism and Culture

Luca Follis and Adam Fish

Hacking is a set of practices with code that provides the state an opportunity to defend and expand itself onto the internet. Bringing together science and technology studies and sociology scholarship on boundary objects and boundary work, we develop a theory of the practices of the hacker state. To do this, we investigate weaponized code, the state's boundary work at hacker conferences, and bug bounty programs. In the process, we offer a depiction of the hacker state as aggressive, networked, and adaptive.

Keywords:

Hacker, hacking, state, boundary object, boundary work

The Hacker State: Entities, Objects, and Work

The contemporary networked state is dynamic and process-orientated. It is a logistical and informational assemblage composed of technological infrastructures like 4G networks, surveillance satellites, internet exchange points and fiber optic cables as well as official bureaus concerned with areas like law enforcement, environmental protection, national security and diplomacy. These domains of competence and action are populated by researchers and scientists, police officers and policy analysts, military contractors and covert operatives—that is, an assortment of humans with differing mandates, levels of agency, expertise and proximity to official structures and objectives. This circuitry of power is increasingly underwritten and interwoven with the nonhuman components of the networked age. Software and malware, algorithms, viruses, exploits and zero-days increasingly form a connective tissue that links these state actors.

This dynamic constellation of state structures seems to be historically and empirically distinctive from the more static characterizations that have appeared and continue to appear in the sociology of the state. Indeed, besides the formal exchanges and encounters that are typically understood as the domain of the state (e.g., diplomacy, treaty negotiation, foreign policy, etc.), a set of less formal and more tenuous forms of engagement—mediated through software, conducted through cyber-proxies and governed by networks—have increasingly complemented the "work" of the state. In this article, we map these less formal encounters by combining science and technology studies (STS) with cultural accounts of state forms, drawn from recent work in political sociology. We integrate these two traditions into an account of how hacking technologies function as a resource for the exercise of state power.

We develop a theory of state boundary work that draws on and contributes to STS theories of boundary objects but also political sociological theories that emphasize that state acts of cultural production (most notably the very idea of the state) are preeminently boundary-drawing exercises. Within STS, these concepts are often theorized in terms of the encounters, translations, and collaborations that emerge between one domain—the methodologies of physical, computer, natural or otherwise "hard" sciences—and another, usually the public (Gieryn 1983, Star 1989) or the social sciences (Ribes 2018).

Within political sociology, these concepts developed in the context of a critique of "state" theory that views the state as bounded, unitary and set apart from a social reality upon which it acts (Abrams 1988, Migdal & Schlichte 2005). Cultural approaches to the state focus on how officials and agencies help construct the "idea" or representation of the state through drawing distinctions (e.g., state/society) and manipulating boundaries (e.g., criminal/legal) (Mitchell 1991, Carrol 2009). Thus, STS and sociological scholarship provides a useful departure point for the application of boundary work theories to the activities of the networked state, its mechanisms for the disposition of hacking technologies, as well as its relationship to the figure of the hacker.

In what follows, we conceptualize the relationship between the state and the hacker in terms of the three phenomena: entities, objects, and work. There exist multidimensional entities such as the state and hackers, objects such as hacker software, and work such as hacking and recruitment that mediate the relationship between states and hackers. Together, the state, hackers, their software, and converging practices constitute a new domain of action.

Entities

State forms and hackers share an "elective affinity"—a concept used by Max Weber (1992) to describe the relationship between Protestant asceticism and the development of capitalism. David Ribes (2018) draws on this concept to illustrate how STS and state-supported data sciences mutually reinforce one another through sharing concepts, learning from each other, and developing theories to make sense of the relationship between data and society. In Ribes' discussion of data science we see a state agency—in this case the USA's National Science Foundation (NSF)—bring sociologists of technology into collaboration with scientists. This is a mutually beneficial enterprise: the scientists appropriate STS concepts and methodologies while the sociologists gain access to valuable field sites and datasets. The former group is compelled to think critically and reflexively about the meaning and impact of their work, while the latter is obliged to explore how well their theorizations fit with actual scientific practice.

In contrast, the relationship between the state and hackers is generally framed in terms of mutual distrust and antagonism. In popular culture, hackers frequently appear as criminal 'savants,' (Steinmetz 2016) technological wizards with subversive intentions and broad ranging powers over computers. This cultural portrayal of hackers has also been buoyed by a decade of high visibility: not only the actions and operations of groups like Anonymous, but also the revelations of Edward Snowden, the document and code dumps of WikiLeaks and the Russian hack of the 2016 US Presidential election. Such a situation inevitably frames hackers as a national security and law enforcement problem that must be managed through criminalization.

Yet the association between state agencies and hackers can also be described in less oppositional terms, much like the collaborative relationships between the NSF and STS scholars sketched above. Historically, state agencies supported the incubation of hacking and its development: hacking was central to the process of developing programming languages and different iterations of mainframe computing, it animated the first government built internet infrastructures, and shaped the geek culture around which the first computer science programs at Department of Defense sponsored research universities developed (Levy 2010). State bureaus like DARPA (Defense Advanced Research Project Agency) funded much of this early work by developing research networks and material infrastructure, as well as providing employment and grants for further technological development. Thus hacking played an important and long-running role in the technical side of statecraft even though its broad deployment as an attack technology is relatively novel.

Hackers are entangled in relationships of proximity and distance with state structures. That is, in some areas of the state, hacking and hacktivism appear as a manifestation of new disruptive illegalities connected with the advent of networked technology. Yet in others (e.g., national security or the military), hacking and hackers appear not as a problem to be overcome but as transformative resources that can be harnessed for strategic or tactical advantage. The horizons and borders of state/hacker interactions are not fixed but fluid, unstable and increasingly mobile. Finally, given that state structures are relatively formal and that logistical coordination is a core state organizational resource, governance strategies "seed", "task," "recruit" and otherwise organize hacking as a resource (Fish, Murillo, Nguyen, Panofsky & Kelty 2011) to navigate the terrain between these two points. In the next section, we focus on how these proximate relationships, this sharing of practices, are anchored by boundary objects like weaponized code.

Objects

The relationship between hackers and the state is mediated through objects such as software and computer code. Susan Leigh Star (Bowker & Star 1999; Star 1988, 2010; Star & Griesemer 1989) developed the boundary object model to describe how things provide opportunities for different groups to collaborate without consensus (Centellas, Smardon & Fifield 2014). Boundary objects have "interpretive flexibility": they are positioned in the middle of groups of actors that possess different viewpoints (Star 1989: 46) and involve a "process of tacking back-and-forth between the ill-structured and well-structured aspects of arrangements" (Star 2010: 601). According to Star, a boundary object can be understood in "both its computer science and pragmatic senses." That is, it is a "thing" that people and other "things," objects or programs "act toward and with" (Star 2010: 603). As such, it is useful for understanding how some objects of computer science—in our case a weaponized suite of penetration testing software—sit at the boundary between different social worlds (e.g., the state, corporate ethical hackers, cybercriminals, and hacktivists), structure a set of dynamic work arrangements, and sometimes permit a form of boundary crossing we label "boundary work".

Patrick Carroll's (2012) discussion of boundary objects further illustrates how this model can intersect with the analysis of the state. Carroll argues that the multiple ways that California came to understand and grapple with the "water problem" formed a core dynamic in the development of its techno-scientific state. Water functioned as a boundary object that helped network the domains of governance and science, it occupied a key position of contact between these distinct areas of institutional practice and generated novel discourses, organizational forms and material structures. In the process, it also wove the domain of governance and science more tightly together.

Our view is that hacking can be understood in terms analogous to Carroll's reading of the Californian "water problem": it sits at the boundary of a host of institutional infrastructures and domains. For example, hacking is the subject of state criminalization campaigns but also an object of significant recruitment activity in both corporate and government sectors. It is increasingly a core resource for the projection of state power but also an enduring vulnerability in the area of public safety or law enforcement. Much like water, hacking has become an important contact point between disparate domains that has spurred novel state assemblages formed at the intersection of organizations, discourses, and material infrastructures.

Yet what we want to focus on in this article is the boundary-spanning (Gasson 2006) properties of hacking objects themselves. Penetration testing toolkits are “repositories” (i.e., modular and indexable) of code and software which are developed in an open source tradition. Much as in Star’s discussion of “tacking back and forth,” these “toolkits” or penetration objects are open to various forms of “structuration” (Star 2010: 615) as in when state hacking groups like the National Security Agency (NSA) customize them for offensive campaigns, when they are compiled into software suites by ethical hackers who use them to test the cybersecurity of states, banks, and corporations, as well as when they are used by cybercriminals and politically motivated hacktivists to find and release information. In this sense, the objects produced in each of these “translations” illustrate the point that shaping or constructing such objects involves the exercise of power and that such a process need not be consensual or collaborative: it can also be unilateral (Boland and Tenkasi 1995; Huvila 2011). As Star notes, such objects exist “between worlds (or communities of practice) where it is ill structured” (Star 2010: 604). Finally, given that the code and the exploits contained in these toolkits are mobile they not only move across different communities of practitioners with sometimes very different ideologies, they also transect, impact and link a score of organizations and institutions far removed from the everyday “practice” of cyber security.

Work

Hacker/state practices can also be understood in terms of work, namely, work expanding a boundary. STS scholarship on boundary work begins with Thomas Gieryn’s (1983) analysis of the rhetorical strategies mobilized by scientists to demarcate science from other knowledge-producing activities. According to Gieryn, the promotion of scientific ideology via the discursive construction of social boundaries (i.e., boundary work) between it and other “non-scientific” knowledge producing occupations serves to carve out a field of professional autonomy for its practitioners, as well as to enlarge the material and symbolic resources that scientists could lay claim to. The public rhetorical style of these practitioners shifted depending on whether the aim was to: expand into domains of activity already claimed by other professionals (flattery), to monopolize professional authority and resources in its self-defined field of activity (exclusion) or to protect the authority of scientists from incursions from other knowledge-producing fields (scapegoating) (1983: 791-792).

Gieryn's wider point is that boundary work is a more generic facet of the social processes involved in "professionalization" and that such strategies proliferate in economic and social organization. Cultural sociologists have long argued that a similar, though simplified, process is at work in the criminalization of deviance. Here, moral entrepreneurs rhetorically marshal public anxieties concerning structural change and social transformation into campaigns against social deviants or "folk devils" (Cohen 1980, Ben-Yehuda 1986) to reaffirm and maintain moral and symbolic boundaries at a time when they are perceived to be in flux.

Finally, sociologists of the state also focused on boundary work through deconstructing a preeminent site of boundary making in contemporary society, the state. These scholars emphasized the extent to which the entire state idea can be understood as an act of ideological projection (Mitchell 1991; Migdal 2001; Carroll 2001) wherein the state gains substance by defining itself as a singular, unitary and bounded entity set apart from a society it governs. Much as in the case of Gieryn's scientists, states claim autonomy and authority over their bounded domains, monopolize symbolic and material resources to further their control, and expand their authority into other fields by strategically valorizing, repositioning or erasing borders. The state is an assemblage, an ideological composite of multiple bureaus and domains of governance, and so boundary practices are as much about staging the exteriority of the state (that is, identifying its outer, societal edge) as they are about defining its interiority: boundary practices shape how chains of authority are arranged as well as structure the logistics and coordination that goes on between them (Maryl & Quinn 2016).

The three versions of boundary work sketched above posit that erecting, crossing and resituating boundaries is a central facet of how organizational authority functions and reproduces itself. Boundary work is a core resource for delineating and maintaining a field of action and authority, but the flexibility and mobility of boundaries is also important in the context of navigating between countervailing imperatives. Earlier we noted that a characterization of the relationship between hackers/hacking and state agencies shifts depending on the imperatives that dominate the field in question (e.g., law enforcement vs. defense department contracts). In what follows, we argue that state agencies mobilize "boundary work" to smooth the inconsistencies between these and other similarly divergent positions: these strategies bring certain hacking practices and hackers closer to state forms while selectively keeping others at arm's length.

The process by which hackers are recruited and employed by the state is an important example of the tensions of proximity. We briefly describe the United Arab Emirates and the weaponized code Pegasus to illustrate how the state hacker domain is constructed through the complex entanglements generated at the intersection of software objects and work-related activity.

Pegasus

Once installed, Pegasus collects all signals intelligence generated by a phone: voice, emails, texts, location data, messages sent on Facebook, Skype, and WhatsApp—uploading updates to command and control servers. It was developed by the Israeli cyber security firm NSO and was first used by Mexico's government to track a wide range of targets including suspected members of drug cartels, journalists, government critics, investigators looking into the mysterious disappearance of 43 students, and supporters of a tax on soda (Scott-Railton, Marczak, Guarnieri & Crete-Nishihata 2017). The most famous use of the software was against Joaquín Archivaldo Guzmán Loera, a man better known as El Chapo, by the Mexican government. Bahrain, Kazakhstan, Morocco, Saudi Arabia, and the United Arab Emirates also use the hacker software (Marczak 2018). For example, Saud al-Qahtani, a lead adviser to the Crown Prince of Saudi Arabia used Pegasus to track the murdered journalist Jamal Khashoggi (Kirkpatrick 2018) and target the iPhone of Emirati human rights activist, Ahmed Mansoor (Marczak & Scott-Railton 2016).

Mansoor was also targeted by another UAE based hacking firm, DarkMatter, which hacked his child's baby monitor to eavesdrop on him and his family. DarkMatter's offices are located in the same building that houses the U.A.E.'s Signals Intelligence Agency, the Emirates' version of the NSA. Yet if DarkMatter is effectively an arm of the UAE state, as *New York Times* reporting claims, then the US is its body (Mazzetti, Goldman, Bergman & Perlroth 2019). DarkMatter's drill sessions are modelled on the CIA's training regime and are led by CAGN Global, an American intelligence company. The latter is funded by the US State Department and licensed by the US government to export its hacking services (McLaughin 2017).

DarkMatter was created when employees from another US State Department sanctioned firm in the UAE, Cyberpoint, raised questions about the increasingly offensive hacking practices pursued by the state (Bing & Schectman 2019). In response, UAE officials founded DarkMatter, hired willing Cyberpoint personnel and recruited security specialists from the U.S. government (i.e., the NSA, CIA and Pentagon) and technology companies (from Google, Qualcomm, McAfee, and Samsung). They presented at security conferences like the RSA summit and sponsored major hacking conferences like Black Hat USA (McLaughlin 2016). Mansoor was targeted with software called Karma, a tool not unlike Pegasus. Once installed through following a malicious link, Karma relayed the phone's information, location and functions to a UAE hacker. Mansoor was convicted in 2017 in the UAE for making Facebook and Twitter posts critical of the regime and sentenced to 10 years in jail, where he remains today (Bing & Schectman 2019).

Hacker tools such as Pegasus and Karma are boundary objects that anchor and thicken the relationships between firms like DarkMatter and other state supported security firms. These boundary workers often share recruitment pools and training practices, they attend and sponsor hacking conferences, and their incursions feed both the lucrative market in vulnerabilities and zero-days as well as fuel the recent expansion of crowd-sourced vulnerability disclosure programs, or bug bounty programs.

In what follows, we describe the state's expansion into the field of grey and black hat hacking through recruitment drives at cybersecurity conferences like Black Hat USA and DEF CON, alongside more variegated practices of crowd-sourced cyber security such as the adoption of bug bounty programs and penetration testing hack-a-thons to harness hacker skill sets while keeping them at-a-distance. Finally, we argue that boundary work practices are anchored by and furthered through software and code objects that sit on the threshold of these diverse fields of action. Boundary objects like Metasploit and other "dual use" penetration testing platforms map onto the very inconsistent and divergent positions alluded to above and make possible strategic movement between fields as well as unexpected collaborations.

Metasploit, a Hacker tool, as a Boundary Object[1]

Internet lore says that the term "ethical hacking" was coined by former IBM Vice President John Patrick in 1995. Patrick used the term to describe the professional practice of penetrating and testing a computer system for vulnerabilities at a time when the cultural

[1] The material in this and the following section draws in part on fieldwork the authors performed in a hands-on hacking workshop on ethical hacking in Manchester, UK during 2017 and at DEF CON 25 (2017).

framing of hackers as a dangerous new criminal class dominated news headlines (Sterling 1992). The use of the term "ethical" much like the terms "white", "black" and "grey" to describe hacking is a discursive strategy in Gieryn's sense, adopted to construct difference and carve out a zone of authority between a set of practices situated at the threshold of multiple boundaries. The very practices ethical hackers adopt are (from the point of view of a computer system that is being tested) indistinguishable from the practices of a malicious intruder. Indeed the emphasis in ethical hacking manuals and workshops on legal liability and professional norms illustrate the extent to which offensive security frequently plays at the margins of legality and professional ethics (in this sense, ethical hackers might be understood as quintessential boundary workers).

The liminal position of the ethical hacker is largely defined by their methodological approach and the package of software tools used to penetrate and test a system. In 1989 Daniel Farmer developed what has been credited as one of the first such toolkits: COPS (Computer Oracle and Password System) which was designed to scan for security vulnerabilities in the UNIX operating system. Four years later Farmer and his colleague, Wietse Venema, laid out the core principles of offensive security in a widely circulated paper entitled: "Improving the Security of Your Site by Breaking into It". The article developed a practical methodology to teach network administrators a new way of thinking about the security of their system and how to probe it for weaknesses:

> The purpose of this paper is to try to get the reader to look at her or his system in a new way—one that will hopefully afford him or her the opportunity to_understand_how their system can be compromised, and how….[It] attempts to give the reader a feel for what it is like to be an intruder and how to go from knowing nothing about a system to compromising its security. (Farmer and Venema 1993, 2-3).

In an interview years later Farmer cited Sun Tsu's dictum—"to know your enemy you must become them"—as inspiration for their "unusual" approach (Rik 2014,33). In addition to describing the techniques and strategies for performing reconnaissance on a target and the modes of exploiting trust in badly configured systems, the paper also announced that the pair had developed a new automated security scanner. SATAN (Security Administrator Tool for Analyzing Networks) compiled the assortment of tools Farmer and Venema used to test systems and bundled them into a single, easy-to-use application. They made the toolkit freely available and generated significant media controversy in the process, because, despite its obvious utility, the software significantly lowered the technical barriers to cracking computer systems. SATAN aggregated vulnerability-scanning tools and simplified their use through an intuitive graphic user interface; it represented a powerful tool for both cybercriminals and security researchers alike.

Since SATAN's release, penetration and vulnerability testing software suites have proliferated and become more powerful. Many are freely available and dramatically simplify the exploitation of vulnerable systems. Much like SATAN, they are known as "dual-use" technologies in that they can be used for legitimate research purposes, as well as criminal ones. A case in point is the widely available Metasploit attack platform—an application which allows for the configuration of exploits (it comes loaded with exploits that target bugs in Windows, Unix/Linux and Mac OS), information gathering on a target's vulnerabilities, choosing and executing payloads (for example loading a shell or backdoor on a remote server), and masking the encoded payload so it is not detected.

When it was first released in 2003 by the prominent security researcher HD Moore it came with only 11 exploits. The following year, when Moore and colleague "spoonm" detailed version 2.0 at security conference DEF CON 12, the platform had grown to 19 exploits and 27 payloads; the current free version boasts over 1,500 exploits. Metasploit streamlined the assembly of exploits and their customization while simultaneously lowering the degree of skill necessary to launch attacks. Once a new vulnerability is discovered, a researcher can quickly develop a new attack script using the platform's built-in components (Wang, R., Peng, N., Tao, X. & Quan, C. 2013). Newly discovered exploits and vulnerabilities are rapidly incorporated within the framework's "modules"—sometimes exploits are released before a patch for the software vulnerability is made available. According to Moore, the code base is updated dozens of times a day by in-house developers and the submissions of the wider community of research contributors (Moore 2011, xiv).

Predictably, as soon as a plugin or release is distributed for Metasploit there is a pronounced two-day spike in the use of these exploits against targets worldwide (Ramirez-Silva & Dacier 2007, 210). Even when a patch is available, as in the case of the Wannacry outbreak, the temporal gap between its publication and the patching of vulnerable systems can be significant. Just days after the release of the Wannacry bug, the NSA exploit "EternalBlue" which the bug is based upon, was available on Metasploit. More recently, three other zero-day exploits that were released alongside EternalBlue—EternalSynergy, EternalRomance, and EternalChampion—were ported into Metasploit (Arghire 2018).

Law enforcement has also been known to use Metasploit: the FBI famously used the "Metasploit Decloaking Engine" to identify Tor users of child pornography sites on the dark web in "Operation Torpedo" (Poulsen 2014). Metasploit is open source—individuals can contribute to its functionality, but it is owned by Rapid7 which retails the platform as a subscription service to corporate and state clients like the US federal government. An advertisement reads:

> Cyber-attacks on Federal government networks and systems are increasingly sophisticated, frequent, and dynamic. Federal departments and agencies need a way to assess the overall effectiveness of their defenses against real-world attack (Rapid7 flyer nd).

Metasploit is but one of a number of "free" vulnerability exploitation tools which automate, significantly simplify and powerfully augment the penetration tester (and hence hacking and cybercriminal) tool kit. For example, Rapid 7 also maintains the very advanced penetration and security auditing platform KaliLinux. The software bundles a number of other freeware, open source and subscription attack tools into an intuitive point and click graphic user interface (GUI). It contains tools for reconnaissance or "scanning", vulnerability analysis, exploitation, wireless attacks, password attacks–as well as forensics, stress testing, sniffing and spoofing.

SATAN, Metasploit and KaliLinux illustrate how code functions as a boundary object. There is translation and modification, as the tools are modified for different purposes. There too is a tacking back-and-forth from the state, to hackers or leakers, and back to different state domains through the contributions of open source code. These penetration suites anchor an indirect but functional set of exchanges and interactions across different domains of practice. On the one hand, security specialists adopt these software tools to detect and patch vulnerabilities in the systems they are paid to protect. To do so effectively they must think like a "criminal" and ensure that the intrusion devices they adopt are current and that the attack vectors they use are imaginative. In the process of this work, these specialists also modify the tools themselves (e.g., they write a new exploit) and help keep the platforms up to date. Yet this also updates the toolkit of potentially malicious hackers who would not necessarily have the skills to do it themselves. Instead of writing the code, they can just download the tool and use it. Thus, the widespread availability of these tools, as well as their relatively intuitive design and innovative character, also potentially multiplies the security problem and completes the collaborative circuit inclusive of state hackers, cybercrimals, hacktivists, and open source coders.

Despite the boundary defining characteristics described above, SATAN and Metasploit are examples unlike those typically examined in the STS literature. The boundary work around them does not result in above the counter and kindly collaboration: it is flexible but the translation it produces is neither intentional nor transparent. A closer look at the circuitous path of EternalBlue, EternalSynergy, EternalRomance, and EternalChampion underscores the point. Once leaked by the Shadow Brokers, these zero-day vulnerabilities were quickly repackaged into the building blocks of malware responsible for three highly destructive global ransomware attacks (Wannacry, Notpetya, Bad Rabbit). Later, they were ported into the Metasploit framework by security researchers and thus formed part of the updated code-base that helps protect government networks and is marketed to federal authorities as a subscription service. Even more recently, EternalBlue has reappeared; targeting local and city governments (i.e., Baltimore, Allentown and San Antonio) in the United States with crippling ransomware attacks (Perloth & Shane 2019). NSA property—after having been utilized in malicious acts around the world—returns home where it finds a place among practitioners working in another arm of the state but also within ageing IT infrastructure—opening up vectors for new attacks. Software like Metasploit establishes links across states, hackers, open source volunteers, freelance security researchers and those targeted by code weapons. It also underscores the wider unresolved ethical issues that come bundled with the enthusiastic adoption of state hacking by both democratic and authoritarian regimes.

DEF CON: Come Meet the Feds

DEF CON is the biggest hacker conference in the world and has been running for twenty-six years. It is a key site to witness the state's steady expansion into the field of hacking as well as the strategic realignment of its boundaries. Hacker conferences like DEF CON, display the "social enchantment and moral solidarity" that comes with shared craft culture—the making and arranging of code (Coleman 2010: 47). It is an elite and costly affair that also works hard to remain liminal and situate itself on the edge of state practices. In earlier incarnations, fugitives and criminals boldly attended (DEF CON 10: 2002; Zetter 2014) but when we arrived at DEF CON 25 (2017), the difficulties inherent in staging a conference at Caesar's Palace, Las Vegas, and maintaining any semblance of counterculture were readily apparent. Well-paid IT professionals come here to recreate while being on the job. White, grey, and black hat hackers and sympathizers attend. Government officials and IT specialists are also present to inflate their cultural and symbolic capital as well as to recruit personnel and gather intelligence.

In a panel session titled “DC to DEF CON”, cyber-security researcher Josh Corman used alliteration around the letter “p” to introduce US Congressmen James Langevin (D-RI) and Will Hurd (R-Texas) from the US Homeland Security Committee. Participants are *protectors*—who want to make the internet safer. *Puzzlers*—who enjoy tinkering and solving problems. Others hack for *prestige*, *power*, *pride*, *profit*, and *professional* development. Some are motivated by *protest*. Corman identified himself as a protector and puzzler who took pride in the growing official recognition of the hacking profession. The panel represented the first time two sitting members of Congress attended the conference and focused on how to develop a “dialogue” between hackers and US legislators.

In his remarks, Rep. Langevin pointed to evidence of this new collaborative relationship in the form of programs like the “Hack the Pentagon”. The program took place over the course of one month in 2017 and involved 1400 hackers identifying 125 security vulnerabilities. According to Langevin this crowdsourced effort was undertaken “...at a fraction of the cost per bug of existing programs” and he announced that the Pentagon would soon expand the program even as other departments, like the Internal Revenue Service, looked ready to follow suit. The audience met the Congressmen’s remarks with a standing ovation, making clear that the partnerships forged at DEF CON between government officials and hackers had been in development for some time.

Indeed, DEF CON 20 (2012) and 21 (2013) are key moments for situating the realignment of hacker/state boundaries. General Keith Alexander, then head of the NSA and US Cyber Command, was invited to give the keynote address in 2012 and his talk—as well as the responses it elicited, illustrate the transitional tension in the earlier years.

> In this room, this room right here, is the talent our nation needs to secure cyberspace…. Sometimes you guys get a bad rep….[but] from my perspective, what you guys are doing to figure out vulnerabilities in systems is absolutely needed. We have to discover and fix those. You guys hold the line.

A number of hecklers in the audience shouted counterpoints like: "Then stop arresting us!" They produced protest signs with statements like "Bullshit." Yet the conference hall was standing room only and hundreds of would-be attendees had to be turned away (Kopfstein 2012, Constantin 2012). In preparation for the conference, the NSA set-up a special recruiting site which reassured applicants with the line: “If you have a few, shall we say, indiscretions in your past, don't be alarmed” (Cowley 2012).

However, a year later, DEF CON’s organizers decided to exclude federal authorities, citing Edward Snowden’s revelations about the scope of US government bulk surveillance programs. Yet a number of professionals and participants balked at this reaction. Jeffrey Carr, CEO of Taia Global (a private cyber-security firm) captured the mood: "It doesn't make any sense to me, especially since so many hackers have built up a close relationship with the government over the years” (Mello 2013).

At DEF CON 25 in 2017, the Feds were everywhere. In between panels titled, “Meet the Feds” and “Hacking Democracy”—two panels that featured former or present federal employees explaining how their work does or should overlap with hackers’—we met a DC lawyer who had been attending DEF CON for years and had also worked with the federal government. He confirmed that the “Feds” were “genuinely good folks” intent on building bridges and developing channels for better communication.

Bug Bounties

Since the mid-2000s there has been a veritable boom in cyber security markets of every stripe. This has been a by-product of the increasing prominence of state hacking and the expansion of contract work in offensive hacking and computer security more generally. For example, although two dozen states maintain active cyber-defense and offense divisions, many more outsource this work to intermediaries or proxies (Maurer 2018: 27). This situation has generated a lucrative market for off-the-shelf attack software, rare exploits and zero-day vulnerabilities. Bug bounty programs (also known as Vulnerability Reward Programs [VRP]) have been in operation since the mid-1990s when Netscape first announced that it would pay up to $1,000 to anyone that reported a flaw with their new browser, Netscape Navigator 2.0 (Ellis, Huang, Siegel, Moussouris & Houghton 2018). This was followed by Firefox in 2004, Google in 2010 and Microsoft in 2013.

Although the rules and parameters vary significantly, “bounty hunters” generally look for bugs in software code that can be exploited and disclose those vulnerabilities to the software vendor or client in return for a monetary reward; they also agree on a timeframe for the public disclosure of the vulnerability (usually after the vendor has produced a patch). Bounties are awarded only if a researcher: is the first to disclose the vulnerability, follows the rules of engagement and if the vulnerability is eligible for reward. These programs give security researchers and hackers an incentive to disclose vulnerabilities rather than sell them for profit on the black market.

The size of this market place is large, growing and diversified. Alongside the established private VRPs maintained by technology companies, much of this activity is increasingly run by specialist “crowdsourced” cyber security firms that sit as intermediaries between the clients opening their systems up for testing and the “hunters” seeking to earn a reward. These companies have varied profit models and boast a range of unique services. For example, Synack, founded in 2013 by two former NSA agents, recruits and trains military veterans to join its “red team” of cyber security specialists (Sheridan 2018). Hackerone, on the other hand favors scale over boutique status: it jumped from a registered pool of a 166,000 hackers to over 300,000 in just two years (Vaas 2018, HackerOne 2019).

One of the areas of significant growth has been government contracts. The US government has accelerated the pace with which it crowdsources vulnerability testing. In 2017, the US Army and the Air Force both ran their own versions of bug bounty programs and in 2017, the General Services Administration announced the first non-military bug bounty program that will run on an ongoing basis with bounties ranging from $200 to $2,000. Since 2016, the Department of Defense has also run parallel awards programs: a private one that tests internal systems (modeled after the private Big Tech initiatives) and a public one that tests public-facing systems. Synack, with its smaller but higher vetted personnel runs a DOD bounty program that focuses on the DOD’s sensitive IT assets (HackerOne and Synack 2016) and now counts up to fifteen US government agencies among its roster of clients including: the Center for Disease Control, The Internal Revenue Service, The Department of Human Services, the Department of Transportation and others.

It is not just the United States government. Singapore’s government partnered with HackerOne in 2017 to identify bugs and vulnerabilities in defense and military websites and broadened the program in 2018 to host a three-week government bug bounty program where hackers were invited to submit vulnerabilities in ICT systems for rewards ranging between $250-10,000 (Kovacs 2018). Switzerland opened up its online election system to a bug bounty program and the European Union has recently announced that it would be launching 14 bug bounty programs for open source software that European Union institutions rely on (Porter 2019, O’Donnell 2019).

Bug bounty intermediaries like Synack or HackerOne and annual meetups like DEF CON can be understood as boundary organizations. They establish “bridges” (Franks 2010, 283) between agents on different sides of the boundary and provide the opportunity for these differently positioned actors to be present at that boundary in a light that is favorable to their divergent perspectives (Guston 2001). As Spence argues, the concept of boundary organizations “…places attention to the mechanisms and operating conditions that enable the flow of ideas, concepts, information and skills between social worlds” (2017, 795). Boundary organizations like DEF CON or HackerOne provide differently situated actors with the legitimacy and credibility to jointly perform work that would be difficult to undertake unilaterally (Spence 2017, 806).

Conclusion: Expansion of the Hacker State Domain

We looked closely at the methods of the hacker state through examples ranging from the proliferation of boutique state-security firms like DarkMatter, the rise of offensive security and ethical hacking, the reframing of the relationship between hackers and the state at cyber security conferences and the crowdsourcing of government penetration-testing through bug bounties. We seek to link the abstract boundary practices of the state articulated in the academic literature to the actual practices of hackers as state boundary workers. We describe hacker toolkits and penetration platforms to illustrate the blurred terrain between the inside and outside of the networked state's boundary. The vulnerability, exploitation, stress testing and sniffing tools would-be ethical hackers and security professionals train on and adopt in their everyday work are the same tools used by supposed cybercriminals as well as politically motivated hacktivists. Hacker tools are "boundary objects" (Star & Griesemer 1989: 393), adaptive materials with common yet distinct meanings that allow translation and mutual understanding across potentially conflicting code cultures. They bridge multiple competing spaces of practice (state hacking, ethical hacking, cybersecurity, hacktivism and cybercrime) opening multiple vectors of recognition and grooming for would-be state boundary workers. At the same time, they also anchor a series of unintentional and disruptive collaborations (with cybercriminals, hacktivists and hostile state actors) which in their way also contribute to the stabilization of boundaries. The wide adoption of exploit kits and vulnerability testing suites by hackers of all stripes provides the rationale for why they must be kept at-a-distance (through criminalization or proxy work) but also the necessity for their transcendence through the structuring of interaction and governance within boundary organizations.

A case in point is DEF CON where we witnessed and engaged in conversations at the boundary between networked state functionaries and hacking practitioners. If in the years between 2012 and 2013, the chances for collaboration between state officials and hackers were framed as contingent, unstable and fleeting; by 2017, there was a clear commitment towards cooperation on information and job security. State assemblages obviously require hackers within their boundaries (not simply at-a-distance) and hackers need jobs and access to sophisticated tools and big data. Events like DEF CON are boundary organizations, spaces where differentially motivated actors come together around a singularly framed opportunity—to co-create the hacking world. Bug bounty intermediaries like HackerOne provide a contrasting model of boundary organizations in that their purpose is not recruitment or facilitating communication across boundaries but the facilitation and production of joint security work. In this case, bug bounty platforms enable "the flow of ideas, concepts, information and skills between social worlds" (Spence 2017, 795) in the absence of stable communication between these two worlds.

As we discuss throughout this article, the boundaries between hackers and state officials are unstable and open to contingency. We map this instability in terms of the attack platforms (boundary objects) cybercriminals, state cybersecurity professionals, security researchers, hacktivists and ethical hackers use in their work. We argue that much like the boundary between science and politics discussed in the STS literature, these boundary objects allow for collaboration and translation across different domains of practice, sometimes contributing to the stability of the border between hacking and the state, and sometimes undermining it. Yet following others we also argue that an important element in negotiating this seeming impasse involves structuring boundary work through governance arrangements (boundary organizations) which internalize the unstable character of boundaries and negotiate these contingencies as part of their daily work (Guston 1999, Franks 2010).

Works Cited

Abrams, P. (1998). Notes on the Difficulty of Studying the State. *Journal of Historical Sociology*, 1(1): 58-89.

Arghire, I. (2018). NSA-Linked hacking tools ported to Metasploit. *Security Week.* https://www.securityweek.com/nsa-linked-hacking-tools-ported-metasploit

Ben-Yehuda, N. (1986). The Sociology of Moral Panics: Toward A New Synthesis. *Sociological Quarterly*, 27(4), 495-513.

Boland, R.J. & Tenkasi, R.V. (1995). Perspective Making and Perspective Taking in Communities of Knowing. *Organization Science*, 6(4), 350-372.

Bowker, G., & Star, S.L. (1999). *Sorting things out: Classification and its consequences (Inside technology)*. Cambridge, Mass.: MIT Press.

Brandom, R. (2016). Apple is launching an invite-only bug bounty program. *The Verge*. https://www.theverge.com/2016/8/4/12380036/apple-bug-bounty-program-vulnerability-security

Carroll, P. (2012). Water and Technoscientific State Formation in California. *Social Studies of Science*, 42(4): 489-516.

Carroll, P. (2009). Articulating Theories of States and State Formation. *Journal of Historical Sociology*, (22):553-603.

Centellas, K., Smardon, R., & Fifield, S. (2014). Calibrating Translational Cancer Research: Collaboration without Consensus in Interdisciplinary Laboratory Meetings. *Science, Technology, & Human Values,* 39(3): 311-335.

Cohen, S. (1980). *Folk devils and moral panics: The creation of the Mods and Rockers*. New York: St. Martin's Press.

Constantin, L. (2012). NSA Chief Asks Hackers at Defcon for Help Securing Cyberspace. *PCWorld*. https://www.pcworld.com/article/260007/nsa_chief_asks_hackers_at_defcon_for_help_securing_cyberspace.html.

Cowley, S. (2012). NSA Wants to Hire Hackers. CNN Money. https://money.cnn.com/2012/07/27/technology/defcon-nsa/index.htm.

DEF CON 10. (2002). Defcon 10 – Wolves Among Us (1 of 7), https://www.youtube.com/watch?v=-jvHkbDcxmw

Donaghy, R. (2012). In the UAE, the future for those who continue to speak out looks bleak. *The Guardian*. https://www.theguardian.com/commentisfree/2012/jul/18/uae-emirates-battle

Ellis, R., Huang, K., Siegel, M., Moussouris, K. & Houghton, J. (2018). Fixing a hole: The labor market for bugs. In H. Shrobe, D.L. Shrier & A. Pentland, New Solutions for Cybersecurity. Cambridge, Mass.: MIT Press.

Farmer, D. & Venema, W. (1993). Improving the security of your site by breaking into it. https://cyberwar.nl/d/1993-FarmerVenema-comp.security.unix-Improving-the-Security-of-Your-Site-by-Breaking-Into-It.pdf

Farrow, R. (2014). Interview with Dan Farmer. *;login:*, 39(6): 32-35. https://www.usenix.org/system/files/login/articles/login_dec14_07_farmer.pdf

Fish, A. (2017). *Technoliberalism and the End of Participatory Culture in the United States*. Cham, Switzerland: Palgrave Macmillan.

Fish, A., Murillo, L., Nguyen, T., Panofsky, A. & Kelty, C. (2011). Birds of the Internet: Towards a Field Guide to Participation and Governance. *Journal of Cultural Economy*, 4:157–187.

Franks, J. (2010). Boundary Organizations for Sustainable Land Management: The Example of Dutch Environmental Co-operatives. *Ecological Economies* 70(2): 283-295.

Gasson, S. (2006). A genealogical study of boundary-spanning IS design. *European Journal of Information Systems*, 15(1): 26.

Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: strains and interests in professional ideologies of scientists. *American Sociological* Review, 48 (6): 781–795.

Guston, D.H. (1999). Stabilizing the Boundary between US Politics and Science: The Role of the Office of Technology Transfer as a Boundary Organization. *Social Studies of Science* 29(1):87-111.

Guston, D.H. (2001). Boundary Organizations in Environmental Policy and Science: An Introduction. *Science, Technology & Human Values* 26(4): 399-408.

HackerOne. (2019). The 2019 Hacker Report. *HackerOne*. https://www.hackerone.com/resources/the-2019-hacker-report.

HackerOne and Synack. (2016). Department of Defense Awards $7 Million Crowdsourced Security Contracts to HackerOne and Synack. *Business Wire* (Press Release). https://www.businesswire.com/news/home/20161020006521/en/Department-Defense-Awards-7-Million-Crowdsourced-Security

Huvila, I. (2011). The politics of boundary objects: Hegemonic interventions and the making of a document. *Journal of the American Society for Information Science and Technology*, 62(12): 2528-2539.

Kirkpatrick, D. (2018). Israeli Software helped Saudis spy on Khashoggi, lawsuit says. *The New York Times*. https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html?module=inline

Kopfstein, J. (2012). NSA Trolls for Talent at Def Con, the Nation’s Largest Hacker Conference. *The Verge*. https://www.theverge.com/2012/8/1/3199153/nsa-recruitment-controversy-defcon-hacker-conference.

Kovacs, E. (2018). Singapore Government Announces Second Bug Bounty Program. *Security Week*. https://www.securityweek.com/singapore-government-announces-second-bug-bounty-program

Levy, S. (2010). *Hackers: Heroes of the Computer Revolution*. Sebastpol, Ca.: O’Reilly Media.

Marczak, B. & Scott-Railton, J. (2016). The Million Dollar Dissident: NSO Group’s iPhone zero-days used against a UAE human rights defender. *The Citizen Lab*. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Marczak, B., John Scott-Railton, S. McKune, Bahr Abdul Razzak, & Ron Deibert. (2018). Hide and Seek: Tracking NSO Group’s Pegasus Software to Operation in 45 Countries, The *Citizen Lab*. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Mayrl, D., & Quinn, S. (2016). Defining the State from within: Boundaries, Schemas, and Associational Policymaking. *Sociological Theory,* 34(1): 1-26.

Maurer, Tim. (2018). *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge: Cambridge University Press.

Mazzetti, M., Goldman, A., Bergman, R. & Perlroth, N. (2019). A New Age of Warfare: How Internet Mercenaries do Battle for Authoritarian Governments. *The New York Times*. https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html

McLaughlin, J. (2017). Deep Pockets, Deep Cover: The UAE is paying ex-CIA officers to build a spy empire in the Gulf. *Foreign Policy*. https://foreignpolicy.com/2017/12/21/deep-pockets-deep-cover-the-uae-is-paying-ex-cia-officers-to-build-a-spy-empire-in-the-gulf/

Mello, J.P. (2013). "The Ban on Defcon Draws a Mixed Reaction." *CIO*. https://www.cio.com/article/2384191/the-ban-on-feds-at-defcon-draws-a-mixed-reaction.html

Midgal, J. S. & Schlichte, K. (2005). Rethinking the State. In J.S. Migdal (Ed.), *The Dynamics of States: The Formation and Crises of State Domination*. Aldershot, UK and Burlington, VT.: Routledge.

Mitchell, T. (1991). The Limits of the State: Beyond Statist Approaches and their Critics. *American Political Science Review*, 85(1):77-96.

Moore, H.D. (2011). Foreword. In Kennedy, D., O'Gorman, J., Kearns, D. & Aharoni, M. *Metasploit: The Penetration Tester's Guide*. San Francisco, Ca.: No Starch Press.

O'Donnell, L. (2019). EU Offers Bug Bounties for 14 Open Source Projects. *Threat Post*. https://threatpost.com/eu-offers-bug-bounties-for-14-open-source-projects/140473/.

Pelroth, N. & Shane, S. (2019). In Baltimore and beyond, a stolen NSA tool wreaks havoc. *The New York Times*. https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Porter, J. (2019). Swiss E-Voting Trial Offers $150,000 in Bug Bounties to Hackers. *The Verge*. https://www.theverge.com/2019/2/12/18221570/swiss-e-electronic-voting-public-intrusion-test-hacking-white-hack-bug-bounties.

Poulsen, K. (2014). The FBI Used the Web's Favorite Hacking Tool to Unmask TOR Users. *Wired*. https://www.wired.com/2014/12/fbi-metasploit-tor/

Ramirez-Silva, E. & Dacier, M. (2007). Empirical Study of the Impact of Metasploit-Related Attacks in 4 Years of Attack Traces. In I. Cervesato (Ed.) *Advances in Computer Science – ASIAN 2007. Computer and Network Security*. Berlin, Heidelberg: Springer.

Ribes, D. (2018). STS, Meet Data Science, Once Again. *Science, Technology and Human Values*, 44(3) 514-539.

Scott-Railton, J., Marczak, J.B., Guarnieri, C. & Crete-Nishihata, M. (2017). Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links. *The Citizen Lab*. https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

Sheridan, K. (2018). Veterans Find New Roles in Enterprise Cyber Security. *Dark Reading*. https://www.darkreading.com/risk/veterans-find-new-roles-in-enterprise-cybersecurity/d/d-id/1333250.

Spence, J. Is a Melting Arctic Making the Arctic Council Too Cool? Exploring the Limits to the Effectiveness of a Boundary Organization. *Review of Policy Research* 34(6): 790-811.
Star, S. L. (1988). The structure of ill-structured solutions: Boundary objects and heterogeneous distributed problem solving. In M. Huhns & L. Gasser (Eds.), *Readings in distributed artificial intelligence*. Menlo Park, CA: Kaufman.

Star, S. L. (1989). *Regions of the mind: Brain research and the quest for scientific certainty*. Stanford, CA: Stanford University Press.

Star, S. L., & Griesemer, J. (1989). Institutional ecology, 'Translations', and Boundary objects: Amateurs and professionals on Berkeley's museum of vertebrate zoology. *Social Studies of Science*, 19: 387-420.

Star, S. L. (2010). This is Not a Boundary Object Reflections on the origin of a concept. *Science, Technology and Human Values*, 35(5): 601-617.

Steinmetz, K.F. (2016). *Hacked: A Radical Approach to Hacker Culture and Crime*. New York: NYU Press.

Sterling, B. 2013 [1992]. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Trediton Classics.

Vaas, L. (2018). Under the Hoodie: What Makes Bug Bounty Hunters Tick? *Naked Security*. https://nakedsecurity.sophos.com/2018/01/22/under-the-hoodie-the-ethical-hackers-keeping-you-running/.

Wang, R., Peng, N., Tao, X. & Quan, C. (2013). MetaSymploit: Day-One Defense Against Script-based Attacks with Security-Enhanced Symbolic Analysis. *22nd USENIX Security Symposium*. http://enigma.usenix.org/sites/default/files/sec13_proceedings_interior.pdf#page=73

Weber, M. (1992). *The Protestant Ethic and the Spirit of Capitalism*. London ; New York: Routledge.

Zetter, K. (2014). A convicted hacker and an internet icon join forces to thwart NSA Spying, *Wired*. https://www.wired.com/2014/07/dark-mail-hides-metadata-from-nsa/